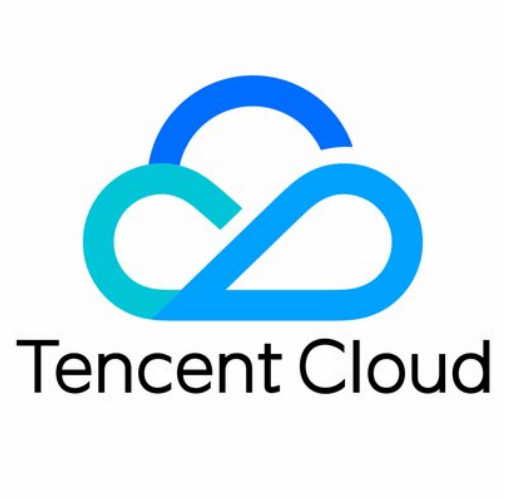
Tencent Cloud Firewall

Operation Guide

Product Documentation



Contents

Operation Guide
Firewall Toggle
Internet Perimeter Firewall Switch

Last updated：2024-10-29 14:45:56

Cloud Firewall offers an Edge Firewall toggle feature. On the **Edge firewalls** page, it can automatically detect the public IPs you own and the associated cloud assets, and configure the corresponding firewall toggle for you. The Cloud Firewall toggle supports one-click protection, eliminating the need for any network access deployment or routing policy configuration. Moreover, there is no requirement to install any image files. The Cloud Firewall offers a plug-and-play product experience.

Traffic Mode Explanation

How It Works	Serial Firewall
Deployment Path	The serial firewall is directly deployed on the path of network data flow. All passing packets need to be inspected and processed by the firewall.
Data Processing	Since a serial firewall needs to process all data packets passing through it, it has high performance and processing capacity requirements. If the firewall performance is insufficient, it may become a network bottleneck, affecting network speed and stability. Therefore, a new firewall instance needs to be created in each region and allocated with the corresponding bandwidth for a serial firewall.
Security Protection	The serial firewall can perform deep inspection and processing of data packets, providing high security. It can prevent malicious packets from entering the network, protecting internal resources from attacks.

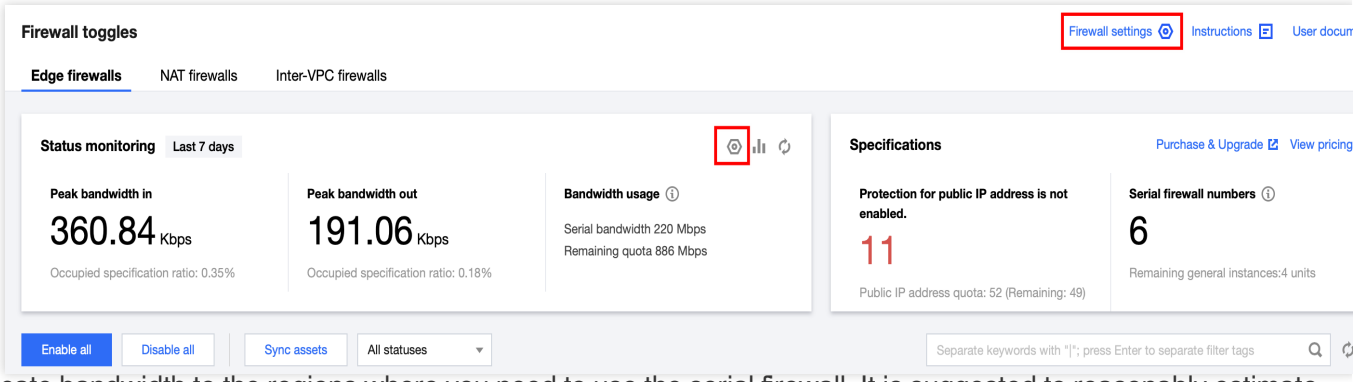
Preparation for Serial Firewall

Before using the serial firewall, please do the following preparations:

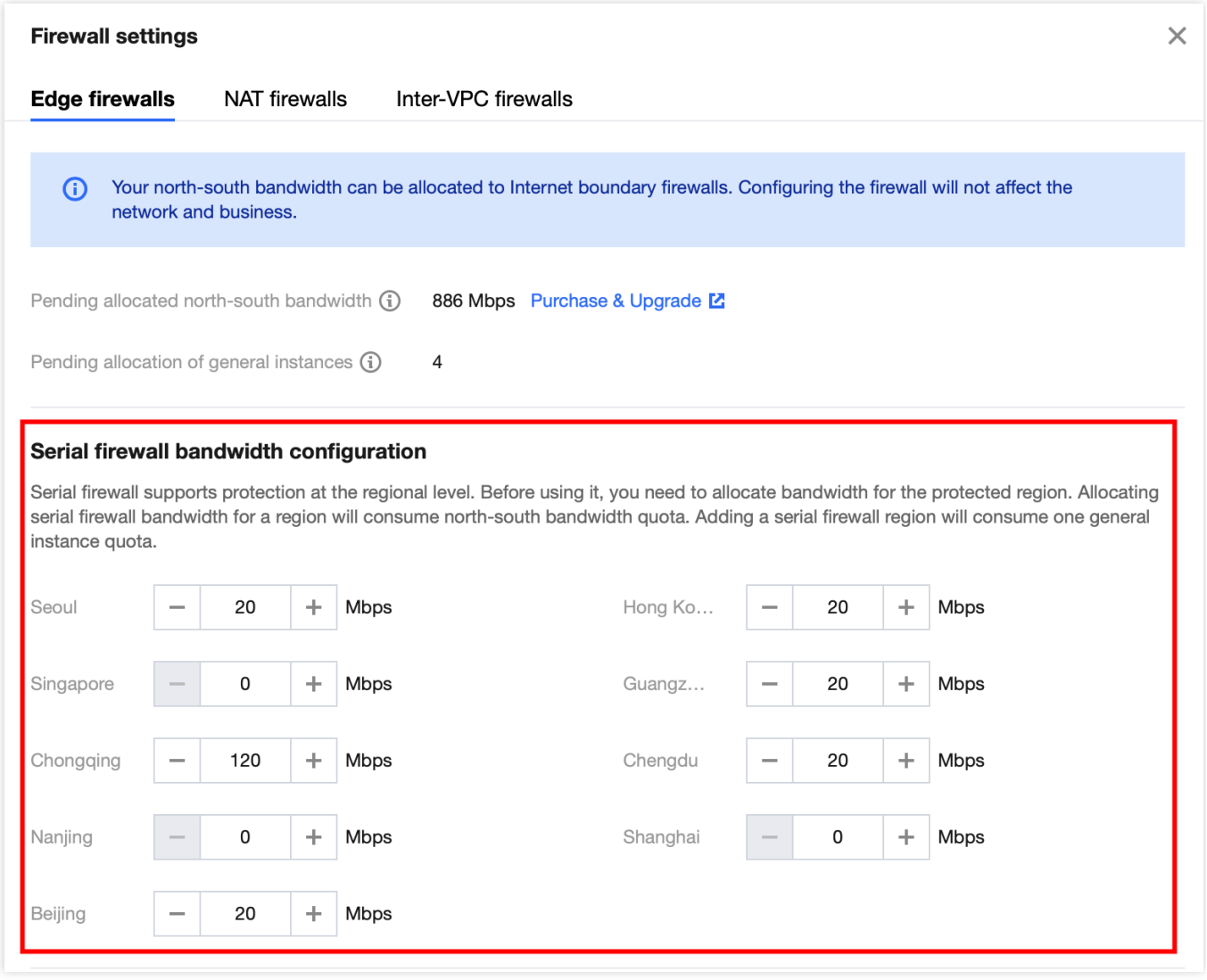
Allocate Bandwidth to the Serial Firewall

Since a serial firewall has regional cluster attributes and an upper limit on protection performance, users need to allocate bandwidth for the regions that need to use the serial firewall.

1. Log in to the Cloud Firewall Console, and in the left navigation bar, select **Firewall Toggles** > **Edge firewalls**.
2. On the **Firewall Toggles** page, click **Firewall settings**.



3. Allocate bandwidth to the regions where you need to use the serial firewall. It is suggested to reasonably estimate based on the business peak. **Excessive bandwidth may trigger service degradation,** causing some firewall toggles to shut down automatically.



Note:

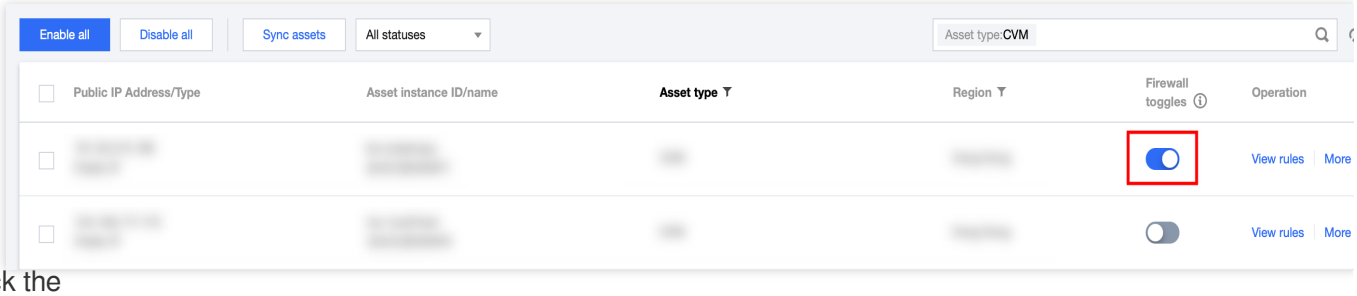
General bandwidth: General bandwidth will be consumed when allocating bandwidth for the serial firewall with the current version. General bandwidth is shared with the NAT Firewall.
General instance: One general instance quota will be consumed for each newly added serial firewall region of the current version. General instance quota is shared with NAT Firewall.
Serial firewall region: the supported regions of the current version are based on the aforementioned serial firewall setting display regions. More regions are gradually undergoing gray release, so stay tuned.

Confirm Assets Within Protection Range

Due to network architecture limitations, the current version of the serial firewall only supports protecting Elastic Public IPs in the latest network architecture, as specifically shown on the console. If you have any doubts, you can contact the Elastic IP team for confirmation. Public network CLB type is not currently supported. If protection is needed, it is recommended to switch to a form that supports protection through EIP + private network CLB.

Serial Firewall Toggle Operation

1. Log in to the Cloud Firewall Console, and in the left navigation bar, select **Firewall Toggles** > **Edge firewalls**.
2. On the **Edge firewalls** page, find the assets to be protected**.**



3. Click the  in the Firewall Toggles column to protect this asset at the edge.
4. The process to enable the serial firewall takes approximately 1 minute and has no effect on the network.

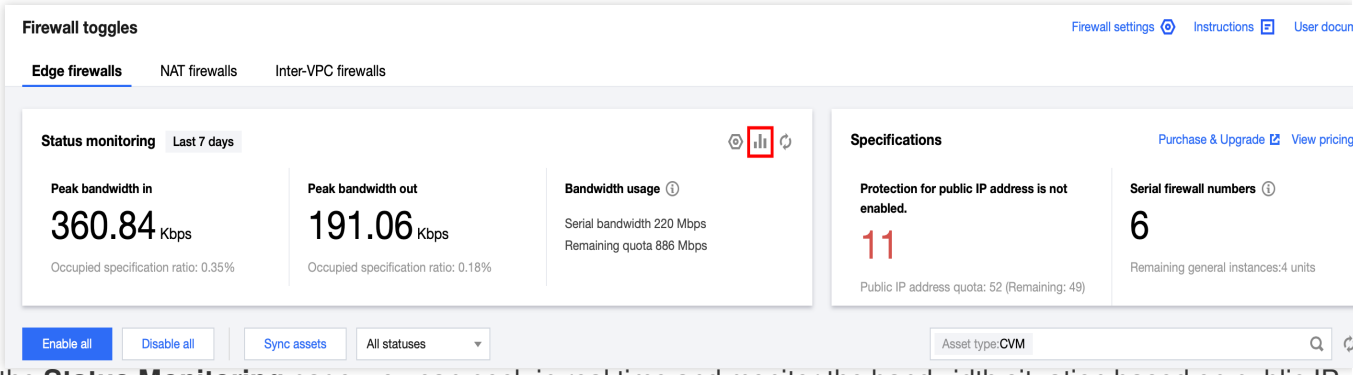
Note:

The serial pattern requires the use of a Private Link to establish a network from VPC to Firewall.
For the first time a EIP within the same VPC enables a serial firewall, a new Terminal Node for Private Link and diversion internal IP needs to be created. There's no additional charge for the Private Link within the scope of your serial firewall, but additional charges may apply beyond that. Please see Private Link Price. A new Private Link does not need to be created when you toggle the serial firewall within the same VPC subsequently.

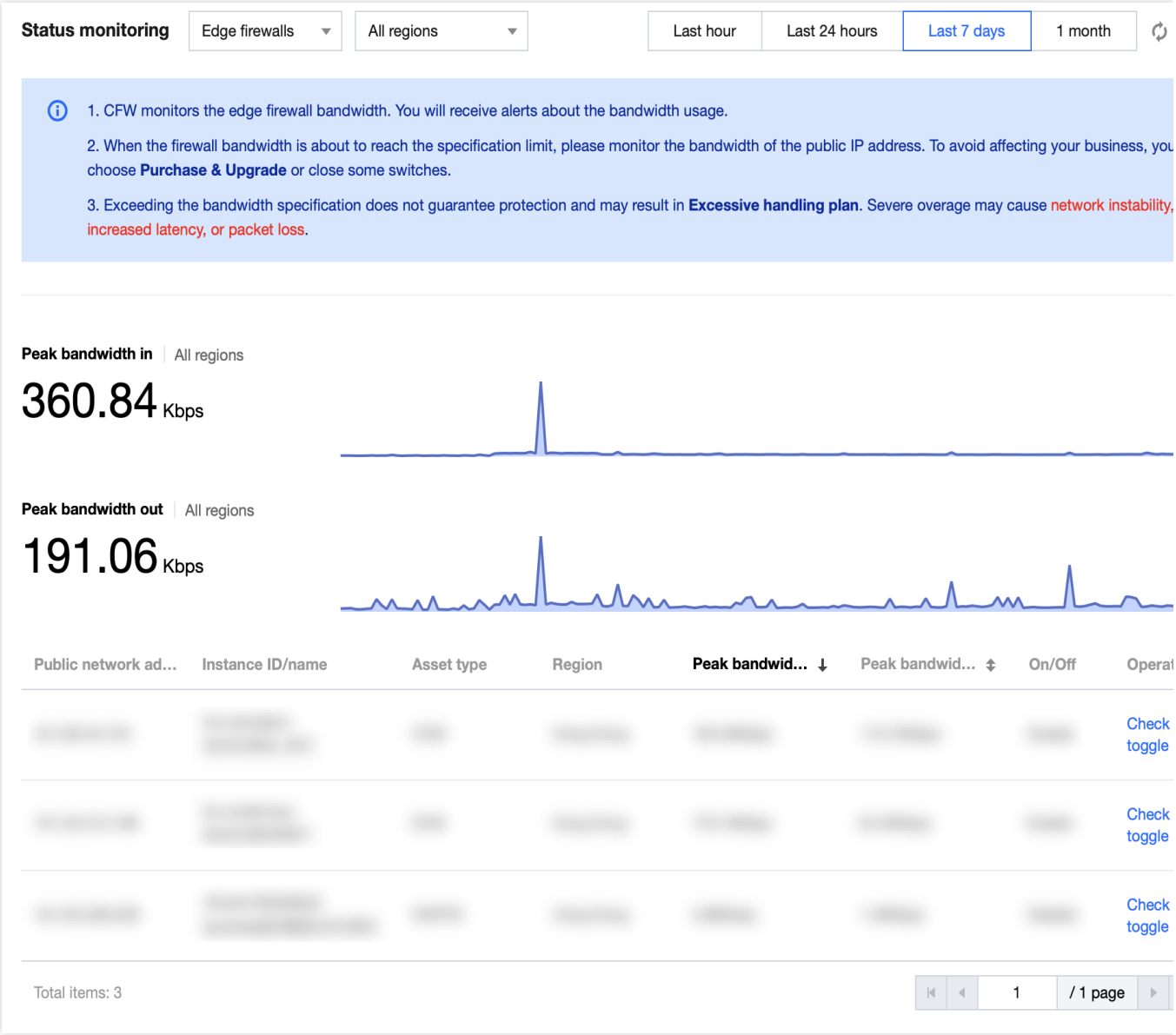
Status monitoring

Users can monitor and view the bandwidth status based on the public IP in real-time, enabling timely adjustments such as scaling or selectively closing toggles.

1. Log in to the Cloud Firewall Console, and in the left navigation bar, select **Firewall Toggles** > **Edge firewalls**.
2. In the upper right corner of the **Status Monitoring** panel on the **Edge firewalls** page, click the icon.



3. On the **Status Monitoring** page, you can peek in real time and monitor the bandwidth situation based on public IP, and perform operations such as expanding capacity or turning off some toggles.

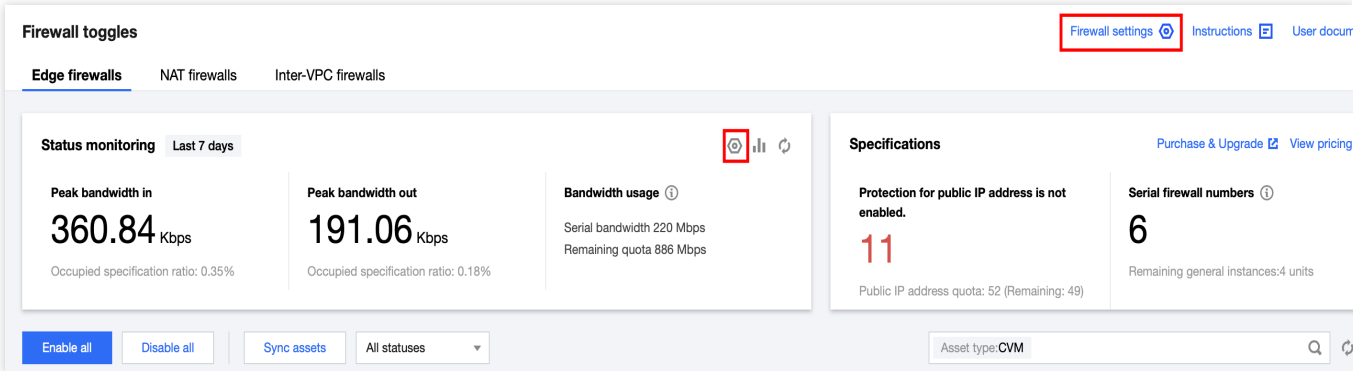


Note:

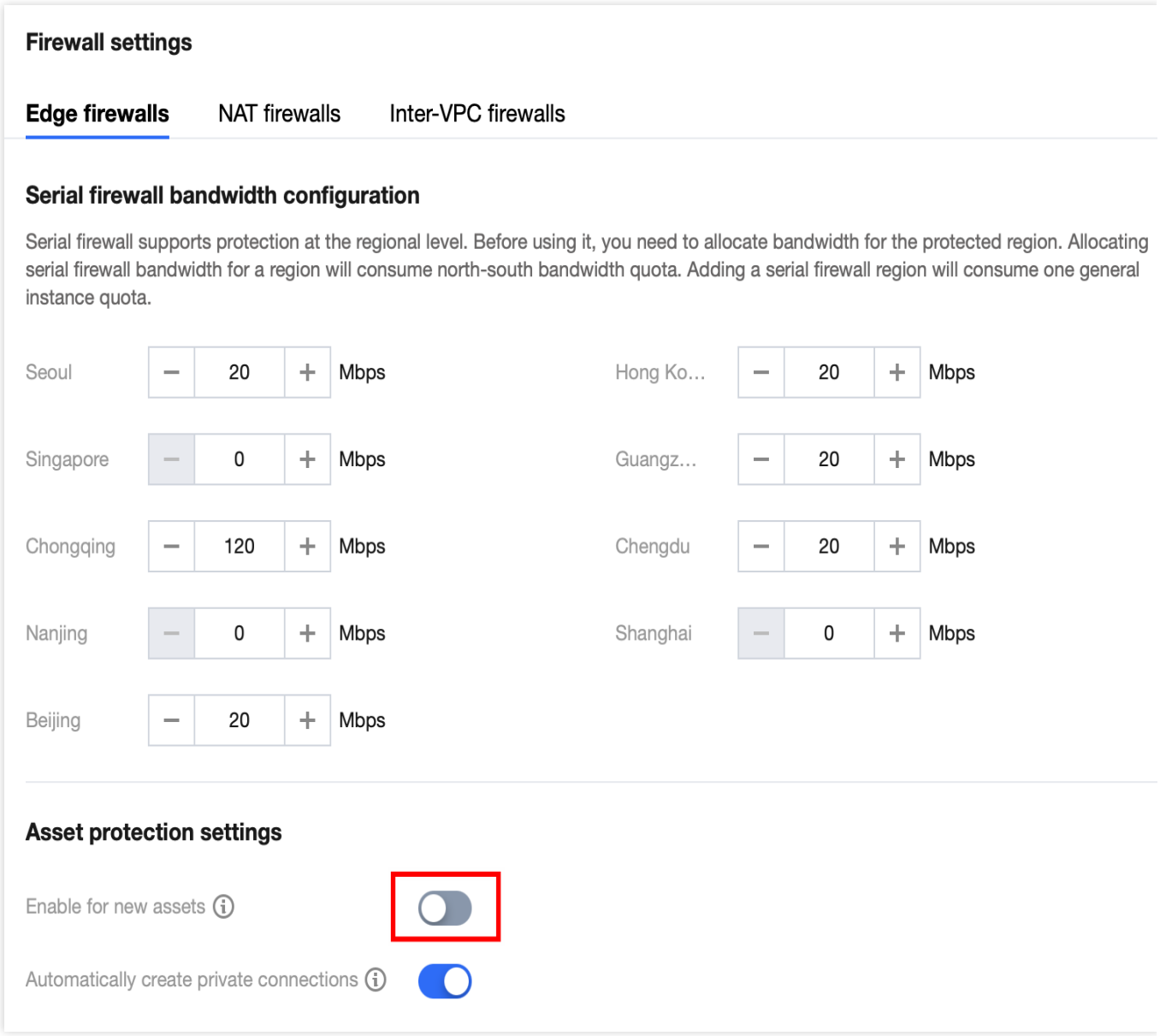
Peak bandwidth refers to the maximum of the upstream and downstream. For example, if you purchase 100 M of bandwidth, then the Cloud Firewall can handle both 100 M upstream and 100 M downstream at the same time.

Automatic Activation for New Assets

1. Log in to the Cloud Firewall Console, and in the left navigation bar, select **Firewall Toggles** > **Edge firewalls**.
2. On the **Firewalls Toggles** page, click **Firewall settings**.

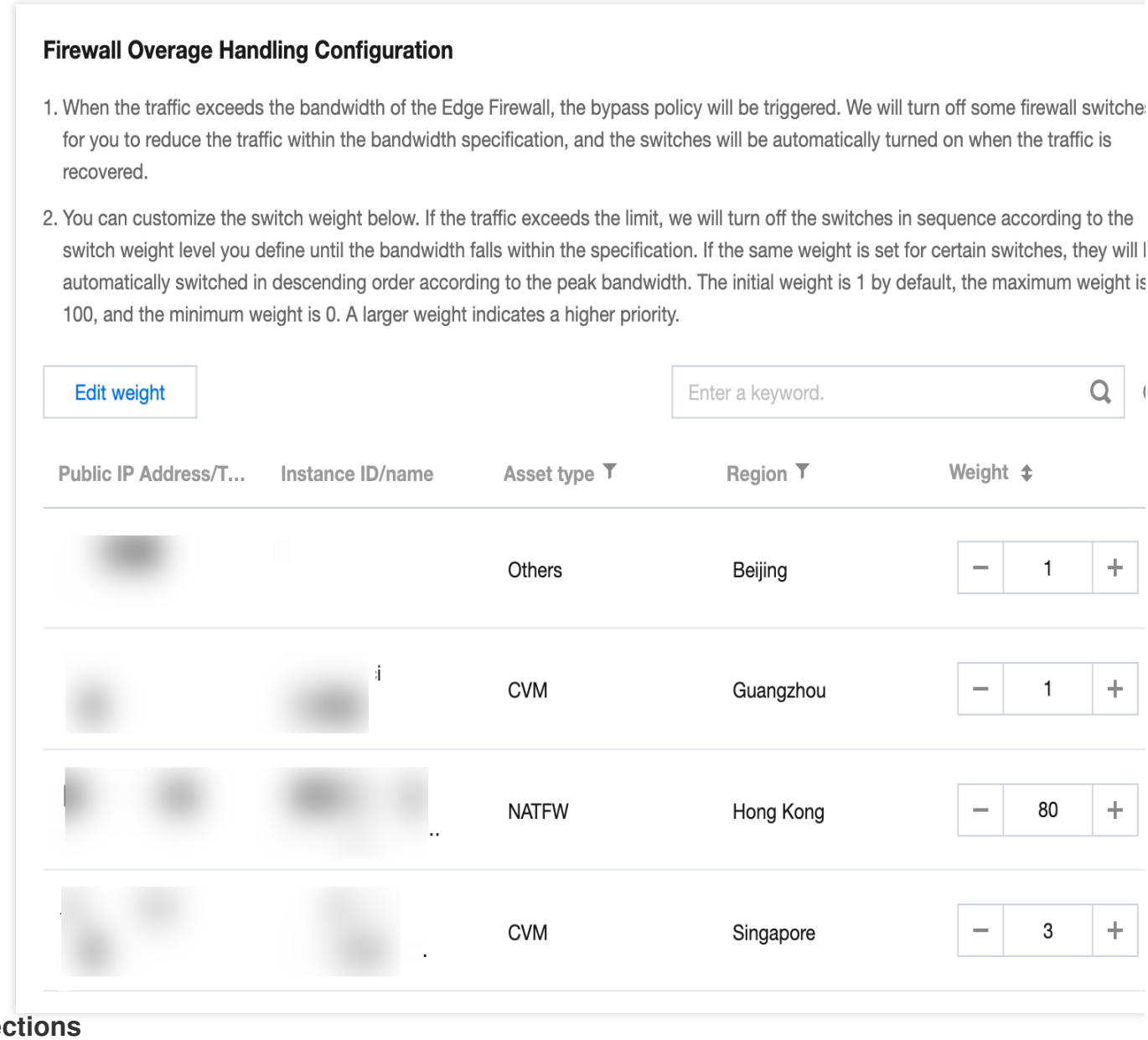


3. Click **Enable for new assets**. Within the allowed Quota of protected public IP, it will automatically enable the Edge firewalls for the newly added public IP assets. You can choose whether to enable the serial traffic pattern by default and whether to automatically create a Private Link.



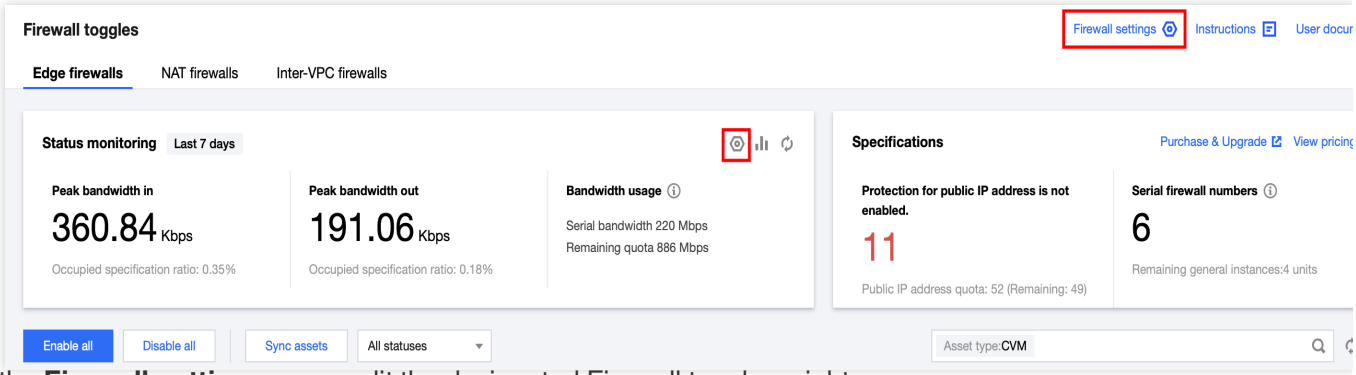
Excessive Bypass Configuration for Edge Firewall

When the business bandwidth exceeds the Edge Firewall bandwidth limit, specific measures will be taken.
You can specify the weights for firewalls. When the business bandwidth exceeds the Edge Firewall bandwidth limit, firewalls will be disabled based on the weights, and the bypass mode will be used until the bandwidth of the corresponding region decreases to below specifications. Firewalls with the same weight will be disabled automatically in descending order of peak bandwidth. The initial weight is 1 by default and can range from 0 to 100. A larger weight indicates a higher priority.

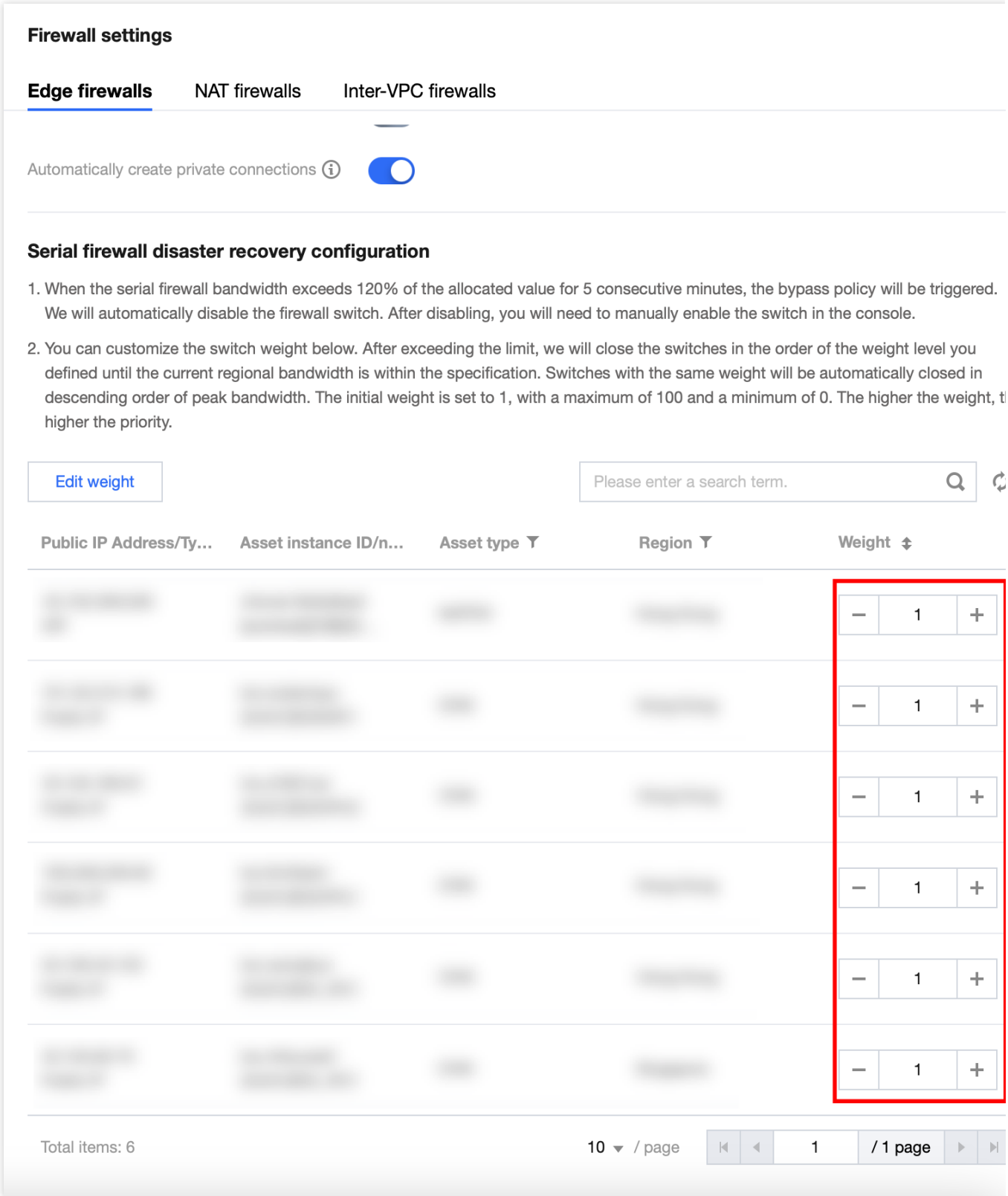


Directions

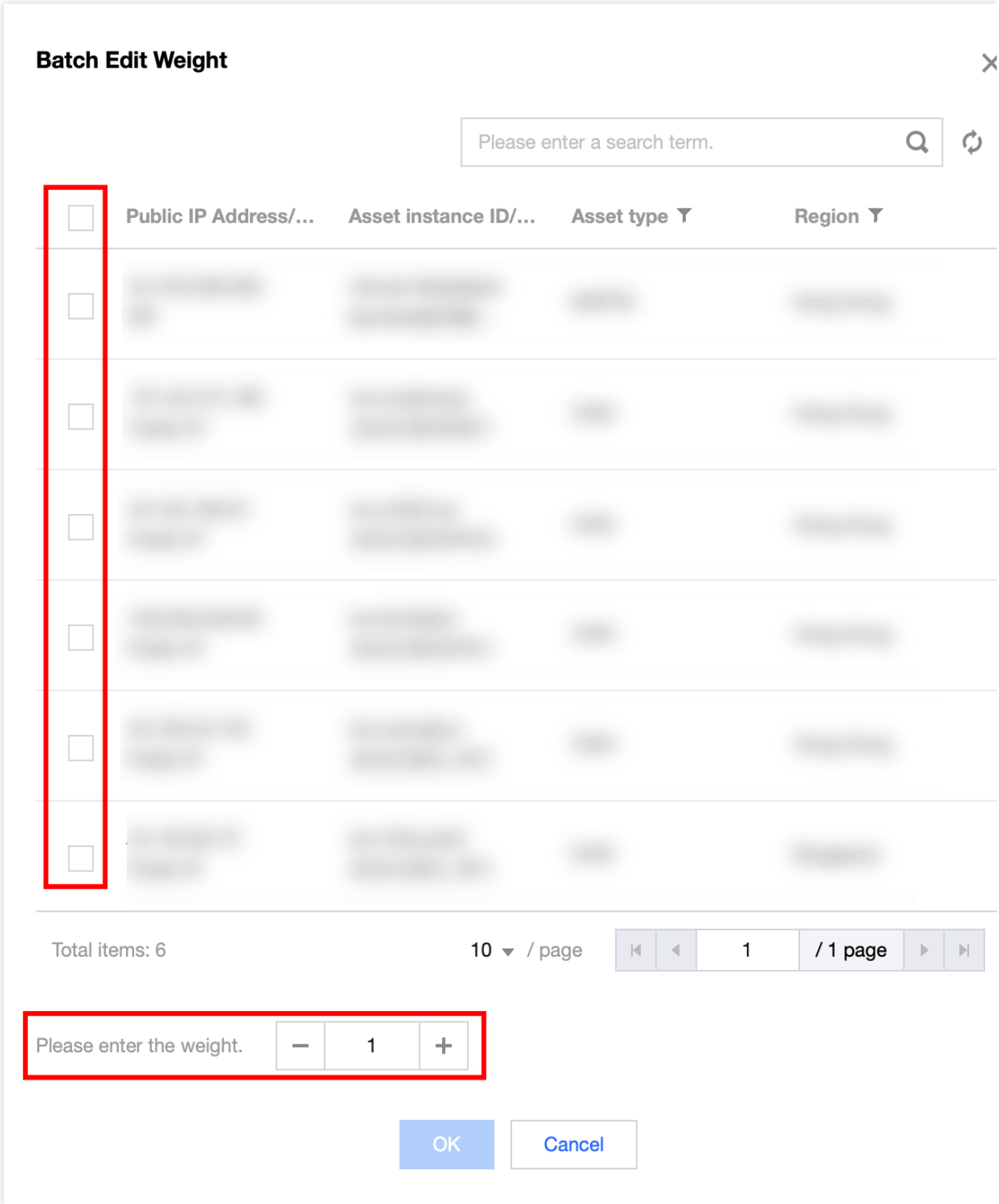
1. Log to the Cloud Firewall Console, and in the left navigation bar, select **Firewall Toggles** > **Edge firewalls**.
2. On the **Firewall Toggles** page, click **Firewall settings**.



3. On the **Firewall settings** page, edit the designated Firewall toggle weight.



4. Click **Edit weight**, you can choose the Firewall toggle, bulk edit switch weight, then click **OK** to save.

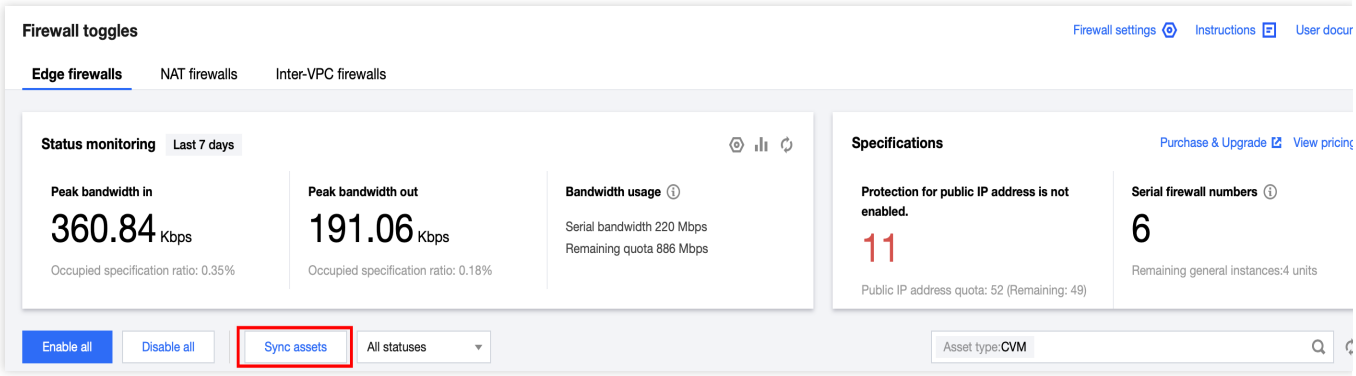


Syncing Assets

The interval for the backend periodically polling user asset information is 5 minutes. Hence, when the user's asset scale changes during this interval and has not been synchronized by the backend, you can go to the top of the list,

click **Sync assets**, to promptly call the backend interface and re-read and synchronize the user's asset information and data.

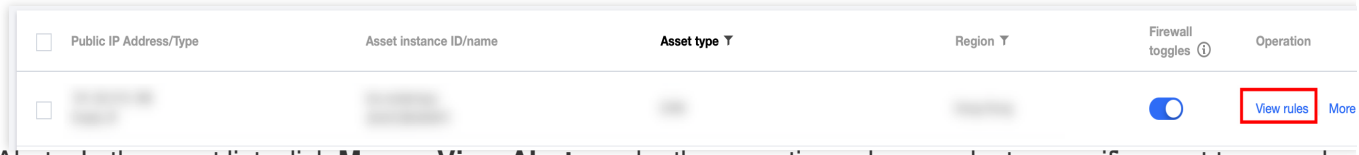
When new assets do not appear in the Firewall Toggles list, you can go to the top of the list, click **Sync assets** to attempt asset synchronization.



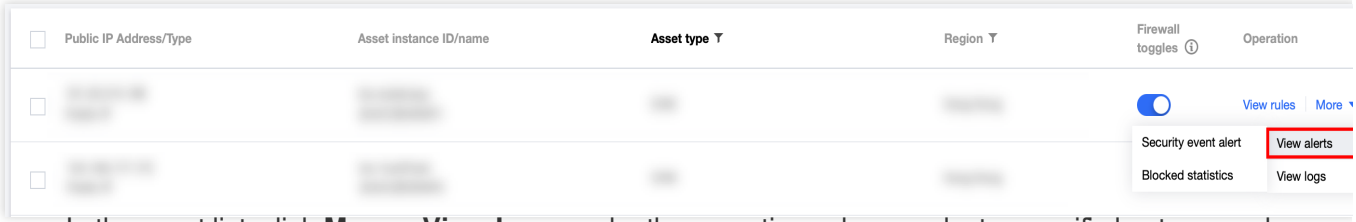
Viewing Rules, Alerts, or Logs

In addition to enabling Firewall Toggles in the asset list, you can perform some other operations, mainly including viewing asset-related rules, alerts, and logs.

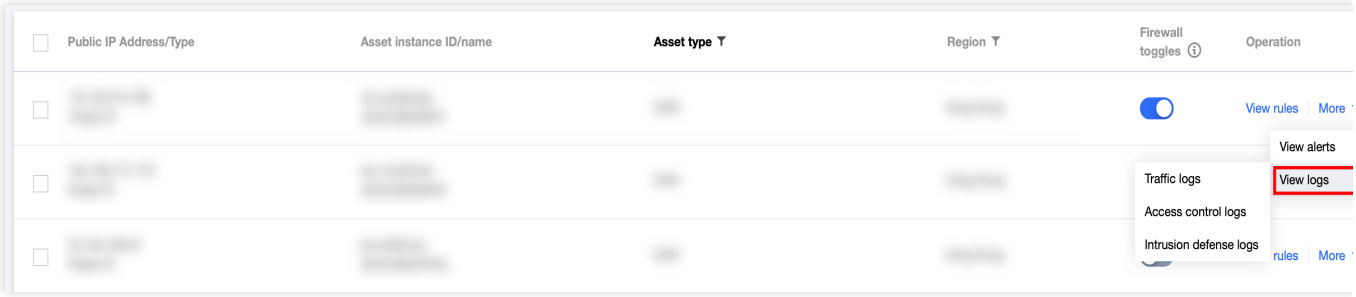
View Rules: In the asset list, click the **View Rules** in the operations column, you will be redirected to the page of rules associated with the asset.



View Alerts: In the asset list, click **More** > **View Alerts** under the operation column, select a specific event type, and you will be redirected to the relevant event page in the alert center.



View Logs: In the asset list, click **More** > **View Logs** under the operation column, select a specific log type, and you will be redirected to the relevant log page.



Business Bandwidth Exceeding Edge Firewall Bandwidth Limit

The business will not be affected if the business bandwidth exceeds the Edge Firewall bandwidth limit. Packet loss or traffic rate decrease will not occur, but the protection feature will be unavailable.
Starting from September 25, 2024, the following measures will be taken when the business bandwidth exceeds 100% of the Edge Firewall bandwidth limit:
Some Edge Firewalls will be disabled, and part of the traffic will be forwarded in bypass mode to protect only traffic within the bandwidth specifications.
The measures are the same for the serial mode. Some firewalls will be disabled to limit the traffic.
Weights can be set to determine the priority for automatically disabling firewalls.

For more details, see Frequently Asked Questions - Bandwidth.

Related Information

If you need to manage traffic and protect assets in the private network, or forward network traffic based on SNAT and DNAT, please refer to the NAT Border Firewall Toggle operation.
If you need to automatically detect VPC information and interconnections, and set a Cloud Firewall toggle for each interconnected pair of VPCs, please refer to the Inter-VPC Firewall Toggle operation.

NAT Firewall Toggle

Last updated：2024-03-18 14:12:58

NAT Firewall Toggle allows you to manage traffic and protect assets in the private network, and forward network traffic based on SNAT and DNAT.

Operation guide

1. Log in to the Cloud Firewall console, and select **Firewall toggle** > **NAT firewall toggle** in the left navigation pane to enter the **NAT firewall toggle** page.

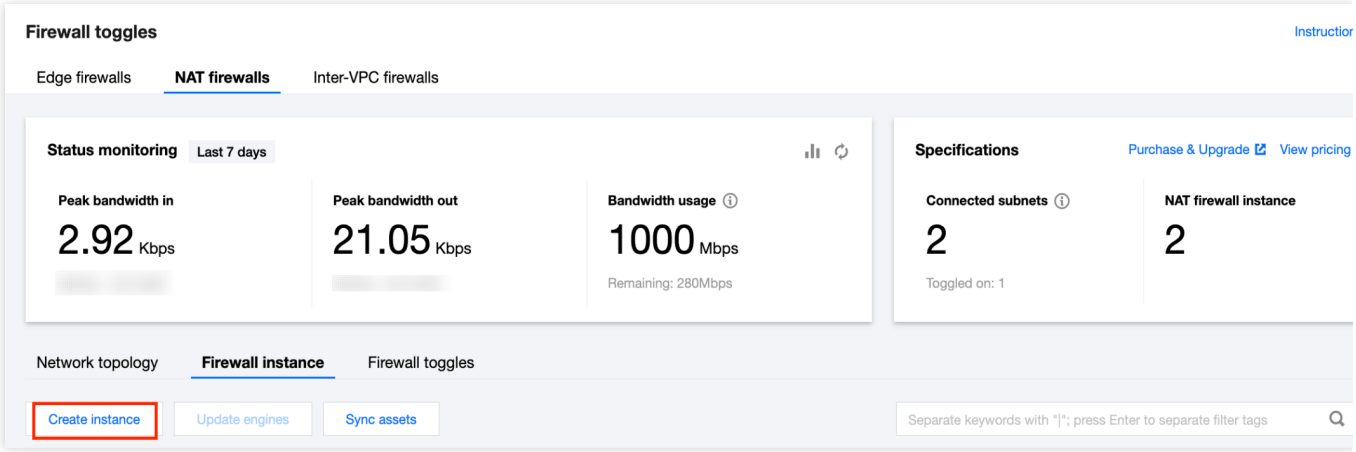
Note

If a NAT firewall toggle is turned on, the Internet traffic of the subnet can go through the firewall. The access control rules and the intrusion defense feature take effect, and the traffic log can be generated.

2. On the **NAT firewall toggle** page, you can create instances, sync assets, and view and monitor the bandwidth of the NAT firewall.

Creating an instance

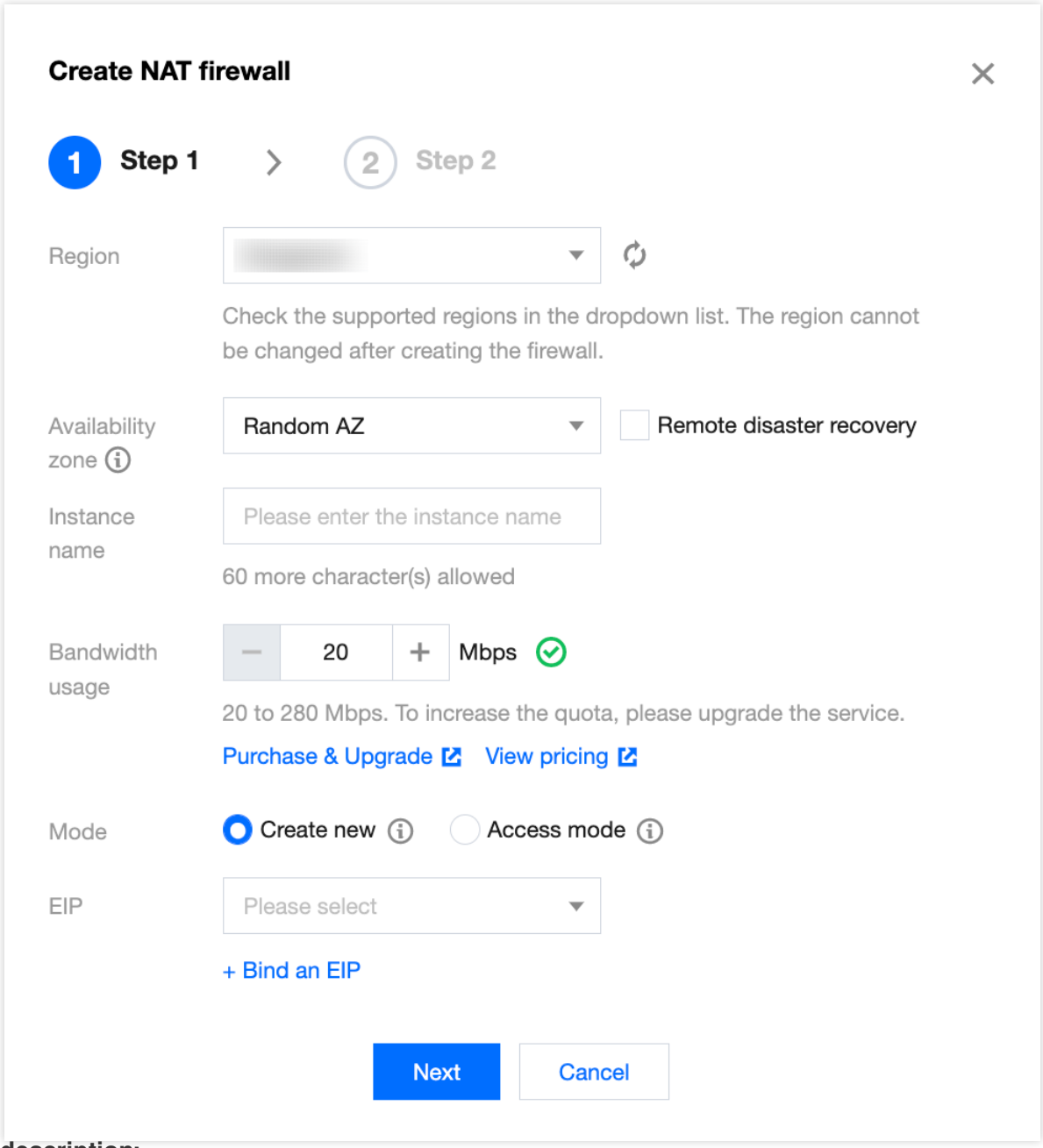
1. On the NAT firewall toggle page, click **Create instance**.



2. In the **Create NAT firewall** dialog box, create a NAT firewall instance for the current account, complete the fields, and click **Next**.

Note

This operation involves lots of backend configuration and needs to take several minutes.



Field description:

Region: Select a region for the instance to be created (all regions in China are available). The region cannot be modified after the instance is created.

Note

You can select one of the regions in China (including Hong Kong) where you have a VPC. Multiple firewall instances can be created for a single region, but the total bandwidth cannot exceed the quota.

Zone: Select an availability zone according to your needs.

Instance name: Enter the name of the instance.

Bandwidth quota: Select a bandwidth quota according to your needs (at least 20 Mbps). For more bandwidth, upgrade your service.

Note

It must match the bandwidth of the edge firewall. For multiple NAT firewalls, their bandwidth sum must be less than or equal to that of the edge firewall.

Mode: Supports the Create new mode and Use existing mode.

Create new: If no NAT gateway is available in the current region, you can create a new NAT gateway and use it as the NAT firewall for Internet access.

Use existing: If a NAT gateway is available in the current region, or you do not want to change your outbound IP address, you can use the Use existing mode to smoothly add a NAT firewall between the NAT gateway and CVM instance.

EIP: If you select to create a new EIP, the system automatically requests an EIP for you. Or you can select and bind one of the idle EIPs.

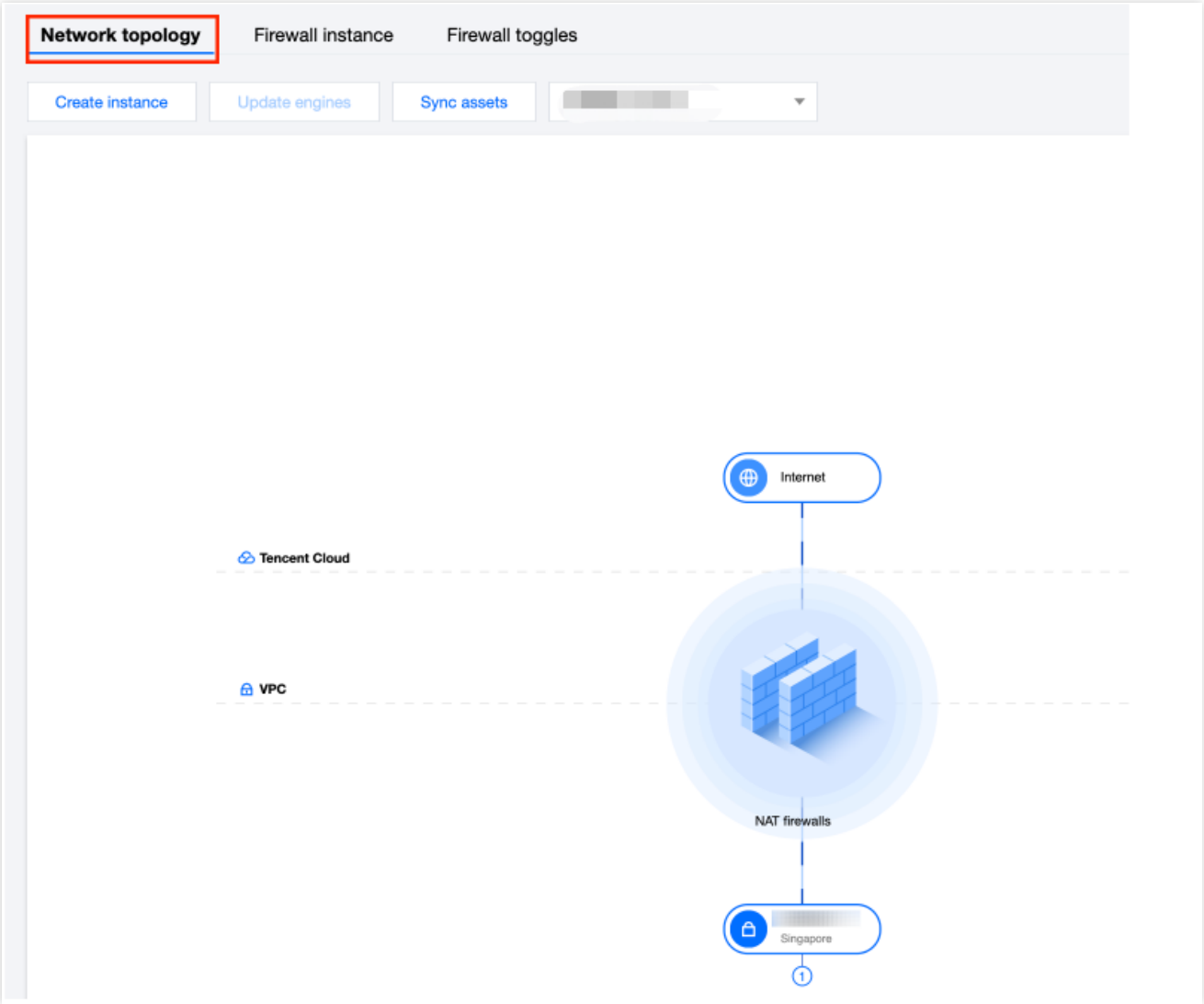
Create instance: After a domain name is created, you can use all the remote operation and database protection services in the current region.

3. Select the VPC or NAT to associate and click **Create**.

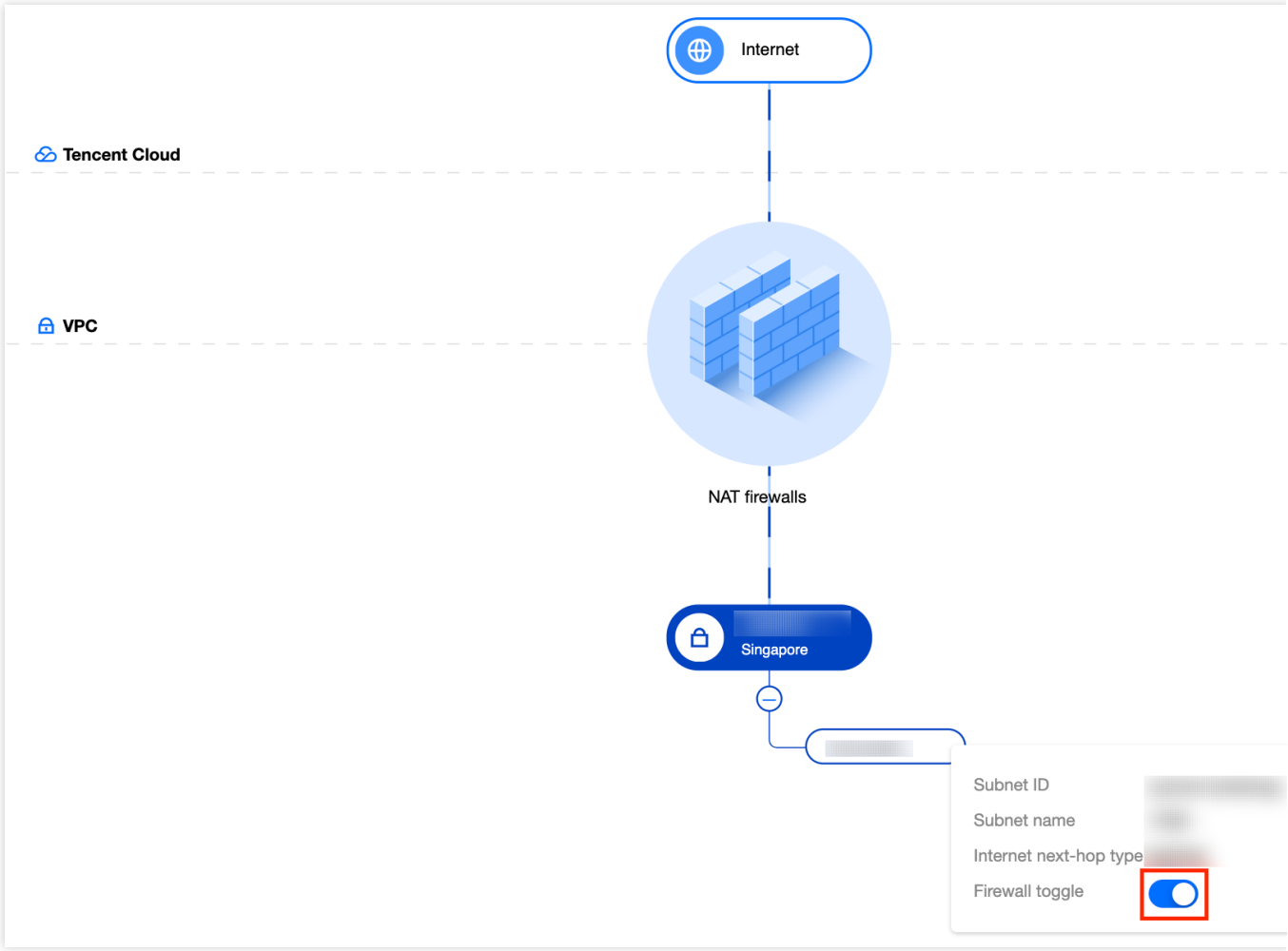
Network topology

Cloud Firewall provides a dashboard displaying the access relation of NAT firewalls. You can check the VPC instances in the VPC.

1. On the NAT firewall toggle page, click **Network topology** to view the access relation of NAT firewalls.



2. Click a VPC node to view subnets. You can turn on or off the firewall toggle only for the current subnet.



Firewall toggle

On the Firewall toggle page, you can enable or disable NAT edge protection. CFW automatically syncs cloud assets on a regular basis, so you don't have to worry about the firewall configuration after an asset change (for example, if a subnet is changed, the firewall will automatically sync in a short period of time).

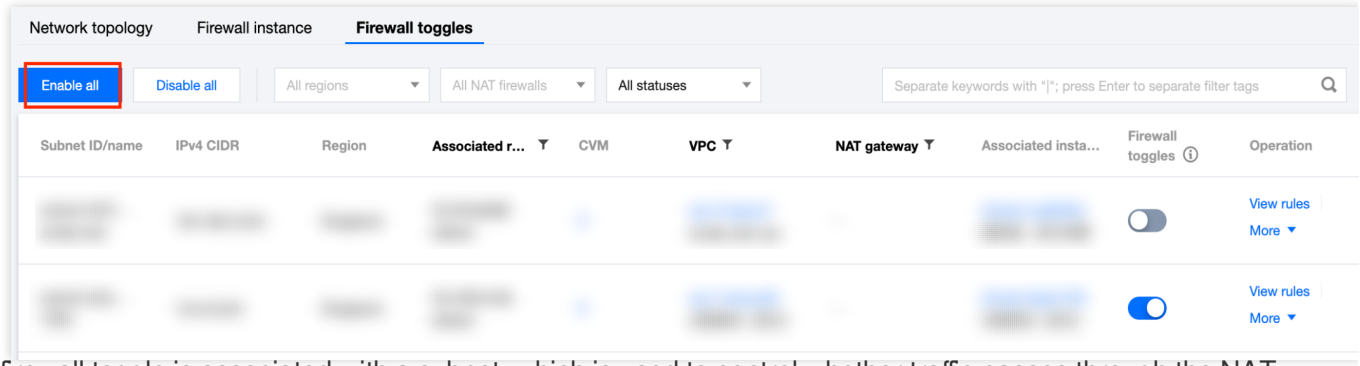
Enable protection:

Above the instance list, click **Enable all**. All NAT firewall toggles are turned on. A routing policy where the next hop points to the NAT firewall is automatically added to all routing tables. The Internet traffic of all subnets will go through the NAT firewall.

Note

When the toggle is on, please do not change the corresponding route manually in the VPC console. Otherwise, the network of your service will be interrupted as the firewall cannot find the route.

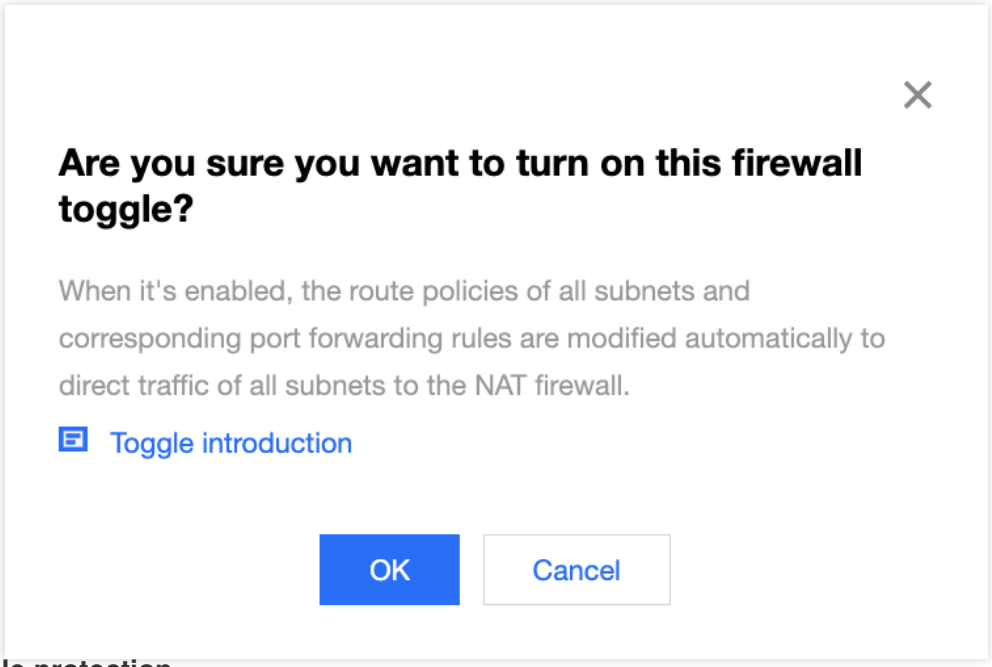
If you enable for all subnets associated with the same routing table, a routing policy is added automatically with the next hop pointed to the NAT firewall. The original routing policy to the Internet are disabled. In this way, all traffic going from the subnet to the Internet must go over the NAT firewall.



Each firewall toggle is associated with a subnet, which is used to control whether traffic passes through the NAT firewall. Subnets associated with the same routing tables will be enabled/disabled at the same time. After the NAT firewall is created, the firewall toggle is on by default to ensure uninterrupted network.

Note

When it's enabled, the routing policies of the subnet routing table and port forwarding rules of the subnet are modified automatically to direct traffic of the subnet to the NAT firewall.

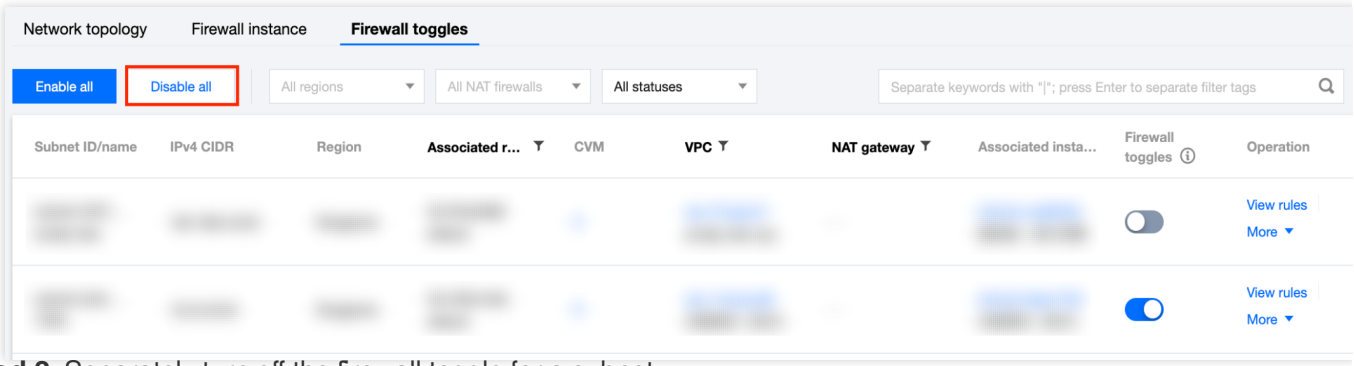


Disable protection

Method 1: Above the instance list, click **Disable all**. All NAT firewall toggles are turned off. All routing policies where the next hop points to the NAT firewall are automatically disabled. All subnets are disconnected from the Internet. You can enable a routing policy in the VPC console.

Note

If you disable for all subnets associated with the same routing table, the routing policy with the next hop pointed to the NAT firewall is disabled automatically. Subnets associated with this routing table are disconnected from the Internet.

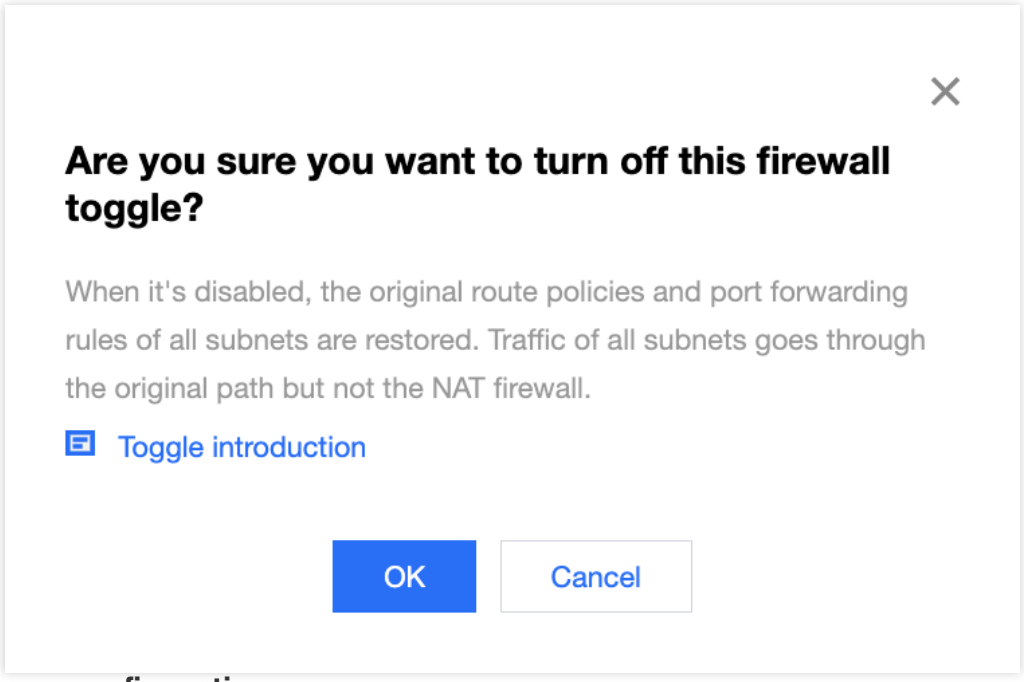


Method 2: Separately turn off the firewall toggle for a subnet.

You can turn off the toggle of the firewall you want to disable in the **Firewall toggle column**. Subnets associated with the same routing table will be disabled at the same time.

Note

When it's disabled, the original routing policies and port forwarding rules of the subnet is restored. Traffic of this subnet goes through the original path but not the NAT firewall.



Instance configuration

On the NAT firewall toggle page, click the **instance ID** or **Instance configuration** on the right side of the firewall instance.

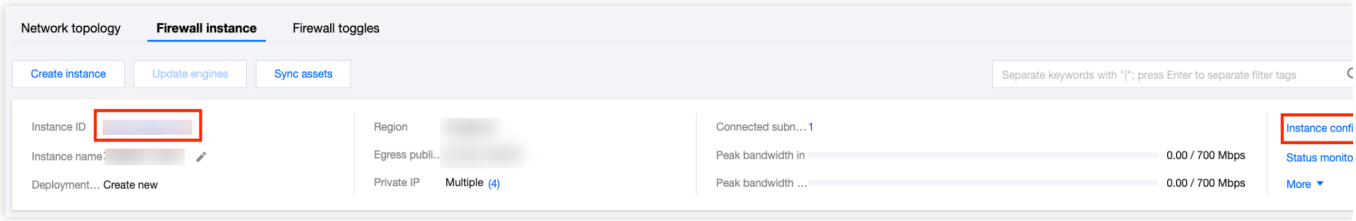
Port forwarding

On the right sidebar, you can view the DNAT port forwarding rules that you added for the NAT firewall instance, and the EIP associated with the instance.

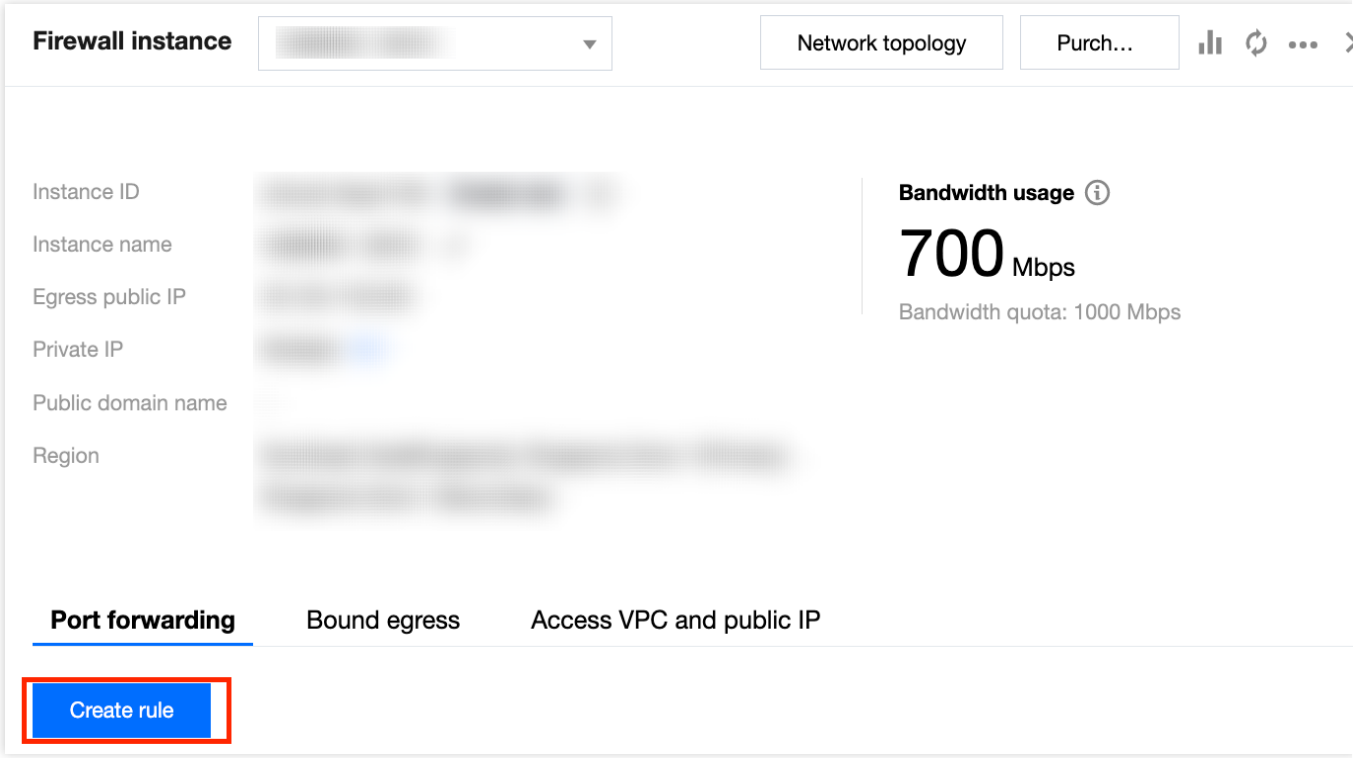
Note

In the **Use existing** mode, the NAT firewall automatically syncs the existing port forwarding rules of NAT gateway to ensure traffic flow. For more operations on the rules, go to the Cloud Firewall console.

When the firewall toggle is on, the SNAT and DNAT traffic of the subnet goes through the firewall. When the firewall toggle is off, the SNAT and DNAT traffic of the subnet goes through the original path.
Do not perform operations on the port forwarding rules in the VPC console. Otherwise, the network may be interrupted.



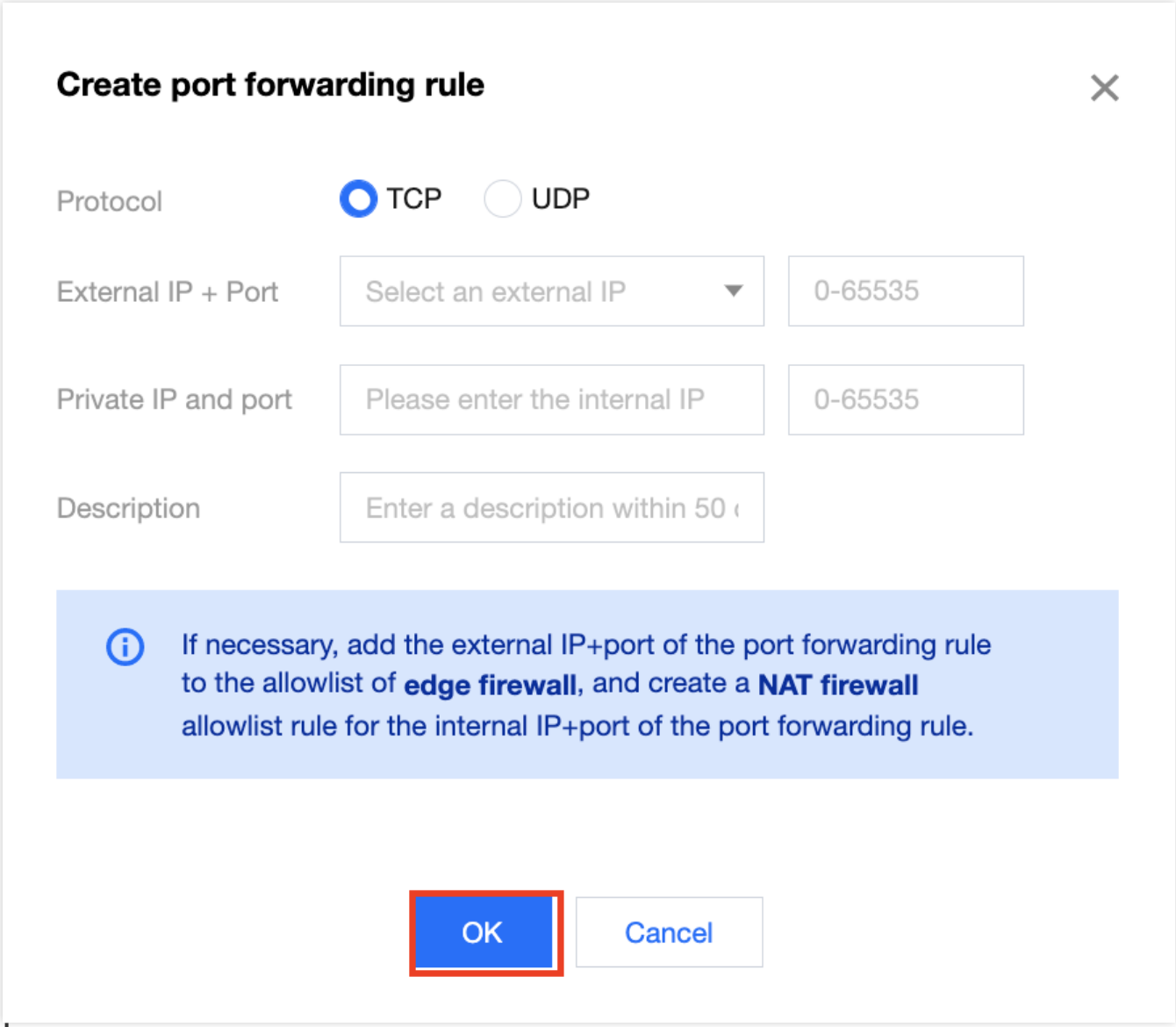
1. On the **Port forwarding** tab of the instance configuration page, click **Create rule**.



2. In the "Create port forwarding rule" dialog box, you can add a DNAT rule for the current NAT firewall instance, with the external IP address being set to the EIP that you bound.

Note

In the **External IP port** drop-down list, the option is the EIP bound to the current NAT firewall instance.
In the "Private IP port", please enter an IP address that is available in the VPC segment of the current region.



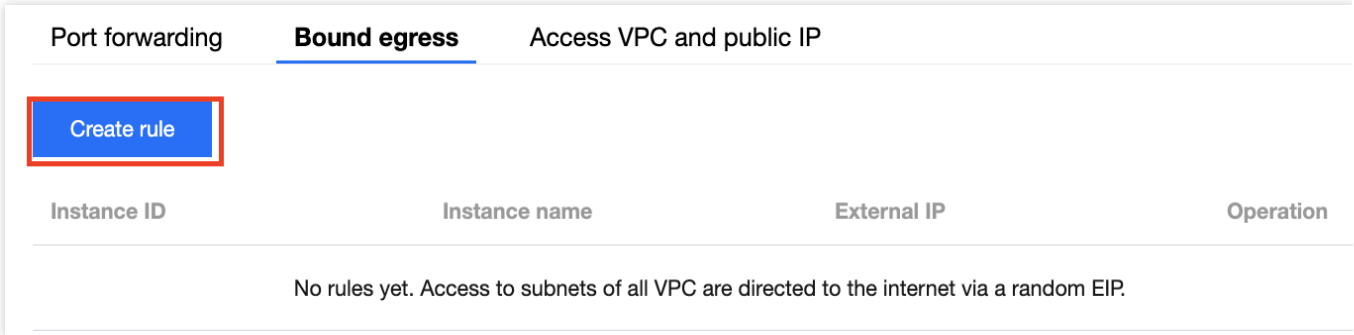
Bound egress

In the **Create new** mode, when the rule list is empty, all VPC subnets will access the Internet via a random NAT gateway.

Note

Bound egress is not supported in the **Use existing** mode.

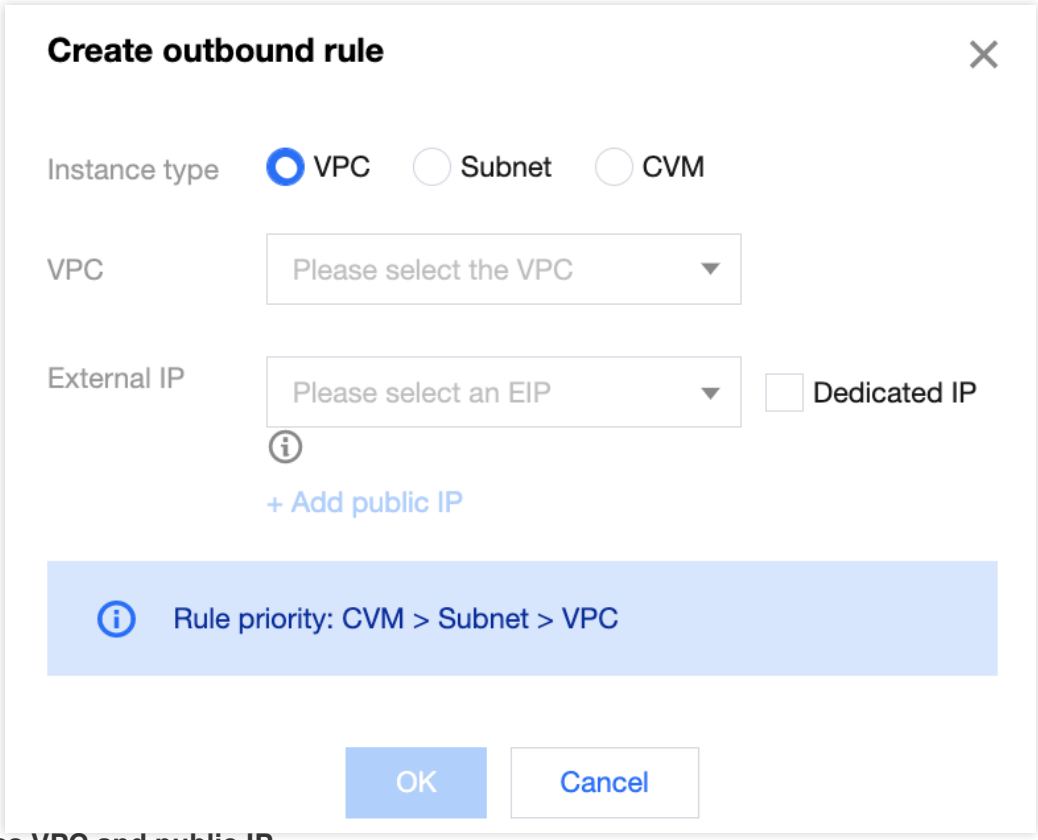
1.1 On the **Bound egress** tab of the instance configuration page, click **Create rule**.



1.2 In the "Create outbound rule" dialog box, provide the firewall instance ID and add a SNAT rule for the current NAT firewall.

Note

You can set **Instance type** to **Subnet** or **VPC**. Then, from the **Subnet** or **VPC** drop-down list, select a subnet or VPC that is connected to the NAT firewall but is not bound to egress NAT rules.

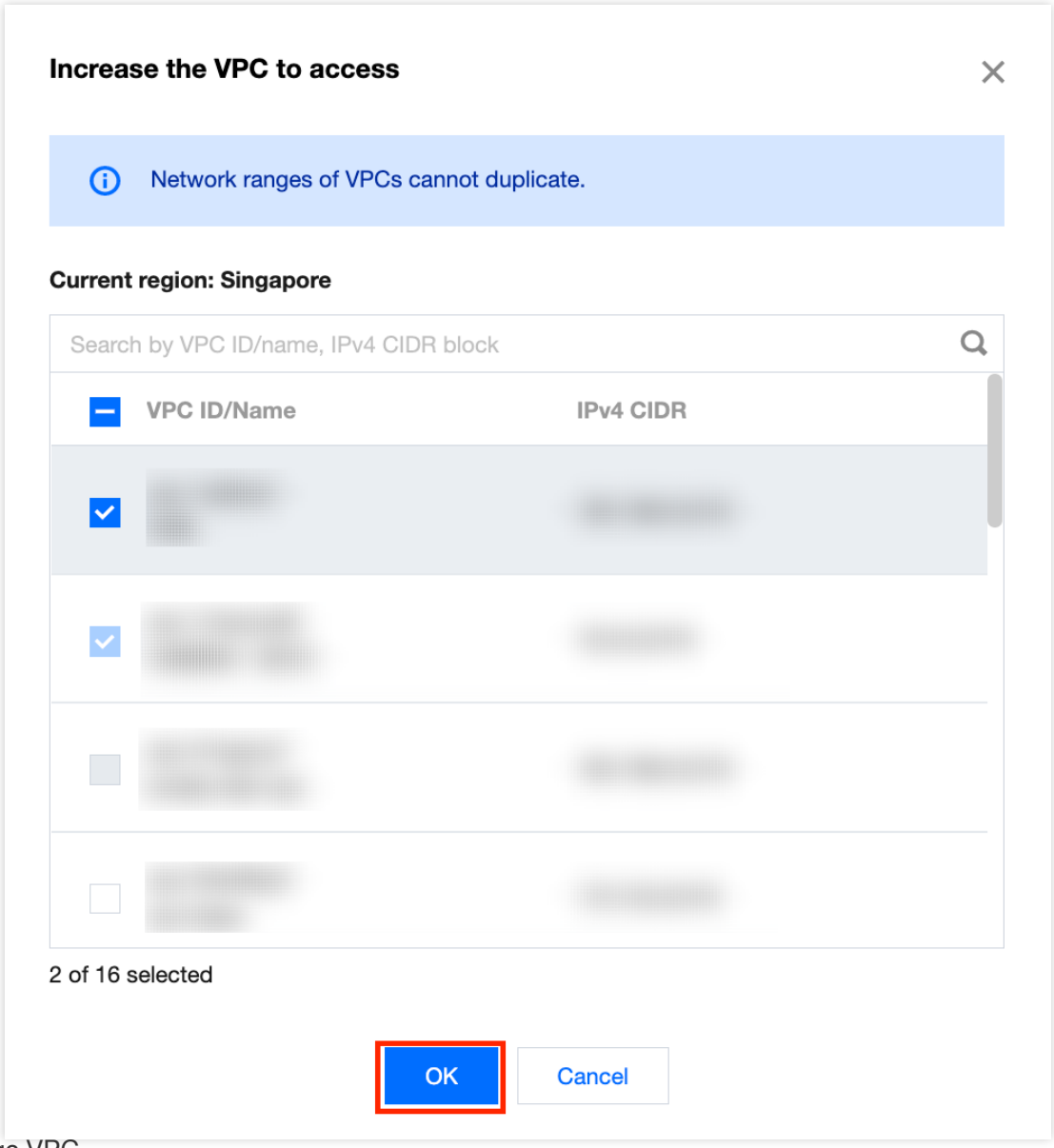


Access VPC and public IP

On the **Access VPC and public IP** tab of the instance configuration page, add a VPC or select another one.

Add VPC

Click **Add VPC**, select the VPC, and click **OK**.

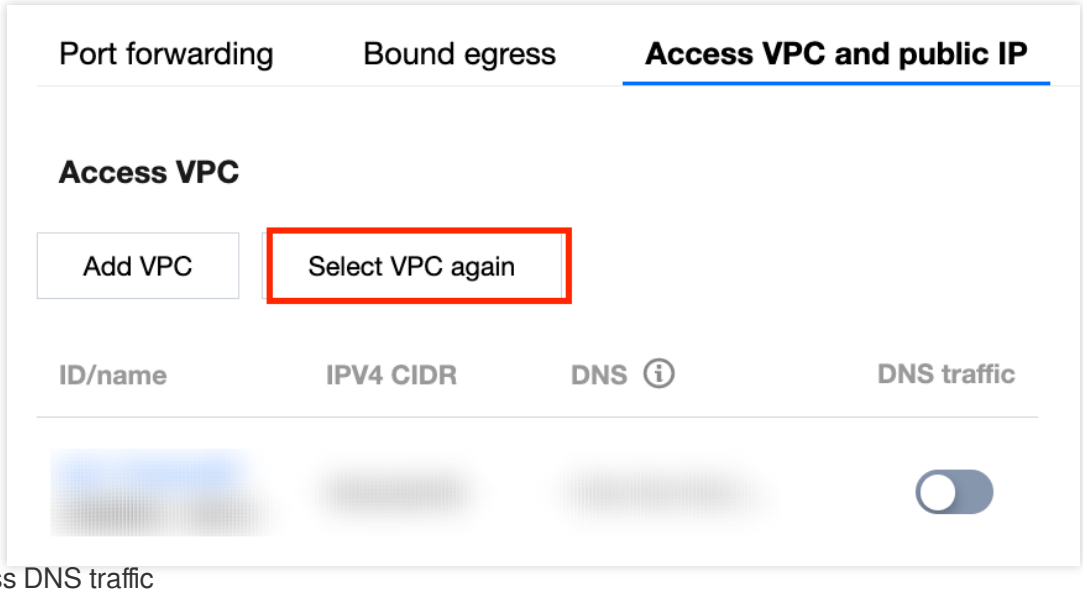


Change VPC

Click **Select VPC again**, select a VPC, and click **OK**.

Note

All subnet toggles and DNS traffic toggles of the current firewall instance must be turned off.



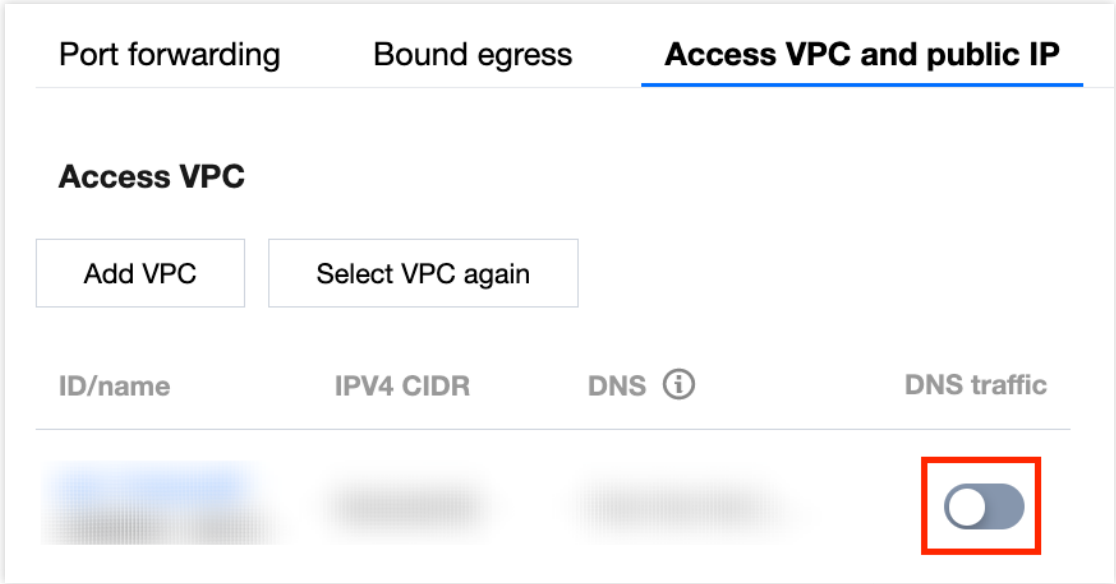
Access DNS traffic

Click the

icon to turn on the DNS traffic toggle on the right side of the VPC. Then, the DNS address of the connected VPC will be changed to direct the DNS traffic to the NAT firewall.

Note

If the connected VPC contains a subnet for which the firewall toggle is off, a significant delay may occur in DNS resolution. It is recommended to turn on all firewall toggles first.



When the DNS traffic toggle is turned off, the original DNS addresses of all VPCs are restored. DNS traffic go through the original path but no the NAT firewall.

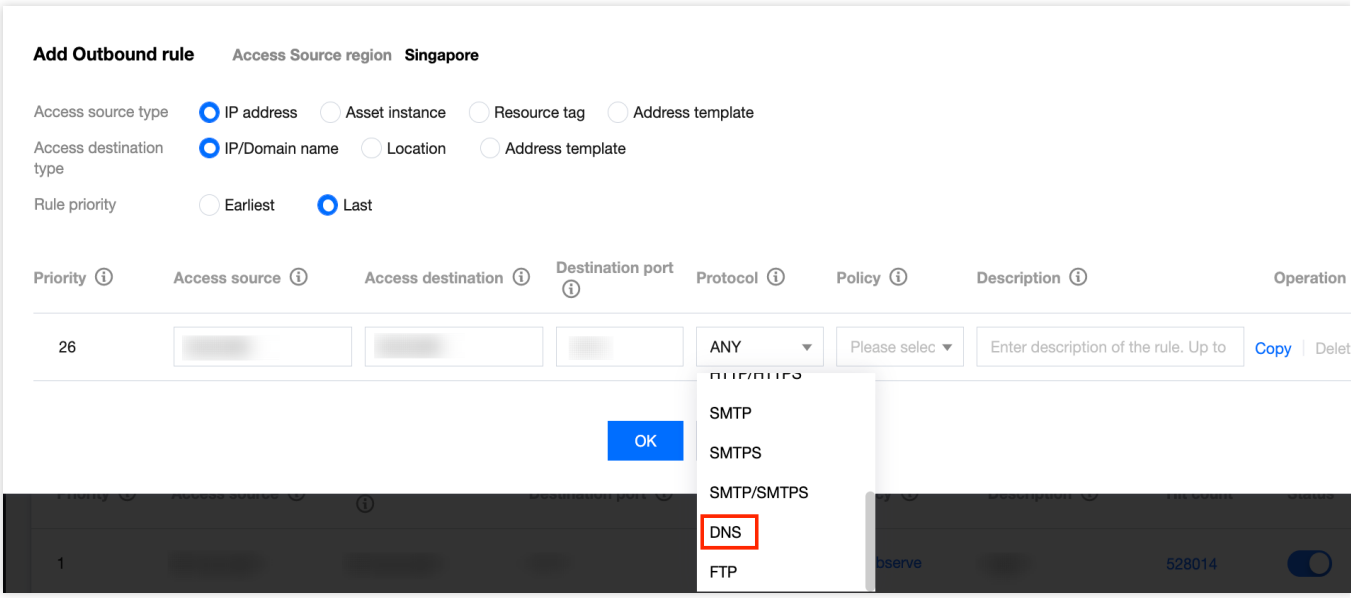
Scenario: The DNS address can be changed to NAT firewall IP to direct DNS traffic to the firewall. The firewall sends the request to a real DNS server and returns the DNS response to the specified server. This feature is supported in

both modes of the NAT firewall.

1.1 On the NAT firewall rules page, click **Outbound rules**.

1.2 On the **Outbound rules** tab, click **Add rule**.

1.3 On the **Add rule** page, complete the fields and select the DNS protocol.



Bind EIP

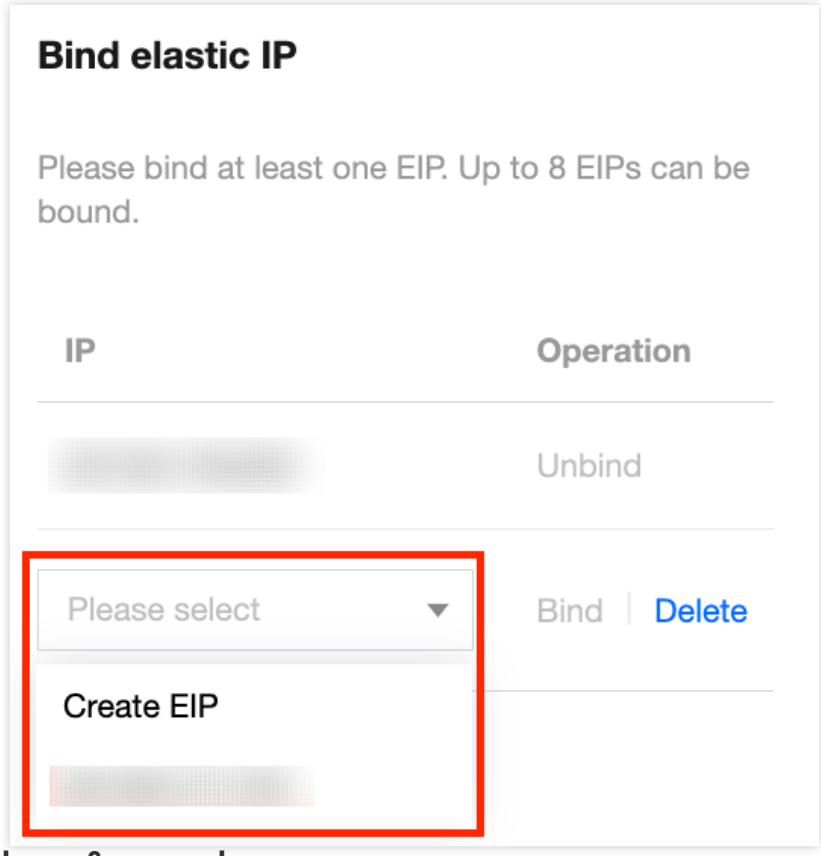
1.1 In the "Bind EIP" module on the right side of the instance configuration page, click **+Bind EIP**.

1.2 In the drop-down list, you can bind the current NAT firewall instance to a new EIP or one of the idle EIPs in the current region.

Note

The EIP binding feature is supported only in the **Create new** mode.

When you unbind an EIP, the DNAT rules associated with the EIP will also be removed.

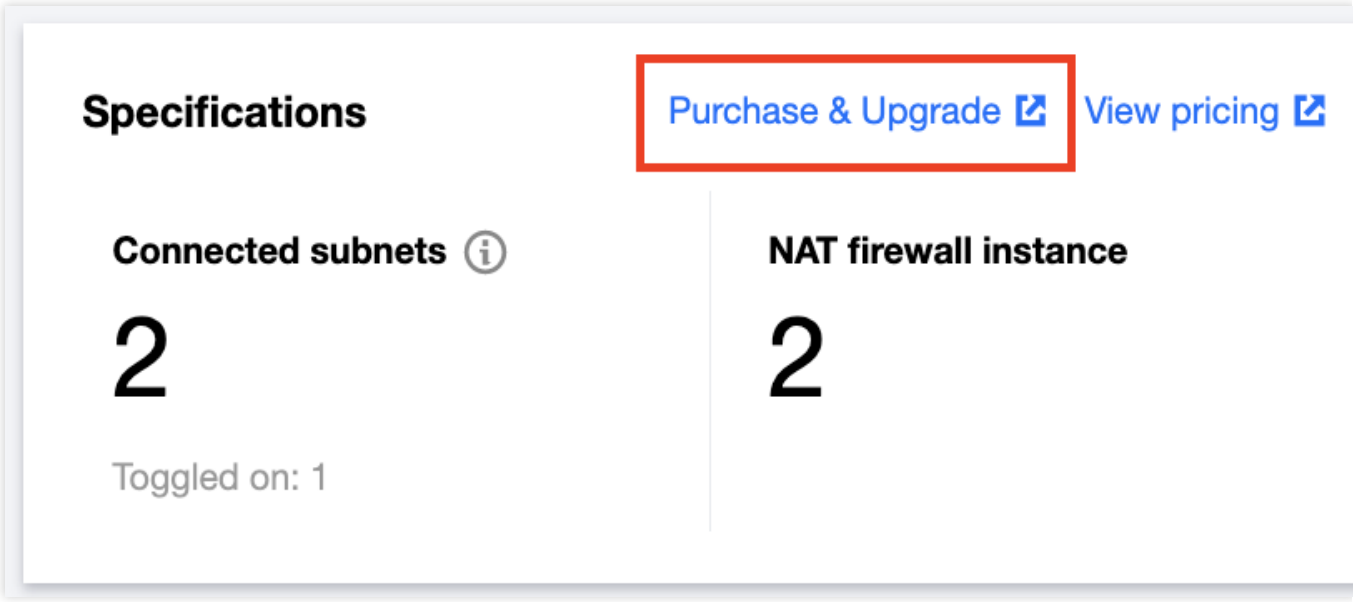


Purchase & upgrade

1. On the NAT firewall toggle page, click **Purchase & upgrade**. On the configuration change page, you can upgrade the bandwidth, version, and log storage.

Note

You can expand the bandwidth (the total firewall bandwidth) only.



2. Upgrade the bandwidth of a single NAT firewall instance by following the steps below:

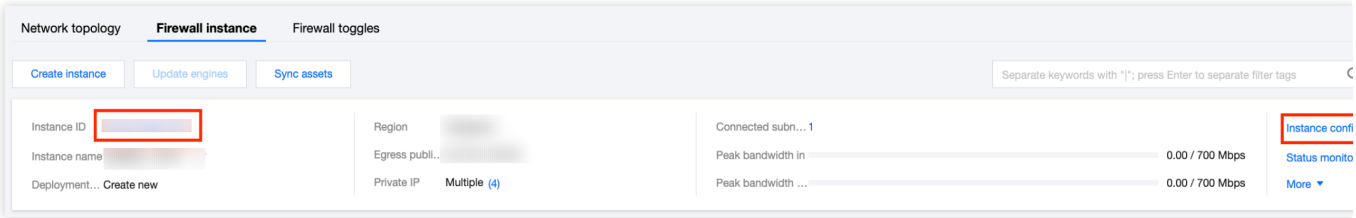
Note

It must match the bandwidth of the edge firewall. For multiple NAT firewalls, their bandwidth sum must be less than or equal to that of the edge firewall.

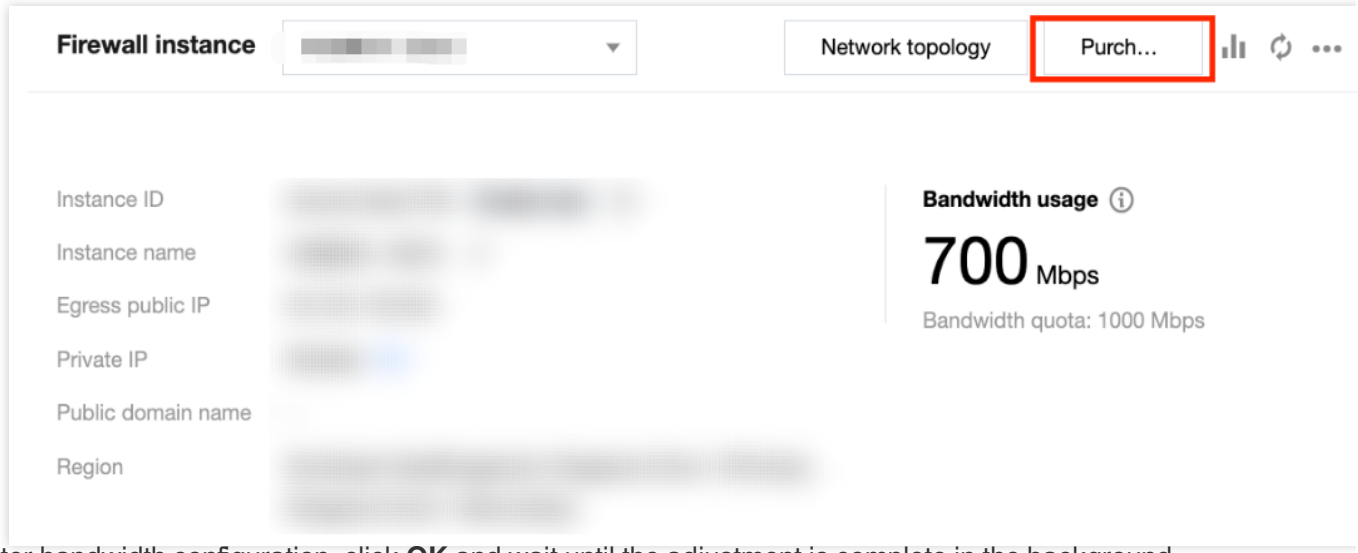
If the target bandwidth is higher than the purchased bandwidth quota, you can click Purchase & upgrade to change the firewall bandwidth.

To make a minor change to the bandwidth, perform in the backend without switching the network. To make a major change to the bandwidth, configure the network first. Otherwise, the service may be interrupted.

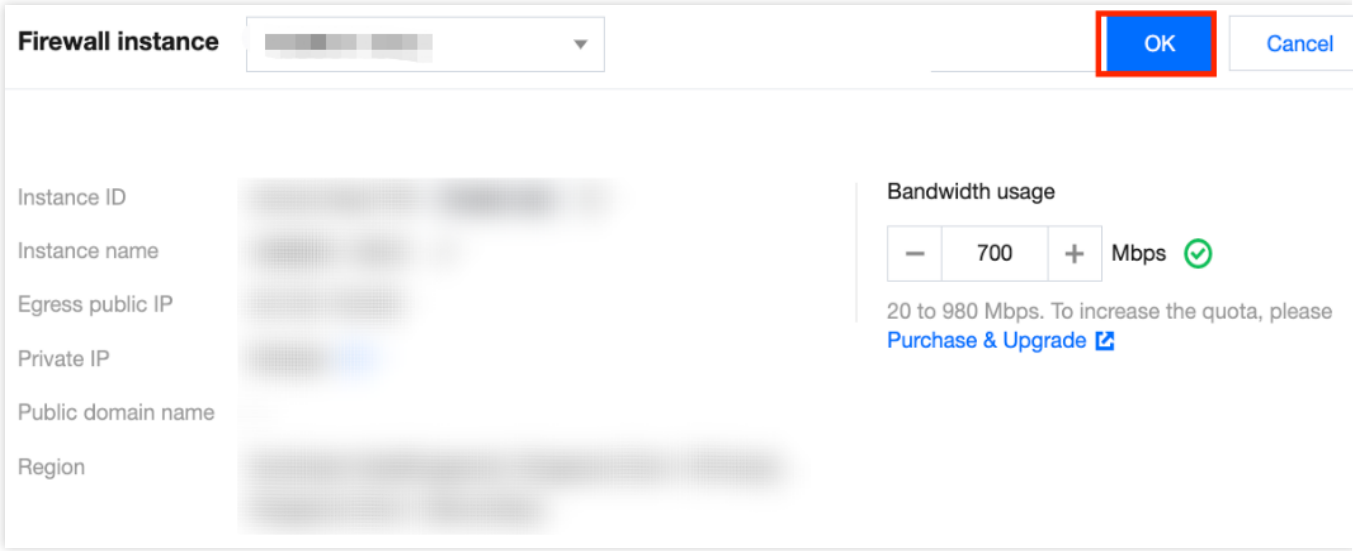
1.1 On the NAT firewall toggle page, click the **Firewall instances** tab. Find the instance for which you want to change the bandwidth, and click the **instance ID** or **Instance Configuration** on the right side of the firewall instance.



1.2 On the **Firewall Instances** tab, click **Purchase & upgrade** in the upper right corner.



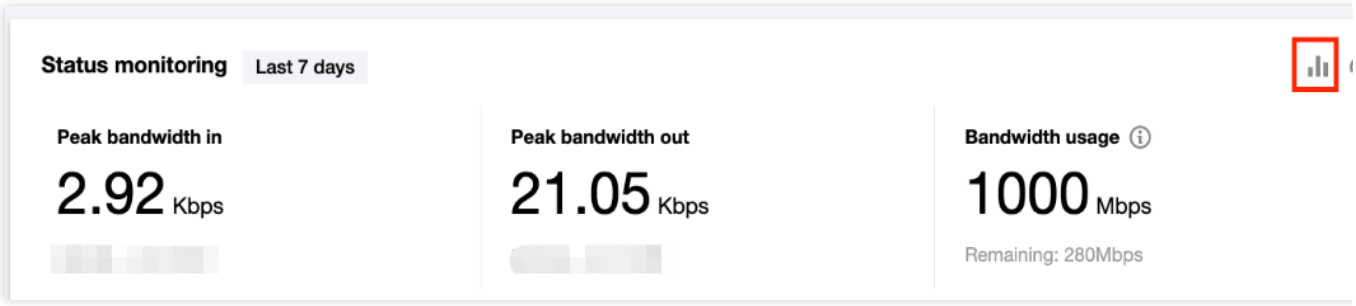
1.3 After bandwidth configuration, click **OK** and wait until the adjustment is complete in the background.



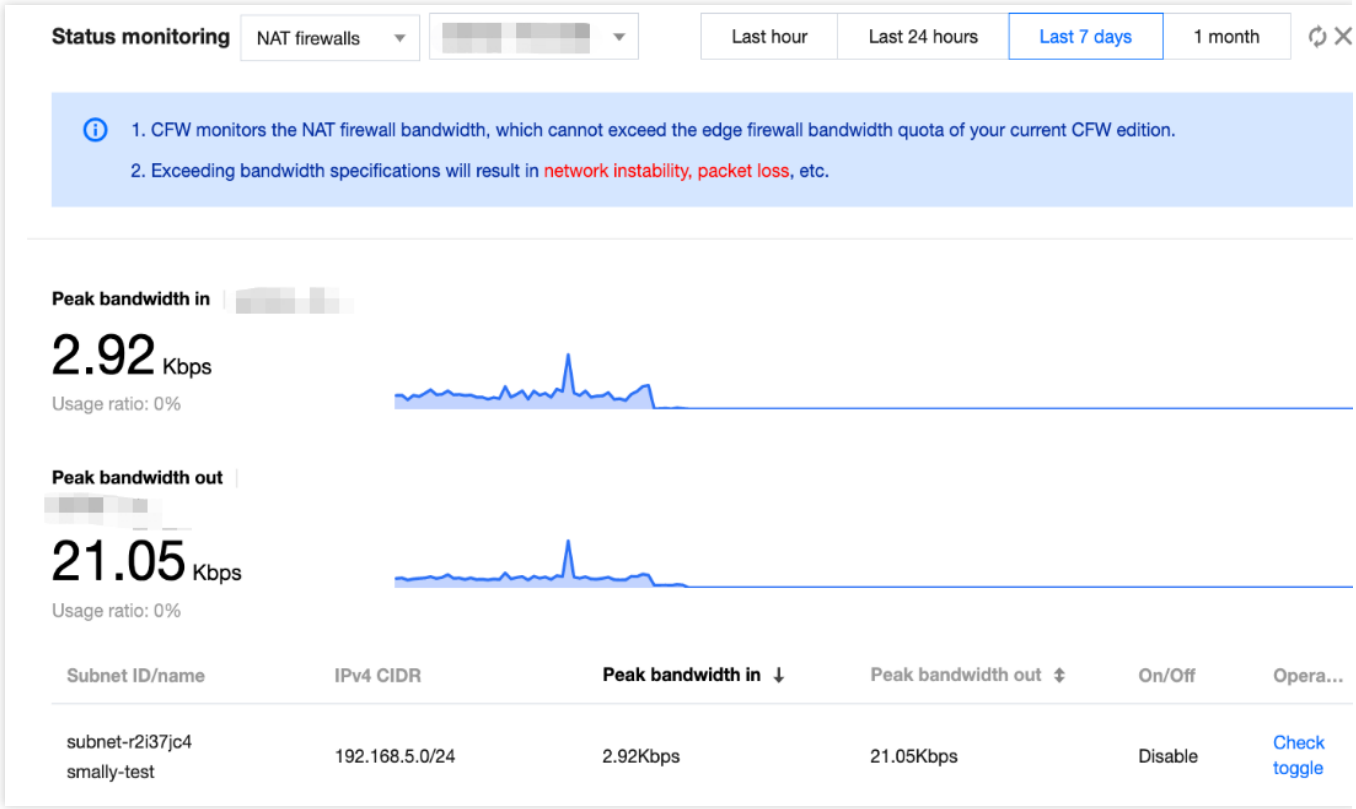
Status monitoring

On the NAT firewall toggle page, you can view and monitor the bandwidths of the NAT firewall, sync assets, and view the network topology.

1. In the upper right corner of the **Status monitoring** area, click the statistics icon. The firewall status monitoring page appears.

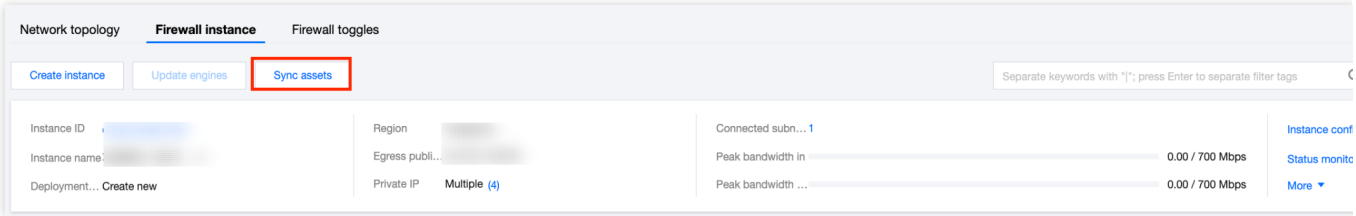


2. On the firewall status monitoring page, you can view and monitor the bandwidths of the NAT firewall. To prevent network packet loss and fluctuation caused by the NAT firewall bandwidth exceeding the quota, you can make adjustments in advance, such as expanding the capacity or turning off some toggles.



Sync assets

On the NAT firewall toggle page, click **Sync assets** to call the backend API to read and sync the asset information of your subnet. This prevents the scenario where the asset scale is changed within the polling interval it the backend but is not synced.

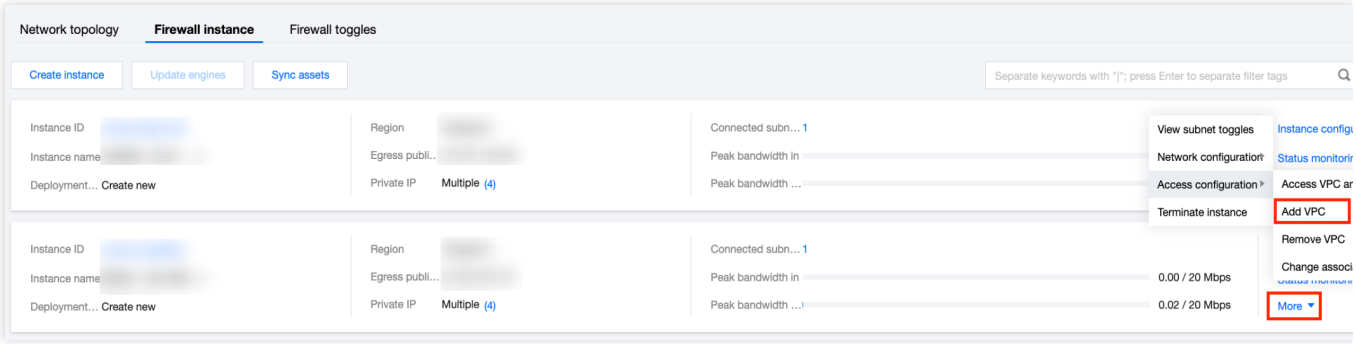


Other operations on VPC and NAT

Add VPC or NAT

Create new:

1.1 On the NAT firewall toggle page, click the **Firewall instances** tab. Click **More** and select **Add VPC** from the drop-down list.



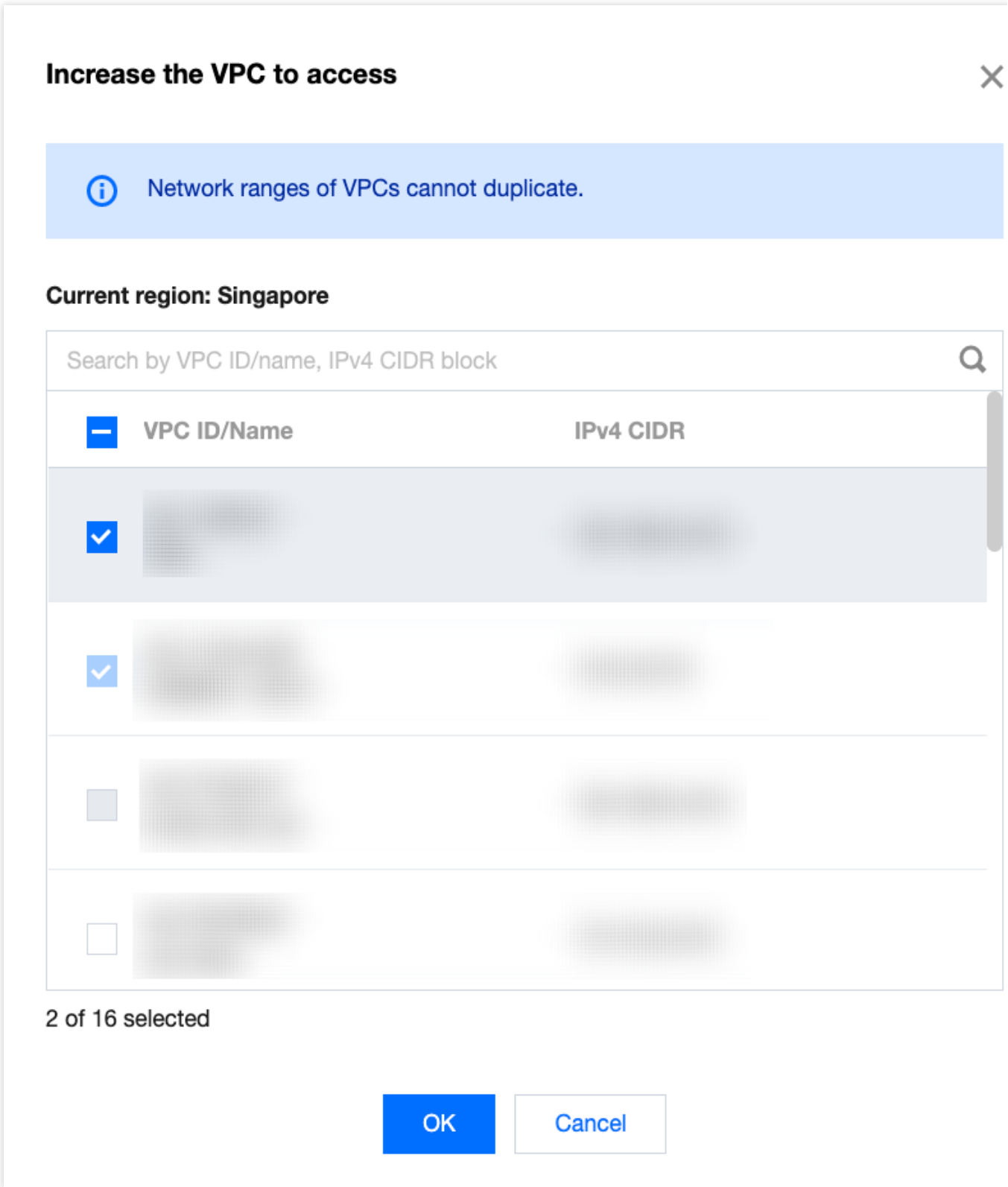
1.2 In the **Add VPC to associate** dialog box, select a VPC, and click **OK**.

Note

You can search for a VPC by keywords, such as a VPC ID, VPC name, and IPv4 CIDR.

Checkbox: The VPCs that you are already connected to are selected by default and cannot be cleared.

After you click **Add VPC to associate**, the NAT firewall toggle of the current region is locked. The toggle will not be unlocked until you click **OK** in the dialog box. When the toggle is locked, if another user in the current region requests to turn on the toggle, a message appears, indicating that a user is re-connecting the VPC.



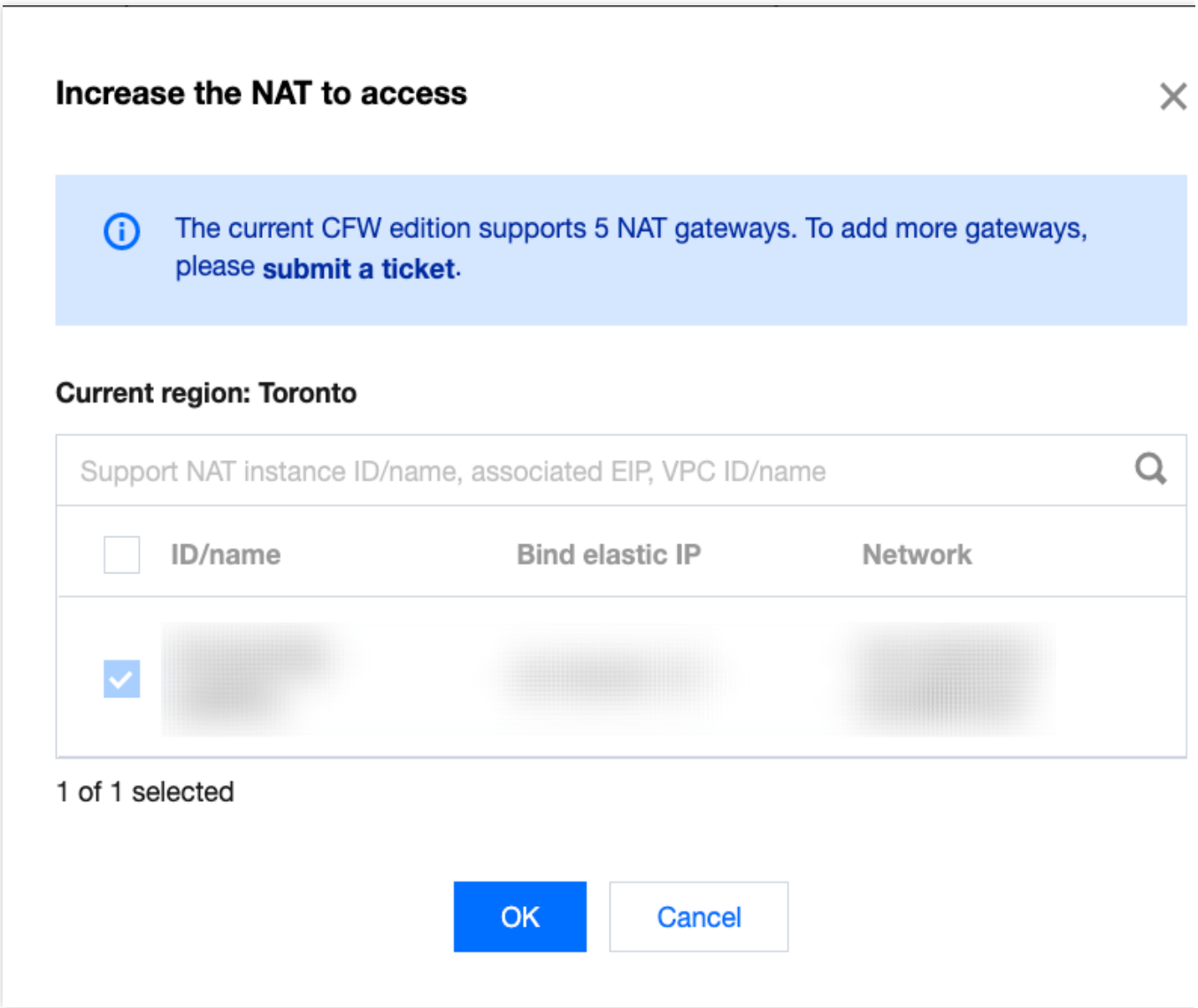
Use existing:

1.1 On the NAT firewall toggle page, click the **Firewall instances** tab. Click **More** and select **Add NAT** from the drop-down list.

1.2 In the **Add NAT to associate** dialog box, select a NAT, and click **OK**.

Note

You can search for a NAT by keywords, such as a NAT instance ID, NAT instance name, bound EIP, VPC ID, and VPC name.
Checkbox: The NAT gateways that are already connected to the current NAT firewall instance are selected by default and cannot be cleared.



Change VPC or NAT

Create new:

1.1 On the NAT firewall toggle page, click the **Firewall instances** tab. Click **More** and select **Select VPC again** from the drop-down list.

Note

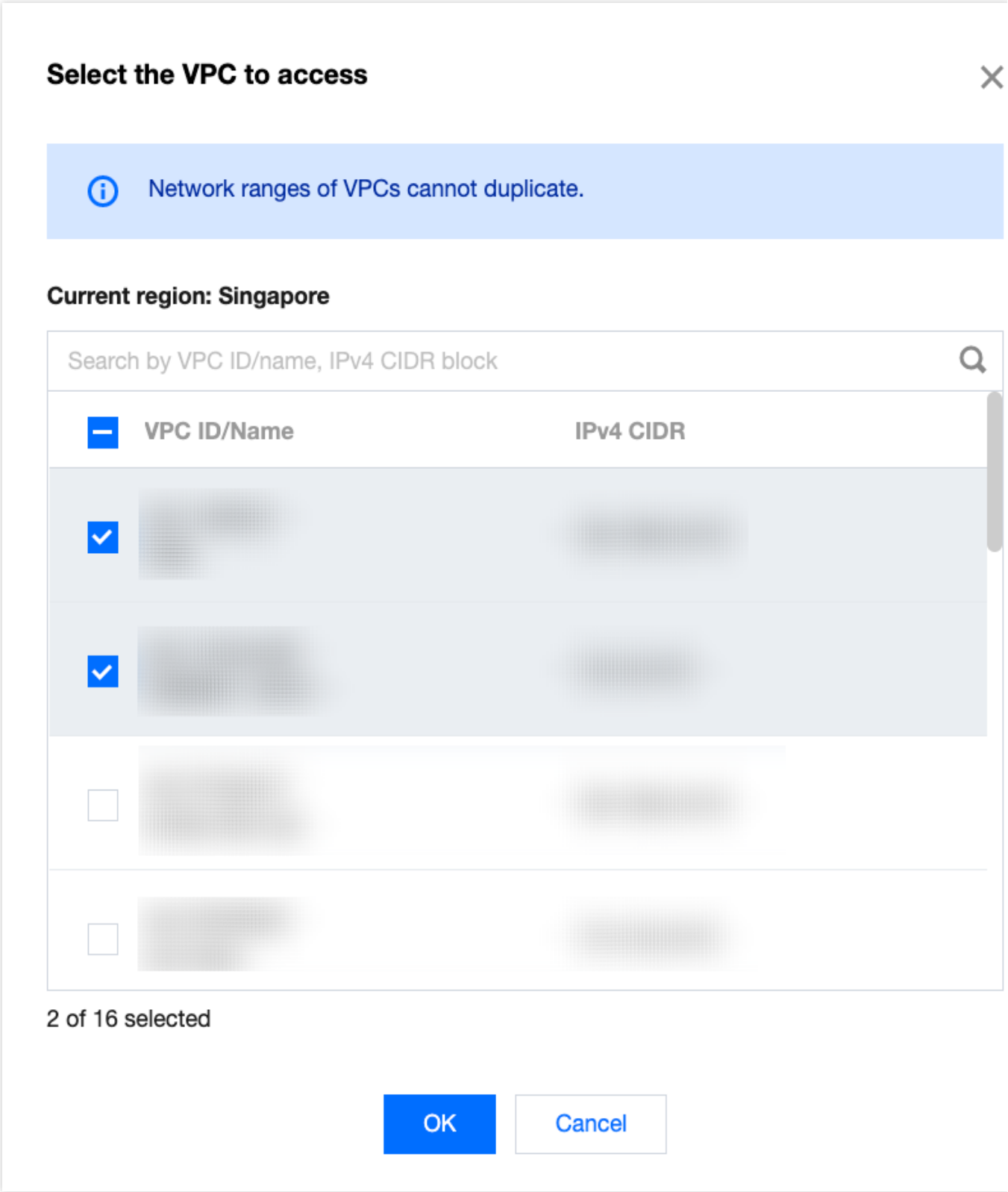
Before you change a VPC, make sure that all the toggles are turned off.

1.2 In the **Select VPCs to associate** dialog box, you can view all available VPCs in the current region. Select a VPC that you want to associate, and click **OK**.

Note

You can search for a VPC by keywords, such as a VPC ID, VPC name, and IPv4 CIDR.

Checkbox: The VPCs that you are already connected to are selected by default and cannot be cleared.

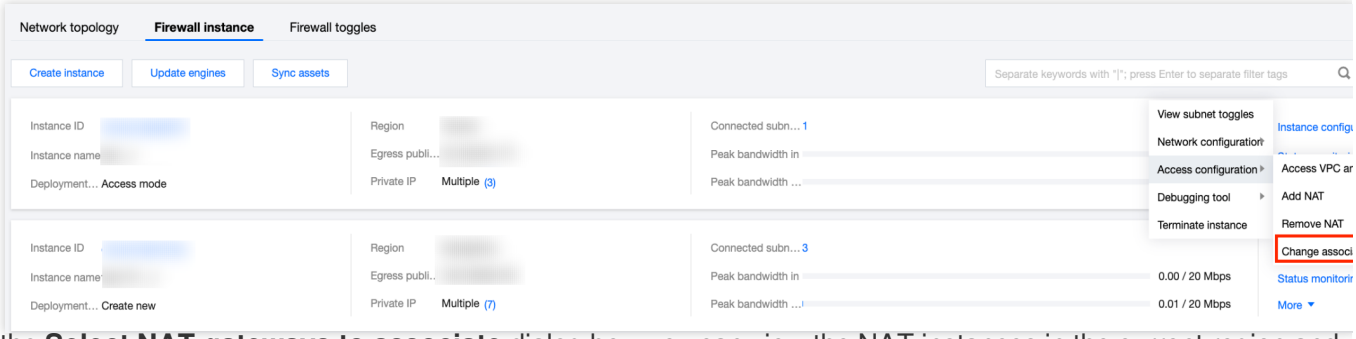


Use existing

1.1 On the NAT firewall toggle page, click the **Firewall instances** tab. Click **More** and select **Change NAT** from the drop-down list.

Note

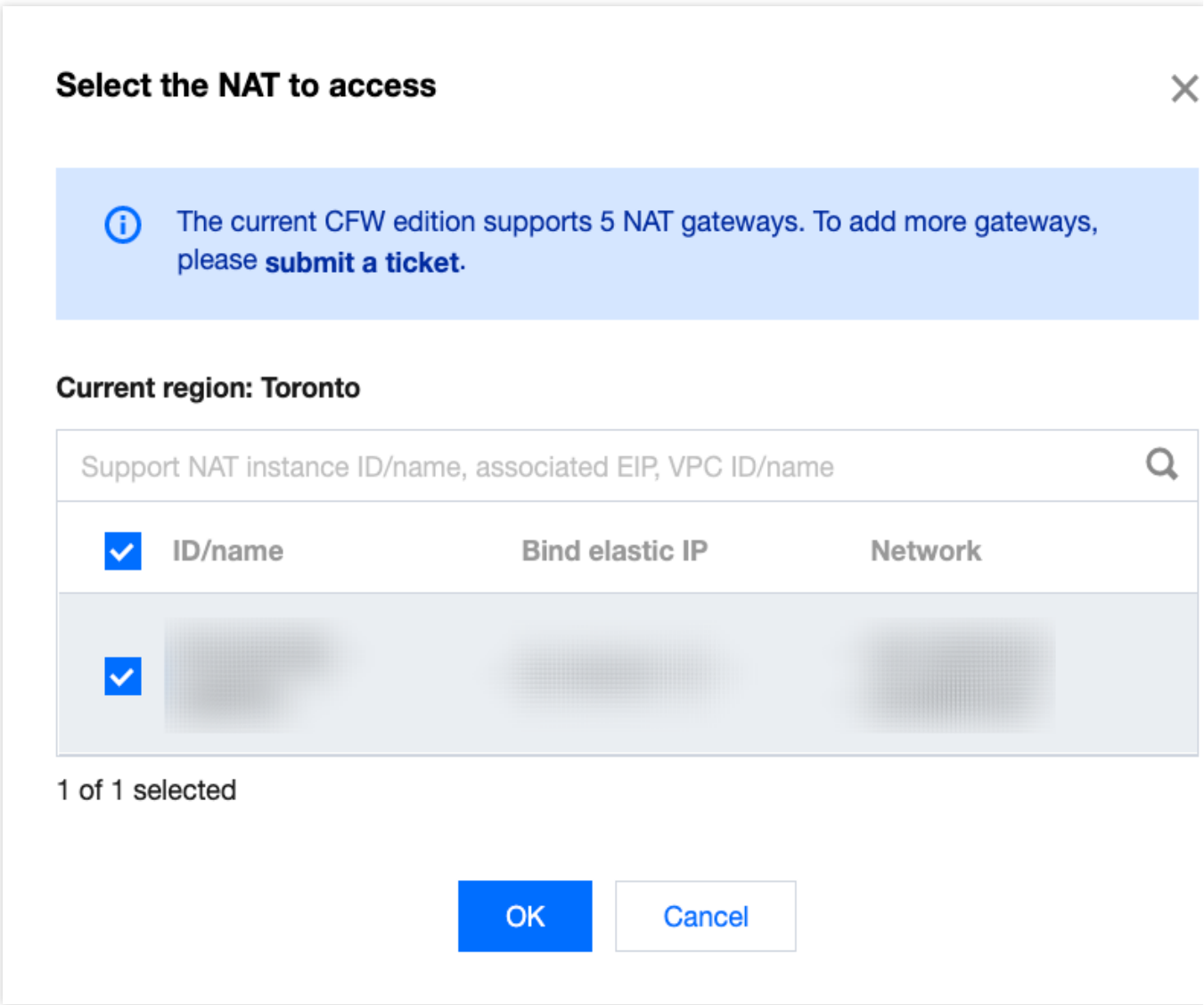
Before you change a NAT, make sure that all the toggles are turned off.



1.2 In the **Select NAT gateways to associate** dialog box, you can view the NAT instances in the current region and select an NAT instance that you want to associate.

Note

After you click **Add NAT to associate**, the NAT firewall toggle of the current region is locked. The toggle will not be unlocked until you click **OK** in the dialog box. When the toggle is locked, if another user in the current region requests to turn on the toggle, a message appears, indicating that a user is re-connecting the NAT.



Terminating an instance

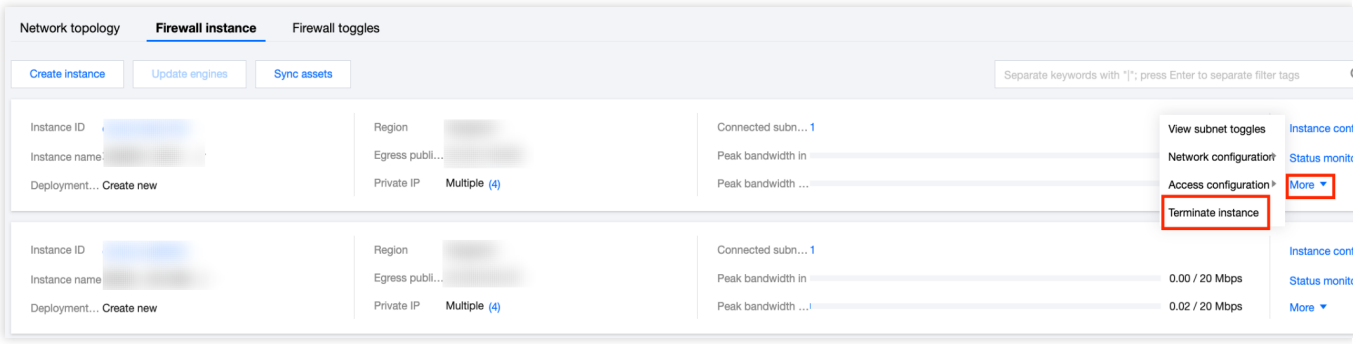
1. On the NAT firewall toggle page, click the **Firewall instances** tab. Click **More** and select **Terminate instance** from the drop-down list.

Note

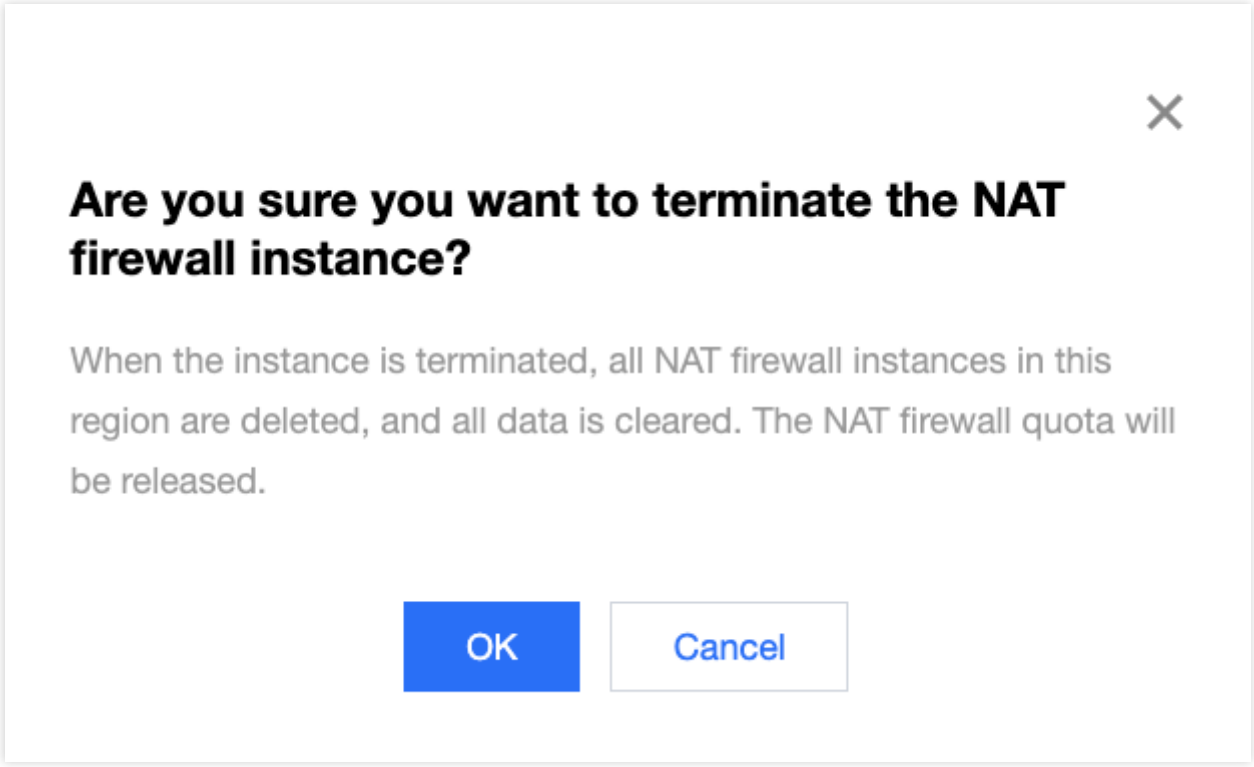
Before you terminate an instance, make sure that all firewall toggles are turned off.

You can terminate any instances as needed.

After the instance is terminated, all the configurations of the instance are deleted, but the log is retained. The quota is returned and the original route and port forwarding are automatically restored. Only the instances in other regions are displayed. If no instances exist in other regions, you will be redirected to the **Create instance** page.



2. In the confirmation window displayed, click **OK** to delete all configurations of this instance.



More information

For more information about how to configure firewall toggles for your public IPs and the associated cloud assets that you own.

For more information about how to automatically detect VPC information and connections and set a Cloud Firewall toggle for each pair of connected VPCs, please see Inter-VPC Firewall Toggle.

For more information about how to access the server via an external IP address, please see Adjusting the Priorities of NAT Gateways and EIPs.

For questions about the NAT firewall, please see NAT Firewall.

Inter-VPC Firewall Toggles Overview

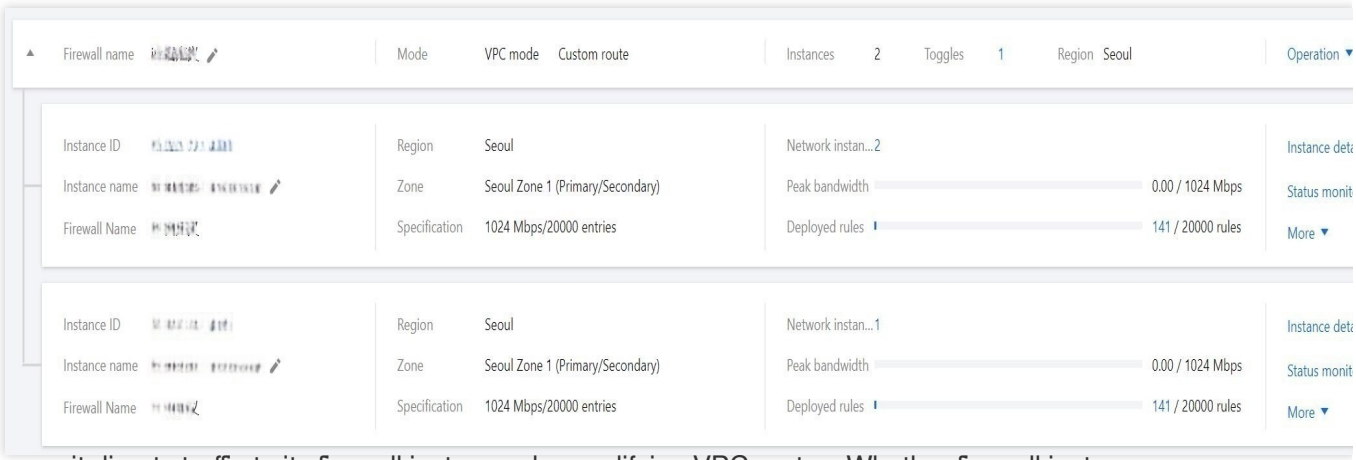
Last updated：2023-11-28 20:33:04

Features

Cloud Firewall allows you to enable or disable the firewall toggle between VPCs. You can create a firewall instance to carry the access traffic between different VPCs. In addition, Cloud Firewall provides access control rules and a log auditing system.
The inter-VPC firewall in the current version can protect Direct Connect gateways. The firewall instance supports multi-level routing provided by Cloud Connect Network (CCN). The Direct Connect gateways connect to the cloud-based VPC assets via CCN. This way, the inter-VPC firewall can detect the traffic in the connections.
This document describes how to create a firewall instance and view its bandwidth usage, specification, network topologies, and firewall toggles on the **Inter-VPC Firewall Toggles** page.

Architecture

Before using this feature, make sure that you understand the components of an inter-VPC firewall.
An inter-VPC firewall comprises multiple firewall instances. Each firewall instance connects a VPC to the firewall.



In essence, it directs traffic to its firewall instances by modifying VPC routes. Whether firewall instances can communicate with each other depends on the reachability of the routes in VPCs, as the firewall instances cannot establish basic networking. However, this can be implemented by modifying the next hop in a VPC route table or multi-route table in CCN.

Handling Abnormal Scenarios

When an inter-VPC firewall is turned on or off, the routing policy changes accordingly, triggering **short network interruptions**. If you need to perform batch or frequent operations on the firewall toggles, it is better to operate at late night.

Notes

Such problem does not occur to edge firewall toggles.

The inter-VPC firewall toggle is on top of the peering connection between VPCs or CCN. If you change or delete the configurations of the peering connection or CCN, the firewall toggle will also be automatically changed or deleted. In order not to affect your business, Cloud Firewall can immediately change or delete only the toggles that are off.

Notes

When the associated Tencent Cloud asset is changed or deleted, the edge firewall toggle will be synced as well within 5 minutes.

If there is no working route between the two VPCs, the firewall cannot be enabled.

Notes

To configure peering connections, see Configuring the Route to Peering Connection. To configure CNN routes, see Route Overview.

When the Cloud Firewall toggle is on, **DO NOT change the associated VPC route tables manually in the VPC console**. This can invalidate the firewall and disconnect the network as the changes to the route tables are not synced to the Cloud Firewall.

When the Cloud Firewall toggle is off, you can change the route of a peer connection or CCN instance. **Please DO NOT enable the route marked with "Firewall"**. This can invalidate the firewall and disconnect the network.

See Also

For more information about configuring firewall toggles for your public IPs and associated cloud assets, see Edge Firewall Toggle.

For more information about managing traffic and protecting assets in the private network or forwarding network traffic based on SNAT and DNAT, see NAT Edge Firewall Toggle.

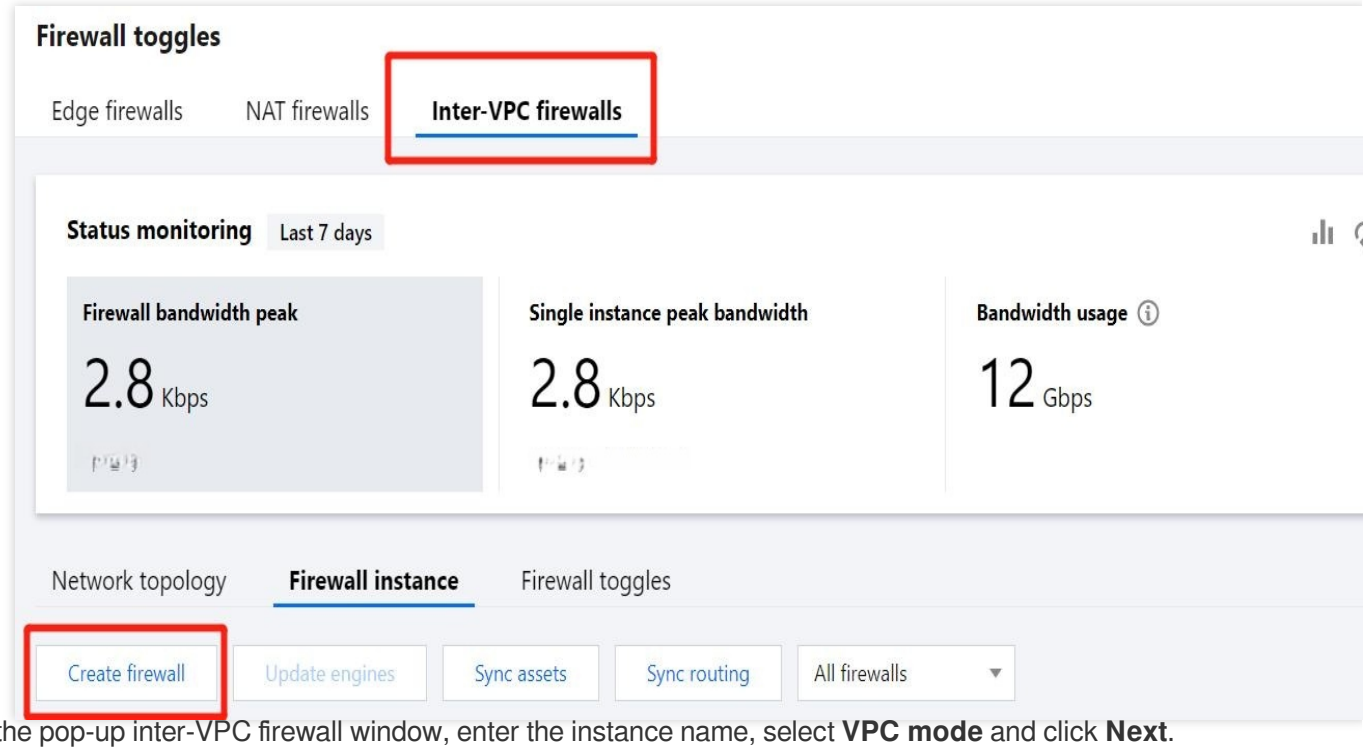
For more information about the inter-VPC firewall, see Inter-VPC Firewall.

Creating Inter-VPC Firewalls

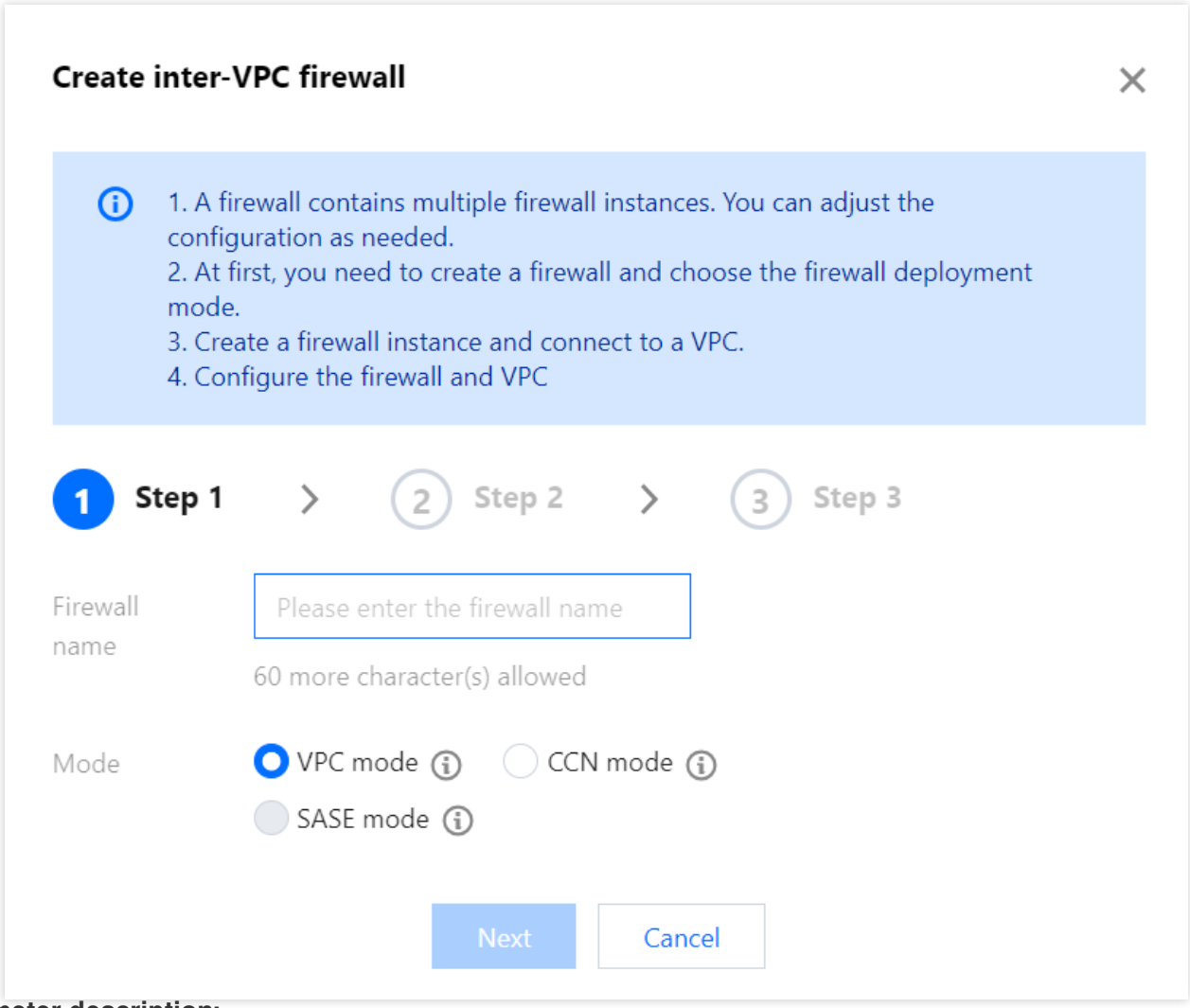
Last updated：2023-11-28 20:37:12

VPC Mode

1. Log in to the Cloud Firewall console, and select **Firewall toggle** > **Inter-VPC toggle** in the left sidebar.
2. On the **Inter-VPC toggle** page, click the **Firewall instances** page and then click **Create instance**.



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



Parameter description:

Instance name: The custom name of the firewall instance.

Modes:

VPC mode: Connect the asset to CFW via VPC. Modify the VPC route table to direct the route.

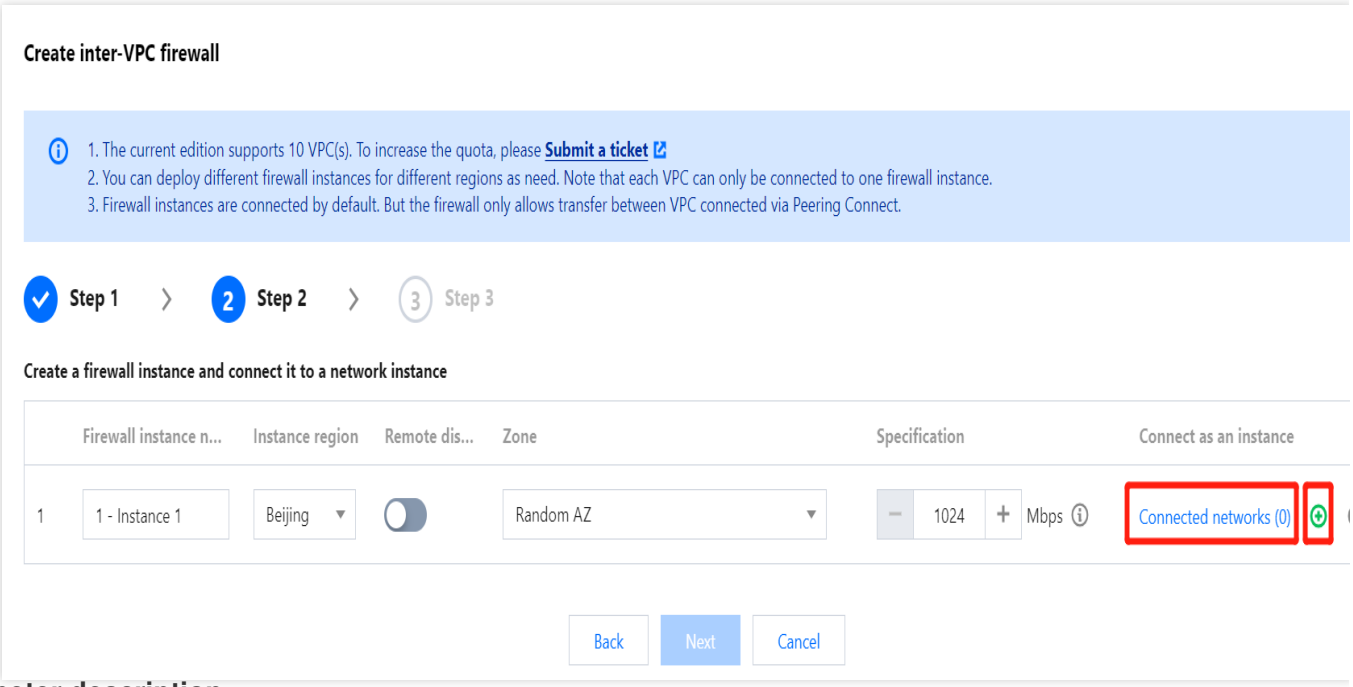
CCN mode: Connect the asset to CFW via CCN. Modify the CCN route table to direct the route. Note that the CCN instance must support multi-routes.

SASE mode: The feature is currently in beta test. To try it out, submit a ticket.

Privet network mode (CDC): It works the same as the VPC mode and only applies to the CDC environment.

4. Enter the firewall instance name and region, configure the disaster recovery, bandwidth and network settings, and click **Next**. To create instances as you want, click

.



Parameter description:

Region: Select the region where the VPC to protect locates.

Remote disaster recovery: Select it to enable remote disaster recovery.

Availability zone: Select an availability zone according to your needs.

Instance bandwidth: An instance supports 1-20 Gbps (up to 5 Gbps configurable). To set a bandwidth greater than the configurable limit, submit a ticket or upgrade your service. If you need more than the maximum bandwidth available, another firewall instance can be created. But make sure the throughput limit is not exceeded for each of your firewall instances.

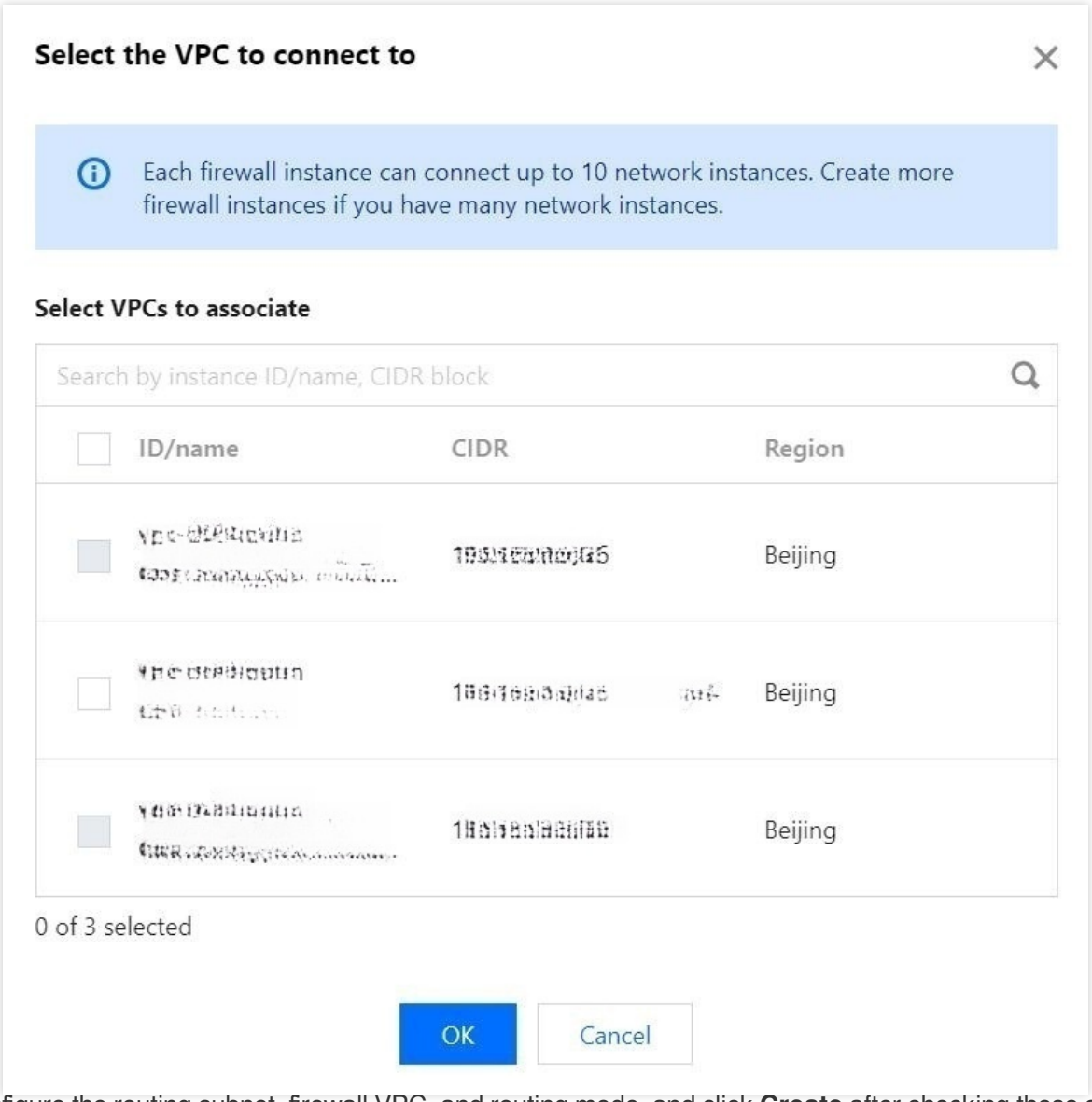
Connect as an instance: Click **Connected networks**, select VPCs within the region required, and click **OK**.

Important

A VPC associates with only one firewall instance.

Inter-VPC firewalls cannot communicate with the classic network, so peering connections or CCN instances must be created between VPCs.

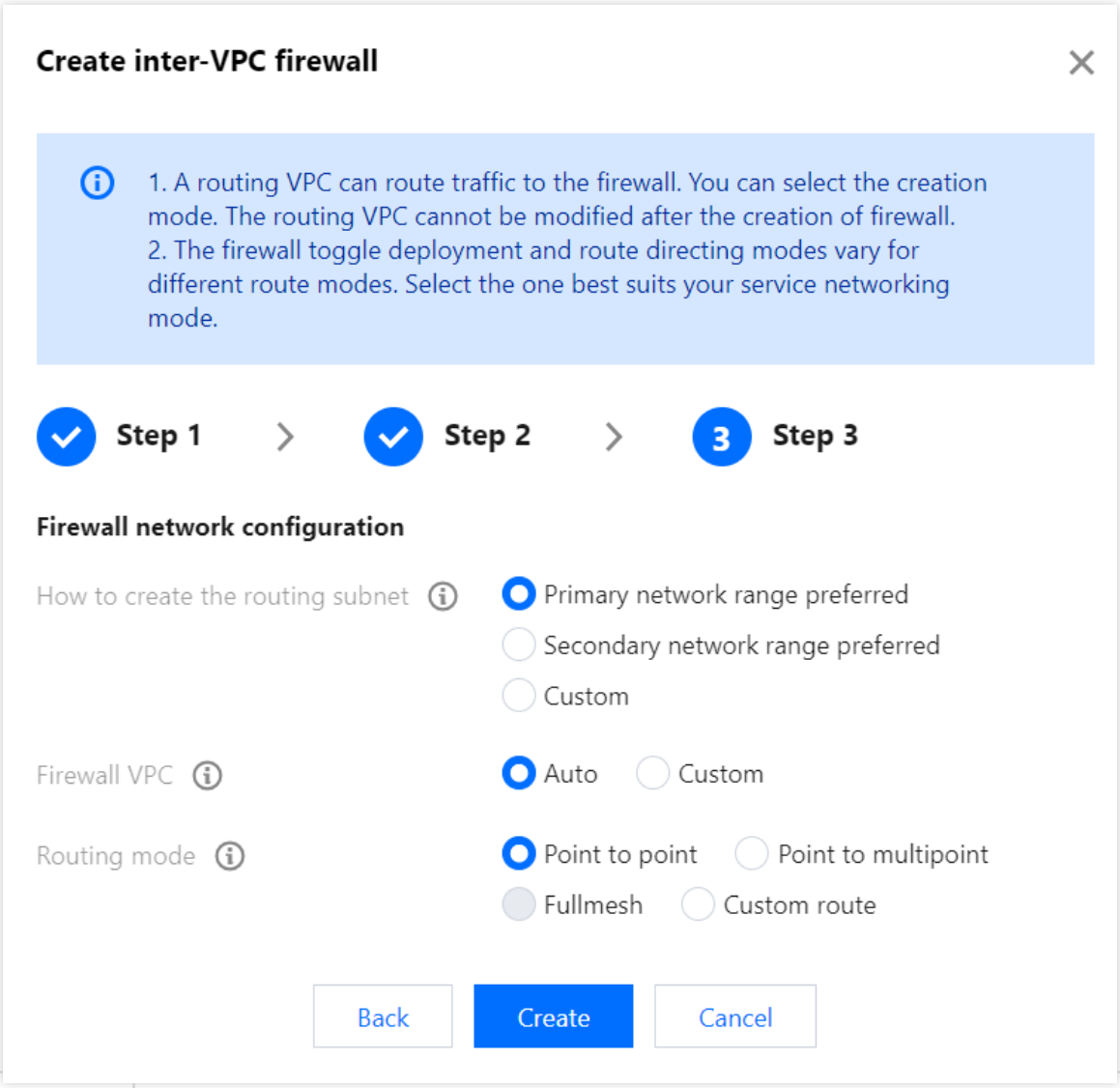
An inter-VPC firewall instance allows up to 10 VPCs in the same region. Multiple instances in the same region are supported. Create an inter-VPC firewall instance based on the region where a VPC is located before accessing the network.



5. Configure the routing subnet, firewall VPC, and routing mode, and click **Create** after checking these settings.

Notes

The creation process takes several minutes to complete.



Parameter	Description
Create routing subnet	CFW creates a 24 subnet in the connected VPC to route traffic to the firewall in three different ways. Once created, the subnet cannot be modified. Primary network range preferred: Automatically select an idle subnet range in the selected VPC. If the VPC does not have available subnet IPs, a secondary network range is used. Secondary network range preferred: Choose an idle secondary network range first. This mode does not consume the VPC's subnet quota. For more information about secondary network ranges, see Editing IPv4 CIDR Blocks. Custom: Specify a 24 network range within the CIDR block of the current VPC, such as 192.168.0.0/24.
Firewall VPC	It connects firewall instances and must be created in the regions where the VPCs you want to connect are located. Auto: CFW automatically creates a VPC with a /20 range that does not conflict with the connected VPCs. Custom: Set a VPC with a /20 range that does not conflict with the connected VPCs, such as 192.168.1.0/20.

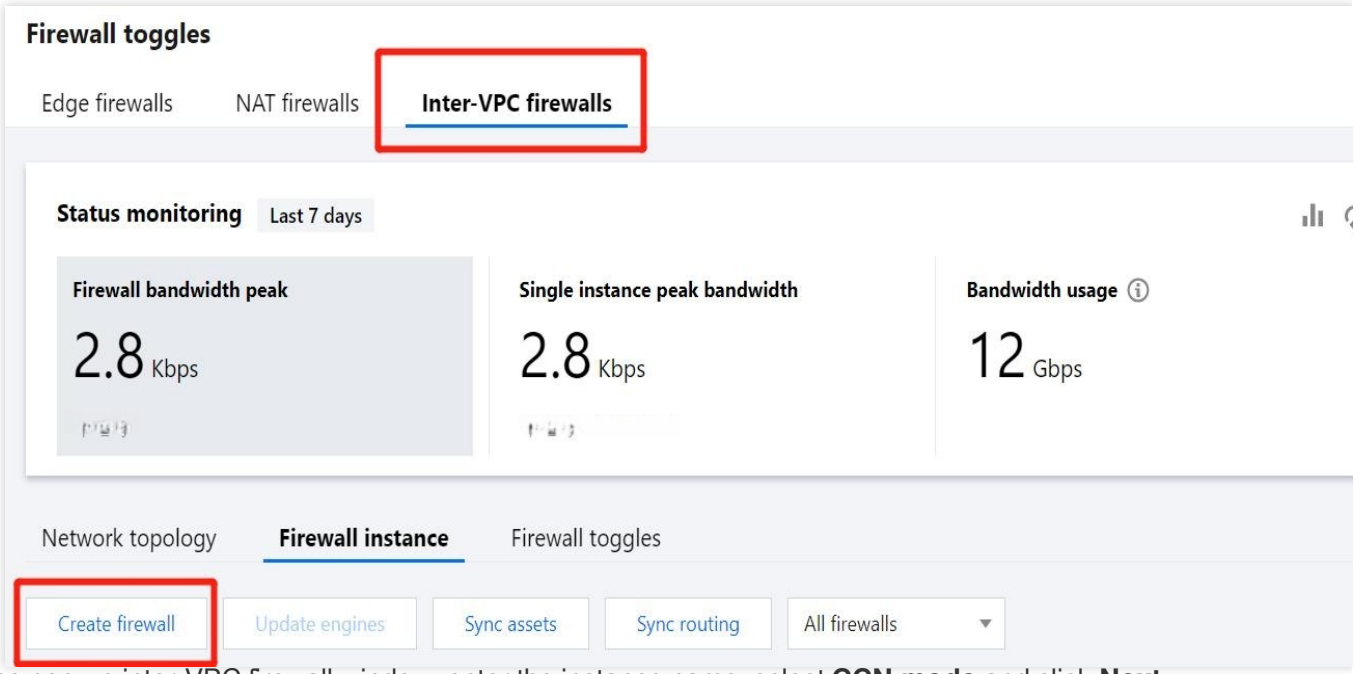
Routing mode	The way that networks are interconnected determines the firewall toggles and routing modes. Choose a routing mode that best suits your needs. Point-to-point: It is suitable for connecting a few VPCs with a simple network topology. In this mode, one toggle is generated for each VPC-to-VPC connection. Point to multipoint: It is suitable for connecting multiple VPCs to a simple network topology, such as a star network topology. In this mode, one toggle is set for each VPC and traffic between two VPCs goes through two firewall toggles. Fullmesh: It is suitable for connecting many VPCs to a complex network topology, such as a mesh network topology. In this mode, only one firewall toggle is set to control all VPC routes. Custom route: In this mode, no firewall toggles are set. You can configure a custom route as guided in Configuring Custom Routes after creating a firewall. Note: Custom route is only supported in multiple regions. For available routing modes, go to the CFW console.

CCN Mode

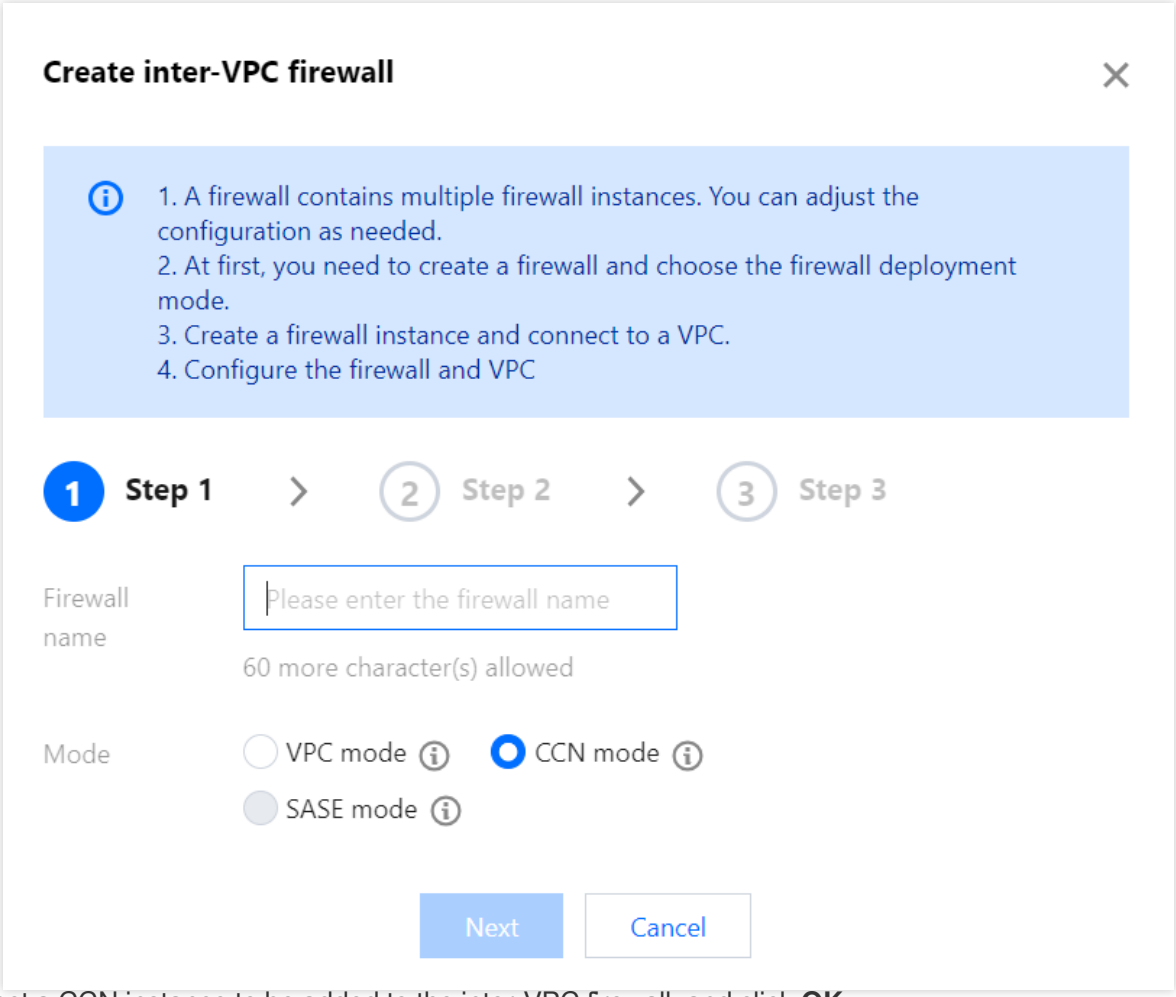
Important:

CCN has begun charging on connected network instances and inbound traffic from July 1, 2023, so creating a firewall VPC for your connected network instance may incur costs. For more details, see Start Charging on CCN Connected Network Instances and Inbound Traffic.

1. Log in to the Cloud Firewall console, and select **Firewall toggle** > **Inter-VPC toggle** in the left sidebar.
2. On the **Inter-VPC toggle** page, click the **Firewall instances** page and then click **Create instance**.



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



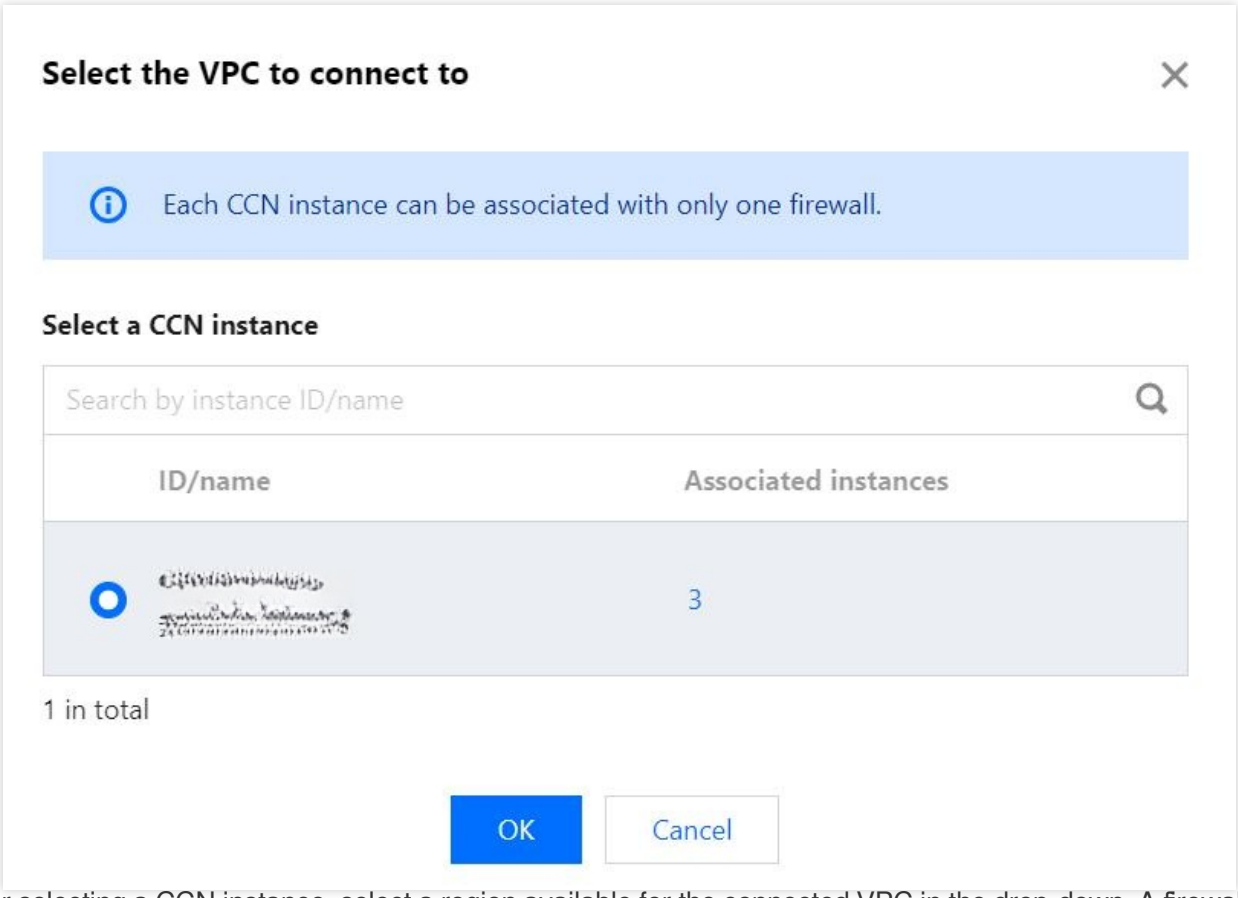
4. Select a CCN instance to be added to the inter-VPC firewall, and click **OK**.

Important

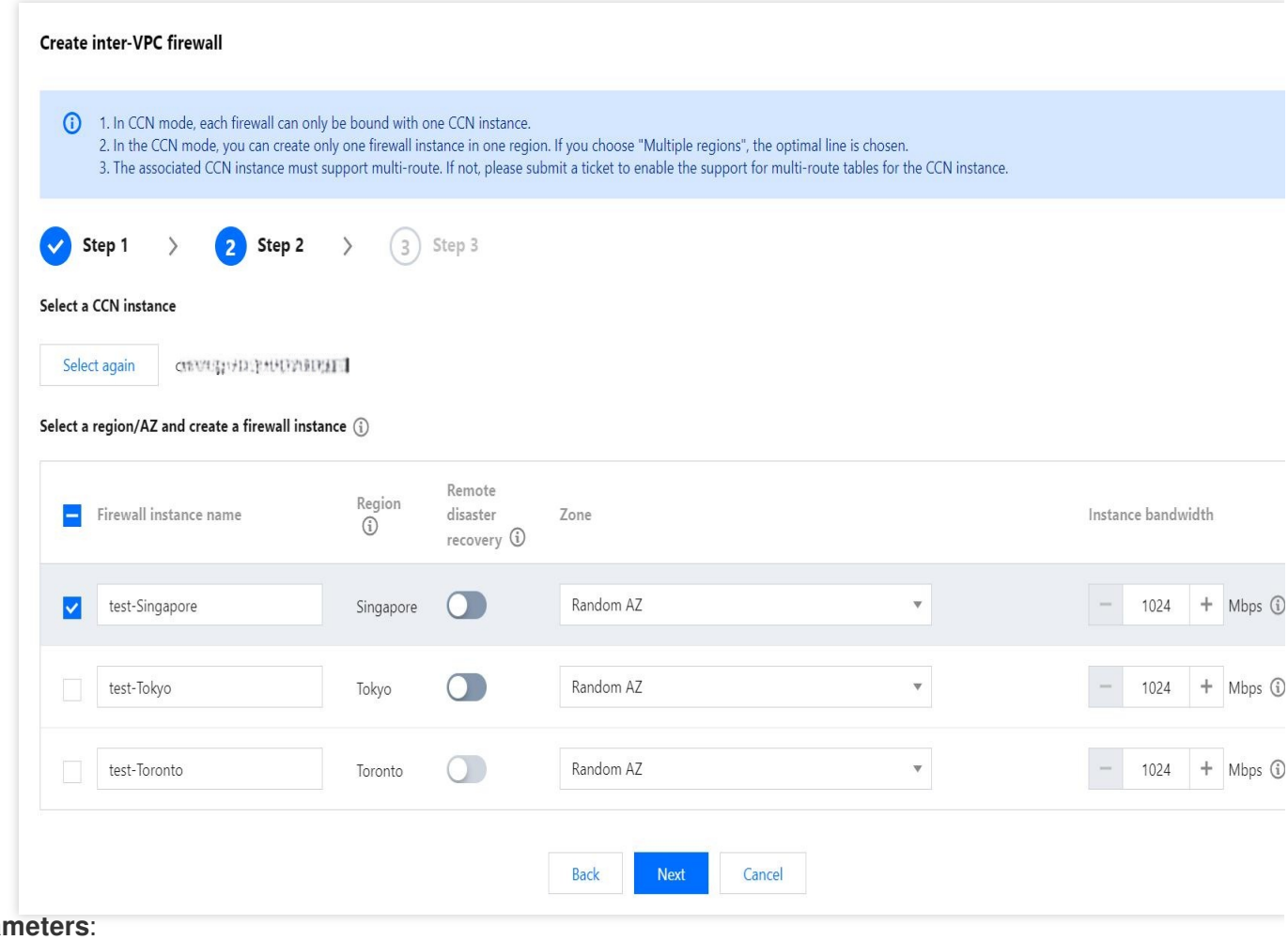
The CCN instance must support the multi-route table mode. If not, contact the CCN side to enable the multi-route table feature.

In the CCN mode, inter-VPC firewalls can be created in specified regions.

In the CCN mode, an inter-VPC firewall is associated with only one CCN instance.



5. After selecting a CCN instance, select a region available for the connected VPC in the drop-down. A firewall instance then will be created in this region. You can configure the firewall instance name, remote disaster recovery, and instance bandwidth specifications, and click **Next**.



Parameters:

Region: Select the region where the VPC to protect locates.

Notes

If only one region is selected to deploy a firewall instance, all inter-VPC traffic with the firewall toggles on will pass through the firewall instance in that region. This is suitable for a business network with a star topology.

If all regions are selected to deploy firewall instances, all inter-VPC traffic with the firewall toggles on will pass through the firewall instances in those regions. This is suitable for a business network with a mesh topology.

Custom route is only supported in multiple regions.

Remote disaster recovery: Select it to enable remote disaster recovery.

Availability zone: Select an availability zone according to your needs.

Instance bandwidth: An instance supports 1-20 Gbps (up to 5 Gbps configurable). To set a bandwidth greater than the configurable limit, submit a ticket or upgrade your service. If you need more than the maximum bandwidth available, another firewall instance can be created.

Important

Make sure the throughput limit is not exceeded for each of your firewall instances.

6. Configure the routing VPC and routing mode. Click **Create** after checking these settings.

Notes

The creation process takes several minutes to complete.

Parameter	Description
Create routing VPC	CFW can route traffic to the firewall through a VPC with /20 range. It can be created in the associated CCN instance via three different ways. Auto: A random idle /20 range is selected. Custom: Set a VPC IP range to be used for the firewall on your own. It must be a /20 range. For example, 192.168.1.0/20. Important: CCN has begun charging on connected network instances and inbound traffic from July 1, 2023, so creating a firewall VPC for your connected network instance may incur costs. For more details, see Start Charging on CCN Connected Network Instances and Inbound Traffic.
Routing mode	The way that networks are interconnected determines the firewall toggles and routing modes. Choose a routing mode that best suits your needs. Point-to-point: It is suitable for connecting a few VPCs with a simple network topology. In this mode, one toggle is generated for each VPC-to-VPC connection. Point to multipoint: It is suitable for connecting multiple VPCs to a simple network topology, such as a star network topology. In this mode, one toggle is set for each VPC and traffic between two VPCs goes through two firewall toggles. Fullmesh: It is suitable for connecting many VPCs to a complex network topology, such as a mesh network topology. In this mode, only one firewall toggle is set to control all VPC routes. Custom route: In this mode, no firewall toggles are set. You can configure a custom route as guided in Configuring Custom Routes after creating a firewall. Note: Custom route is only supported in multiple regions. For available routing modes, go to the CFW console.

Viewing Inter-VPC Firewalls

Last updated：2023-11-28 20:40:15

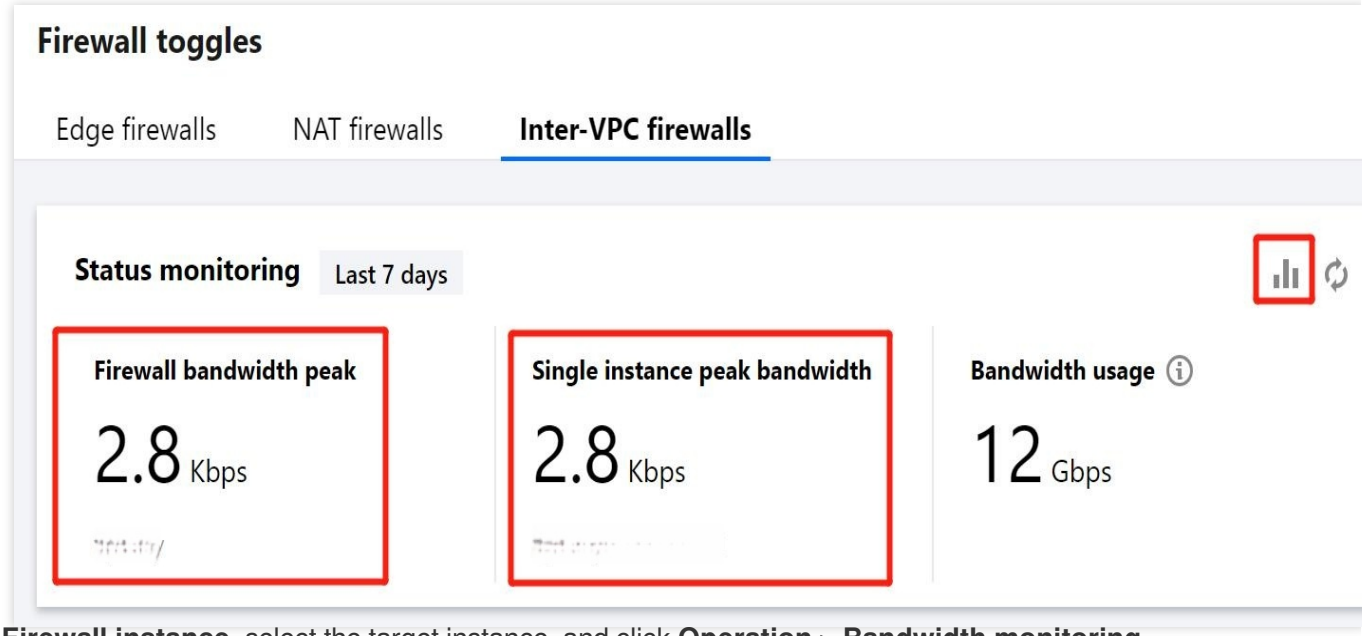
Viewing bandwidth monitoring

Inter-VPC firewalls support monitoring the bandwidth of the entire firewall and individual instances. You can query in different ways.

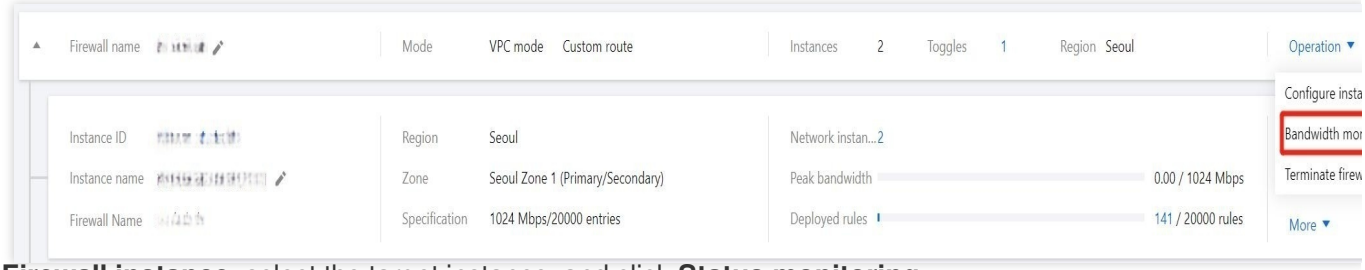
1. Log in to the Cloud Firewall console, and select **Firewall toggles** > **Inter-VPC toggles** in the left sidebar.
2. On the page that appears, open the monitoring panel via one of these three methods:

Click

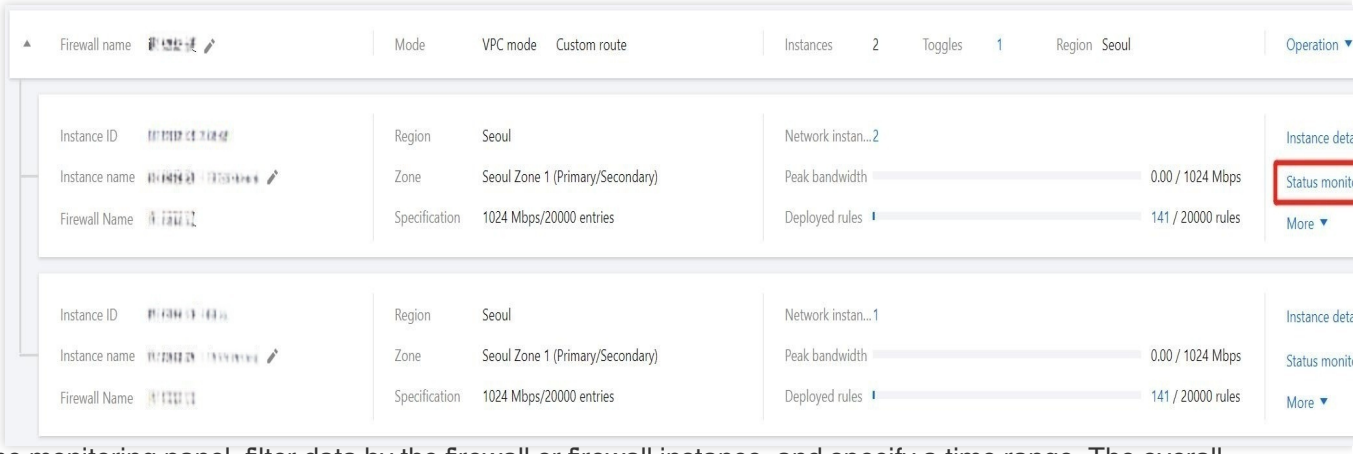
in the top right corner, or click **Firewall bandwidth peak** > **Single instance peak bandwidth**.



Click **Firewall instance**, select the target instance, and click **Operation** > **Bandwidth monitoring**.



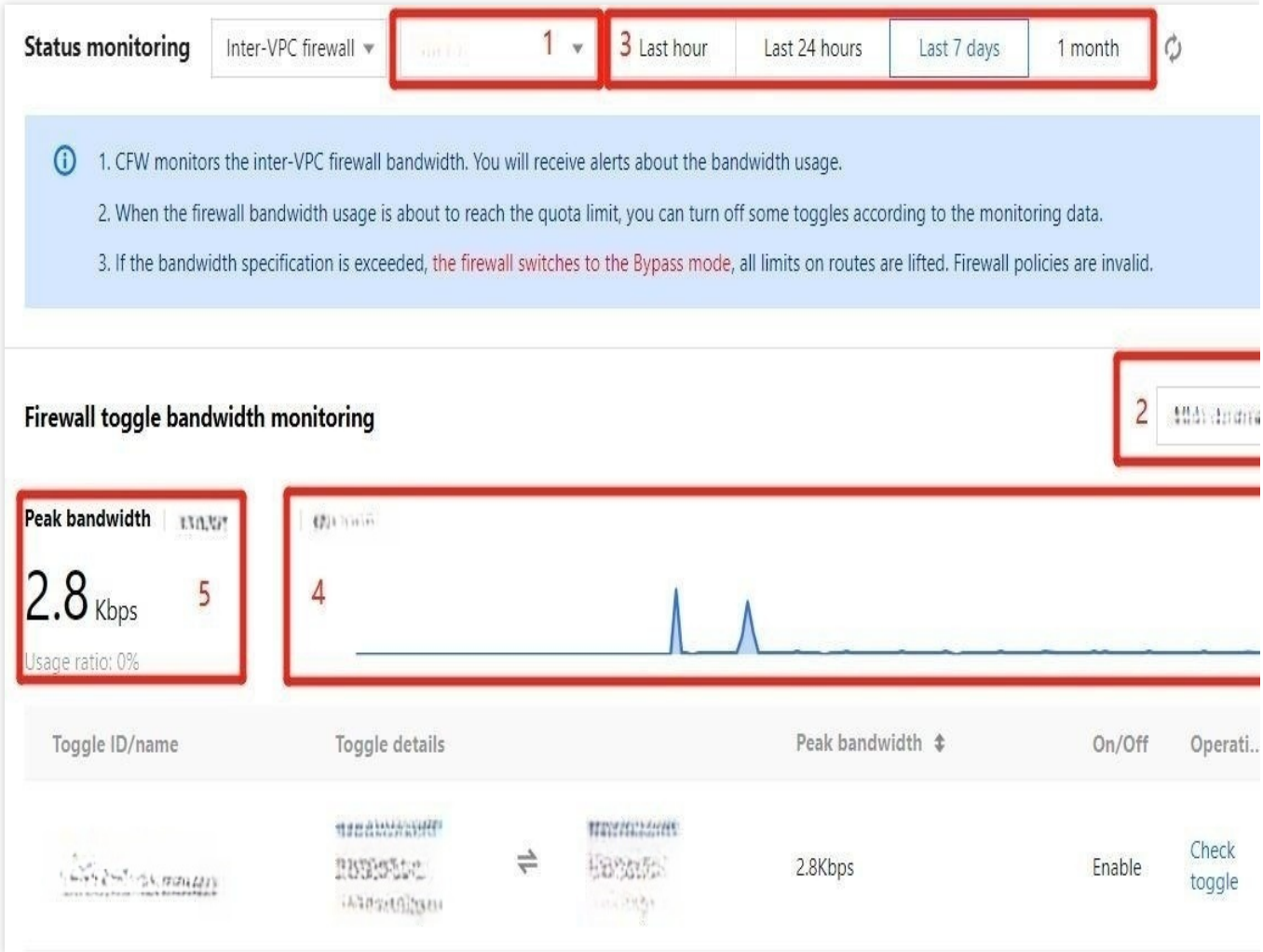
Click **Firewall instance**, select the target instance, and click **Status monitoring**.



3. In the monitoring panel, filter data by the firewall or firewall instance, and specify a time range. The overall bandwidth usage and the peak amount will be displayed.

Important

The minimum granularity affects the accuracy of the observed peak bandwidth. To get the actual peak value, go to the TCOP console or view specific metrics in the monitoring panel.

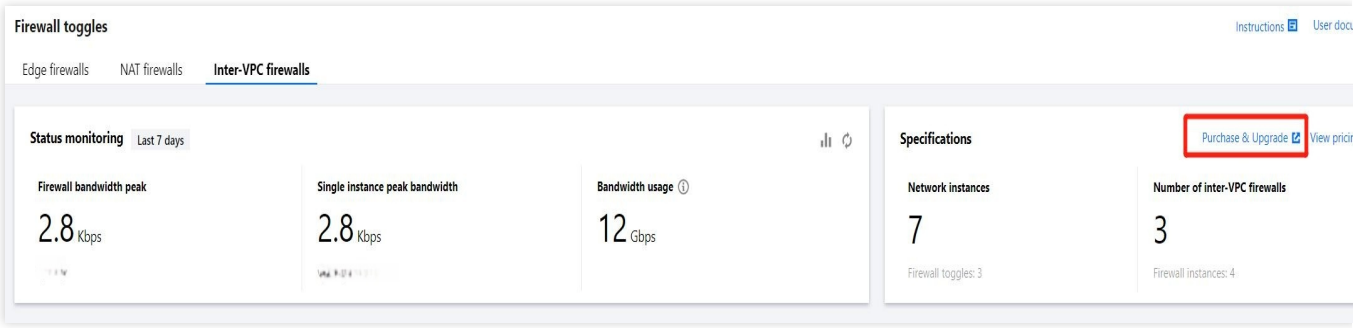


4. In the monitoring panel, click **View all monitoring metrics** to open a dashboard that shows all metrics of a firewall instance, including concurrent connections, and both inbound and outbound private packets and private bandwidth.

These metrics are also viewable in the TCOP console, and alerts can be configured as needed.

Viewing specifications

To check specification information of connected network instances and inter-VPC firewall instances, go to Firewall toggles page > **Specifications**. Click **Purchase & Upgrade** in the top right corner to go to the purchase page. For users of CFW Enterprise, one inter-VPC firewall can be created. For CFW Ultimate users, up to 3 inter-VPC firewalls are allowed.



Managing Inter-VPC Firewalls

Last updated：2023-11-28 20:41:56

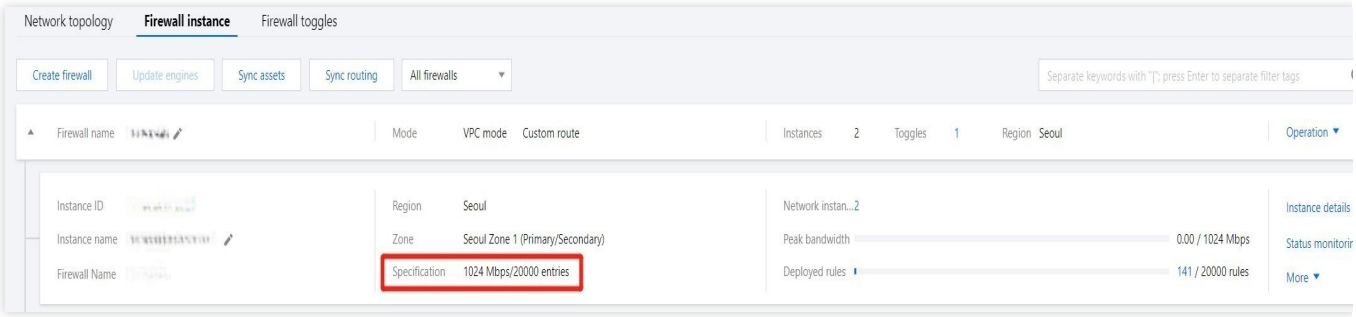
After an inter-VPC firewall is created, you can manage its instances separately.

Viewing an Instance

1. Log in to the Cloud Firewall console, and select **Firewall toggle** > **Inter-VPC toggle** in the left sidebar.
2. On the page displayed, click **Firewall instance** to view the created firewall and its deployed firewall instances.

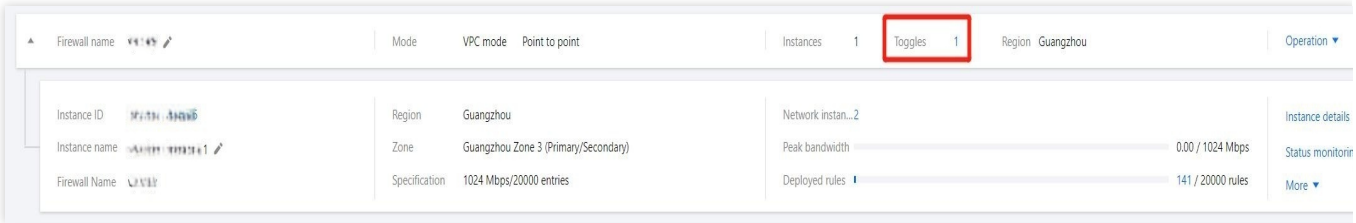
Notes

Specification: The maximum amount of bandwidth and maximum number of rules for the current firewall instance. For more details, see NAT Firewall Toggle.



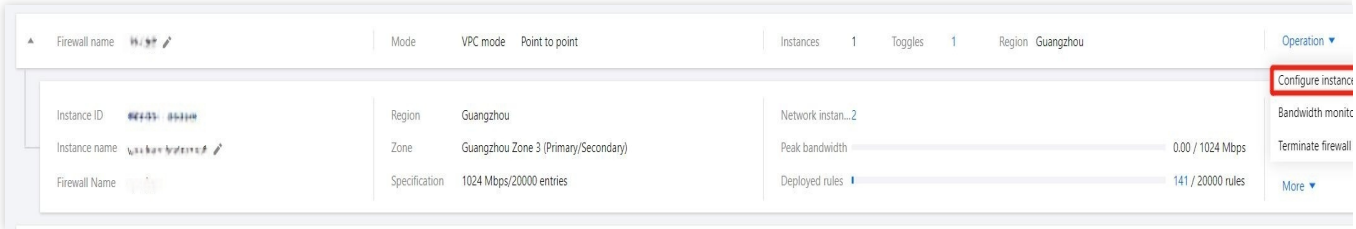
Viewing Associated Toggles

To filter associated firewall toggles, click **Toggles** on the firewall instance page.

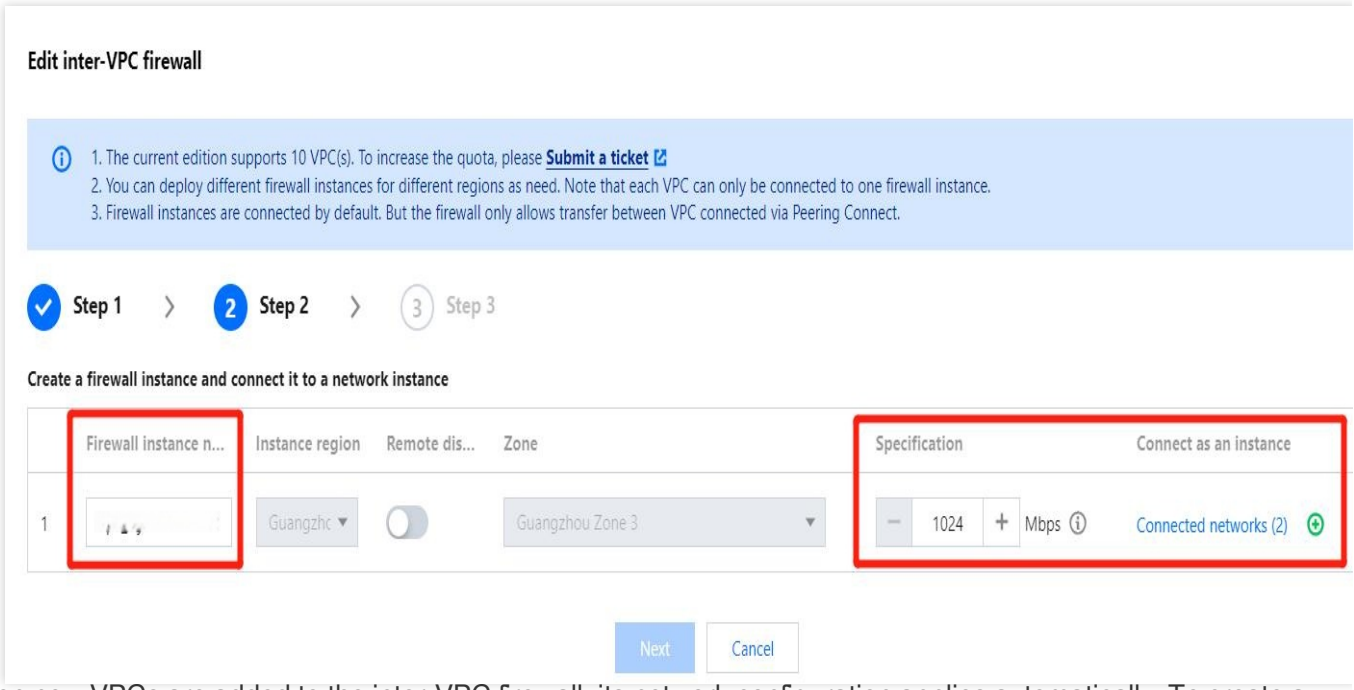


Configuring Firewall Instances

1. On the firewall instance page, locate the target inter-VPC firewall and select **Operation** > **Configure instance**.



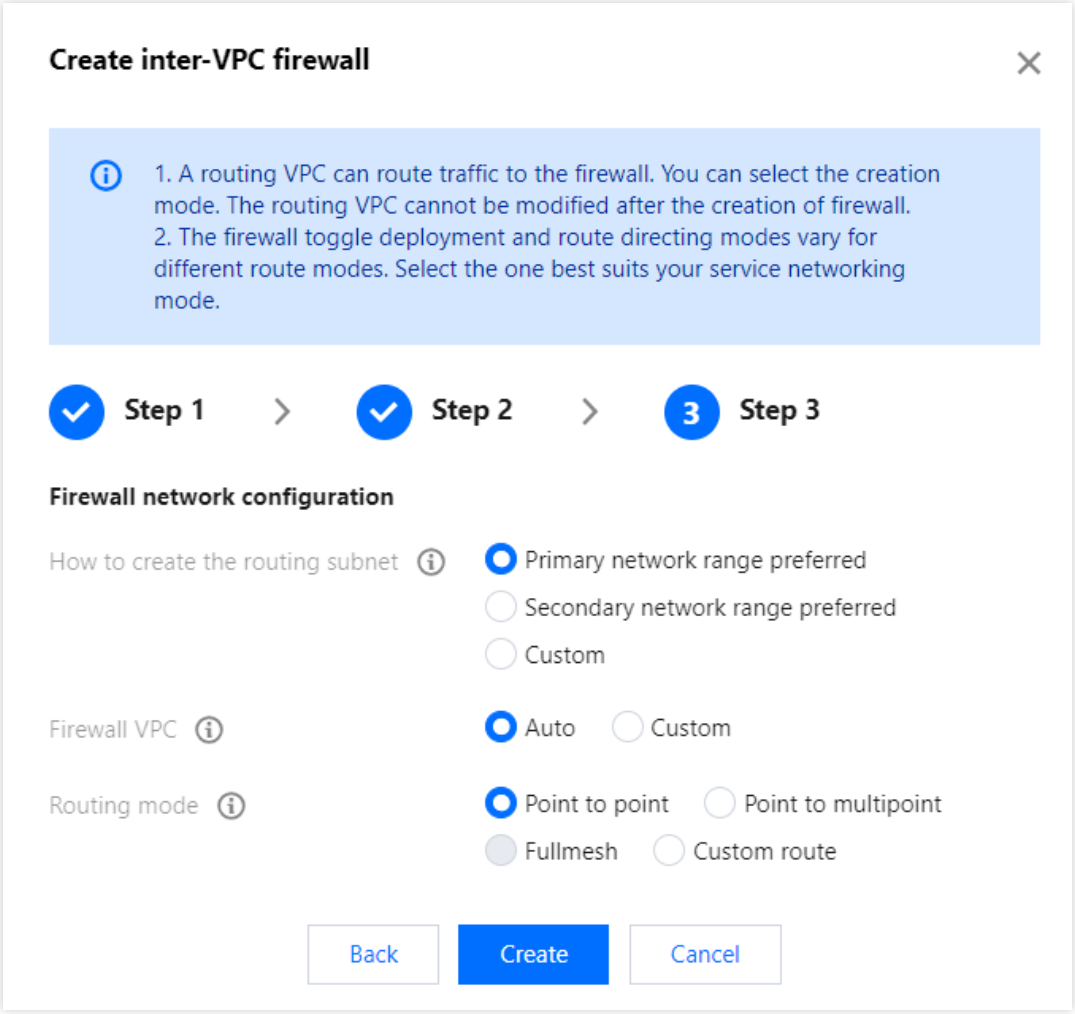
2. Modify the name, specification and connected network instances initially configured when the firewall instance is created, and add new instances as needed.



3. When new VPCs are added to the inter-VPC firewall, its network configuration applies automatically. To create a custom forwarding subnet, add the corresponding subnet CIDR manually.

Important

The firewall network configuration cannot be changed.

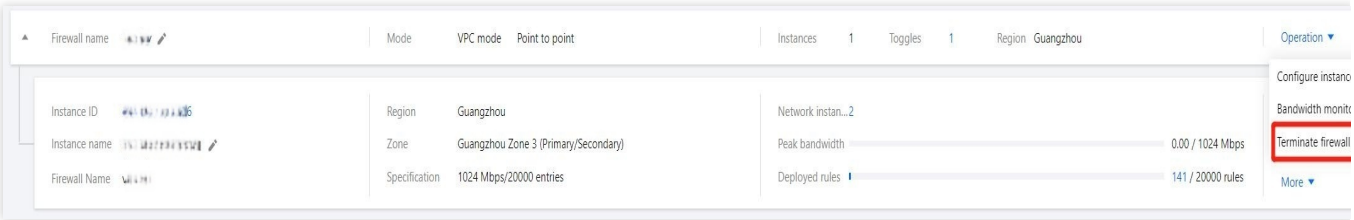


Terminating Inter-VPC Firewalls

On the firewall instance page, locate the target inter-VPC firewall and select **Operation** > **Terminate firewall**. It will then be terminated after your confirmation.

Important

If **Custom route** is set, you need to restore the route manually.



Managing Inter-VPC Firewall Instances

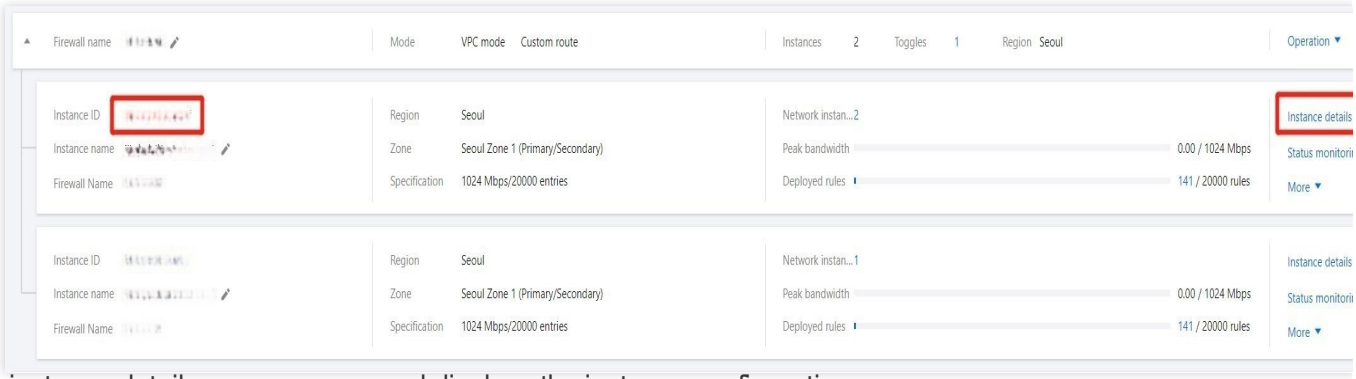
Last updated：2023-11-28 20:45:15

After an inter-VPC firewall is created, you can manage its instances separately.

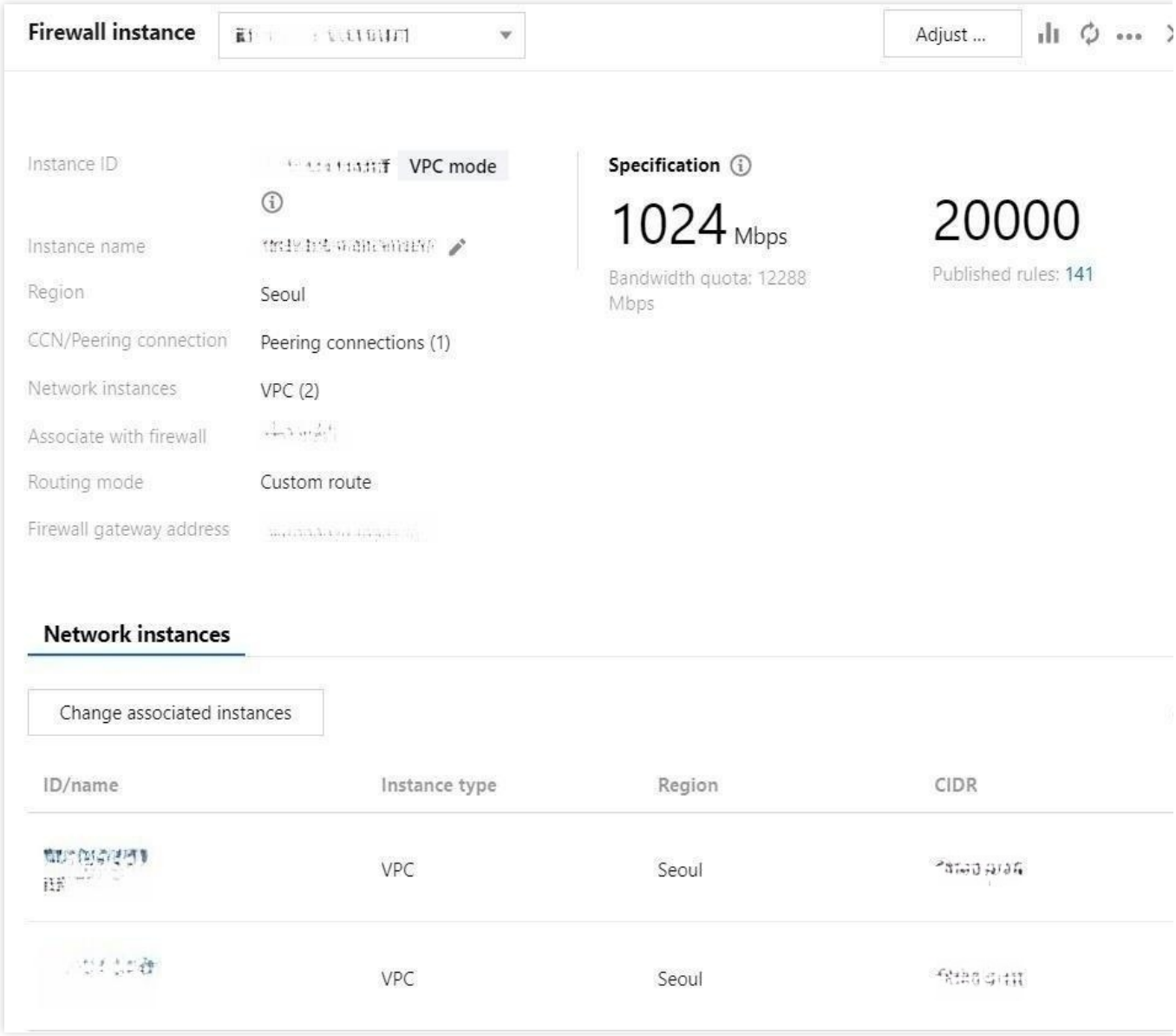
1. Log in to the Cloud Firewall console, and select **Firewall toggle** > **Inter-VPC toggle** in the left sidebar.
2. On the **Inter-VPC toggle** page, click **Firewall instance**.

Viewing Instance Details

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

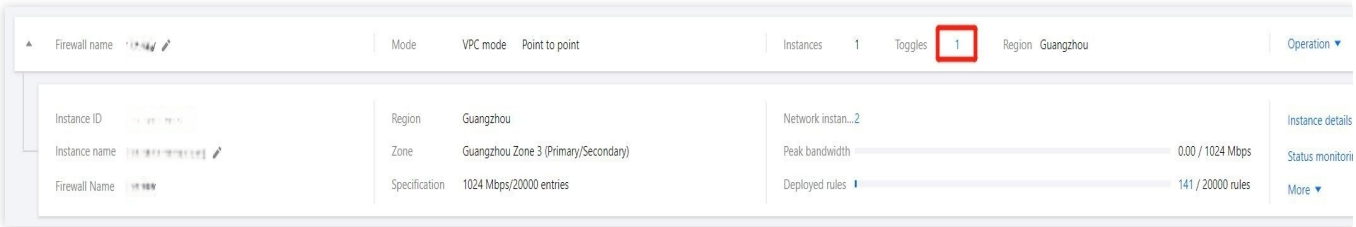


2. The instance details page appears and displays the instance configuration.



Viewing Associated Toggles

To filter associated firewall toggles, click **More** > **View firewall toggles** on the firewall instance page.



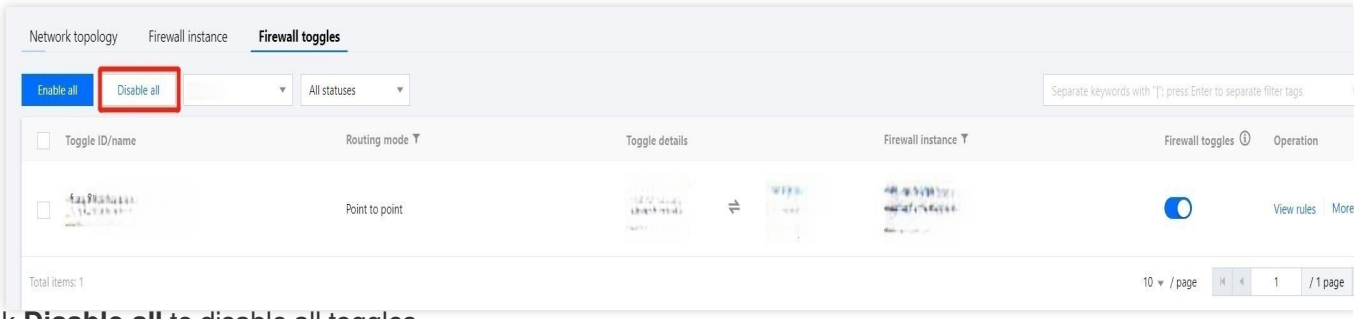
Notes

A toggle can be associated with multiple firewall instances and controls traffic going through these firewall instances.

Terminating Inter-VPC Firewall Instances

To terminate any firewall instance, all toggles must be disabled.

1. On the firewall instance page, click **Toggles** on the right of the corresponding inter-VPC firewall.

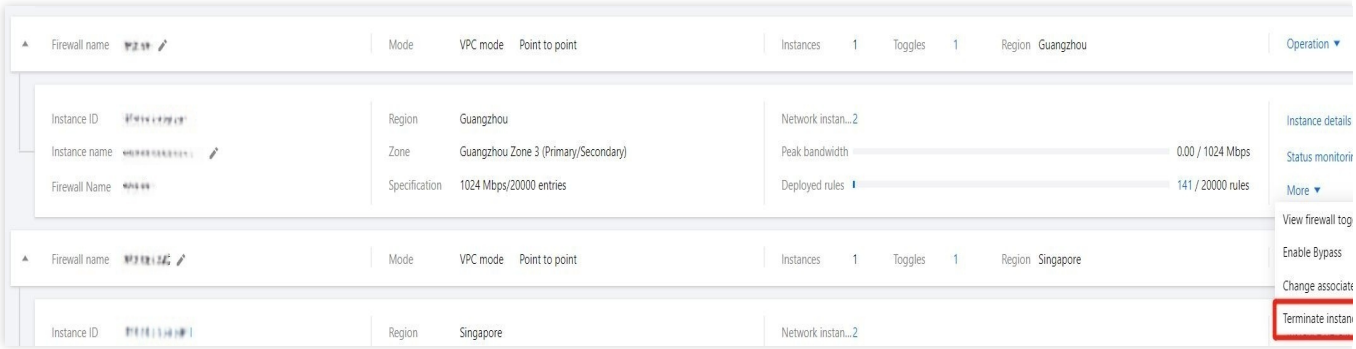


2. Click **Disable all** to disable all toggles.

3. Click **More** > **Terminate instance**. The current firewall instance will be terminated after confirmation.

Notes

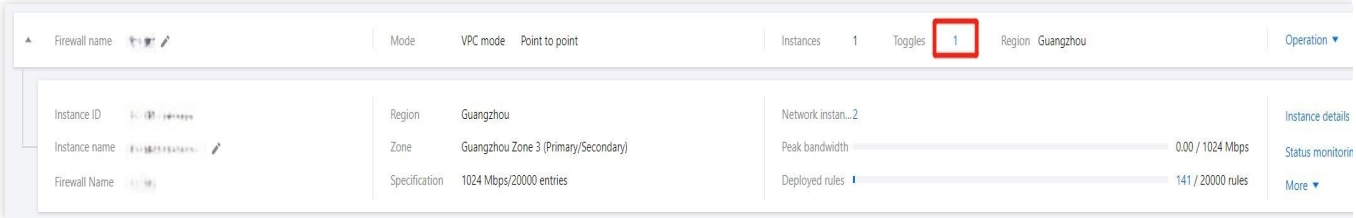
After termination, the VPCs will be automatically disconnected and the corresponding quota will be returned.



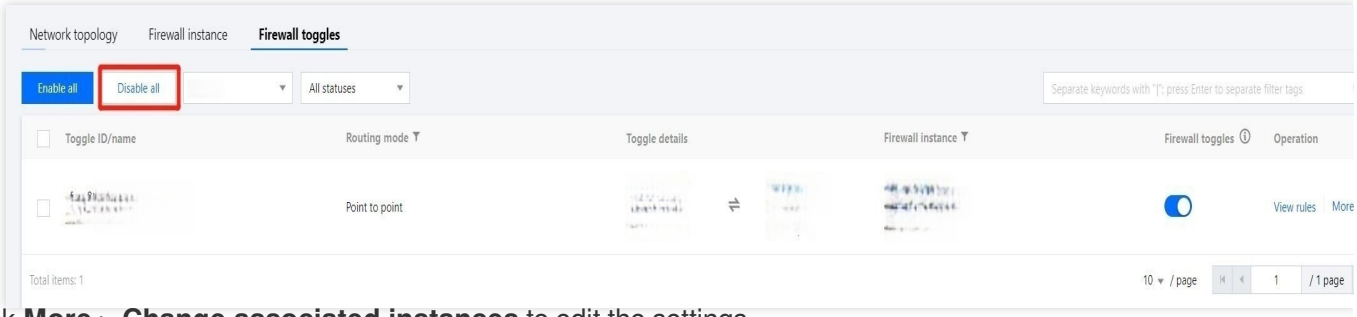
Changing Associated Instances

To change the associated instance, all toggles must be turned off.

1. On the firewall instance page, click **Toggles** on the right of the corresponding inter-VPC firewall.



2. Click **Disable all** to disable all toggles.

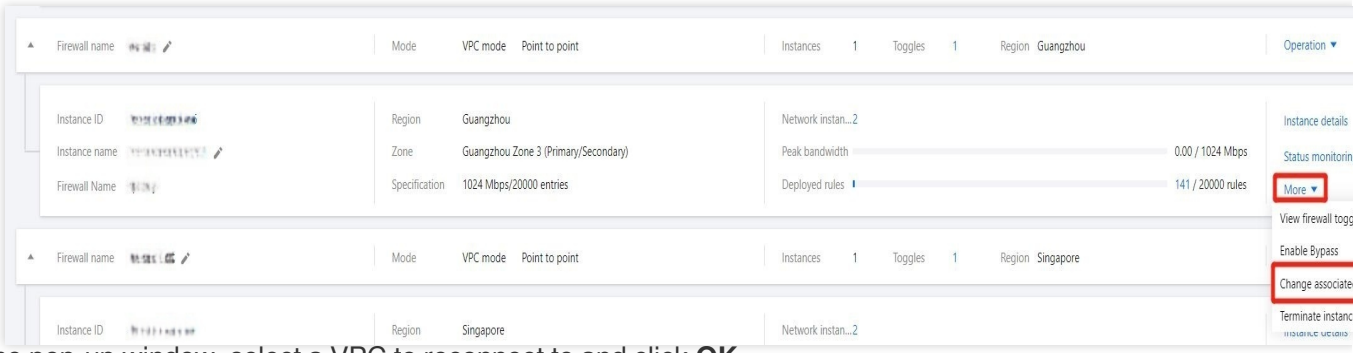


3. Click **More** > **Change associated instances** to edit the settings.

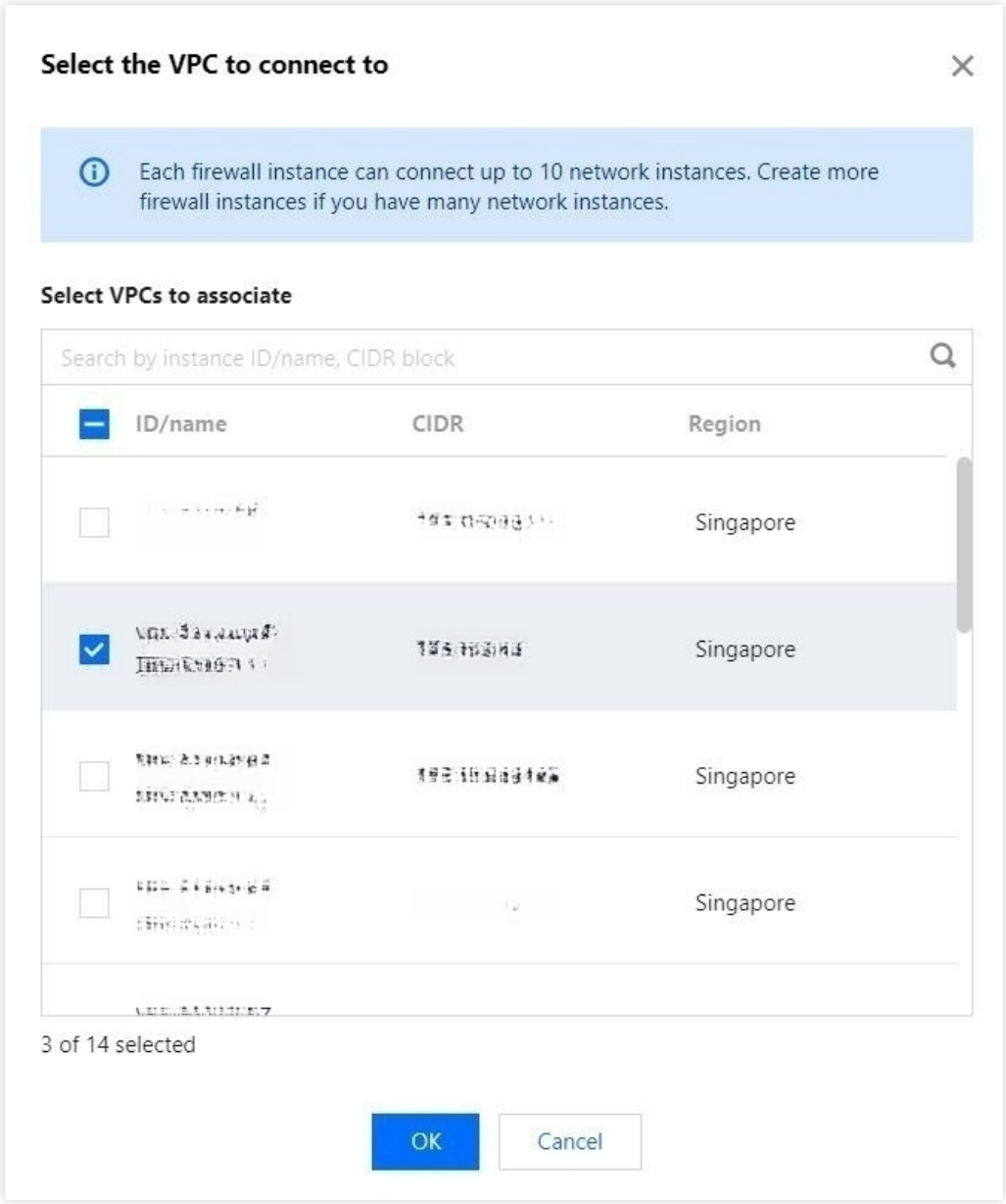
Important

Associated instances can be changed if an inter-VPC firewall is connected in the VPC mode.

If it's connected in the CCN mode, this feature is unavailable.



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



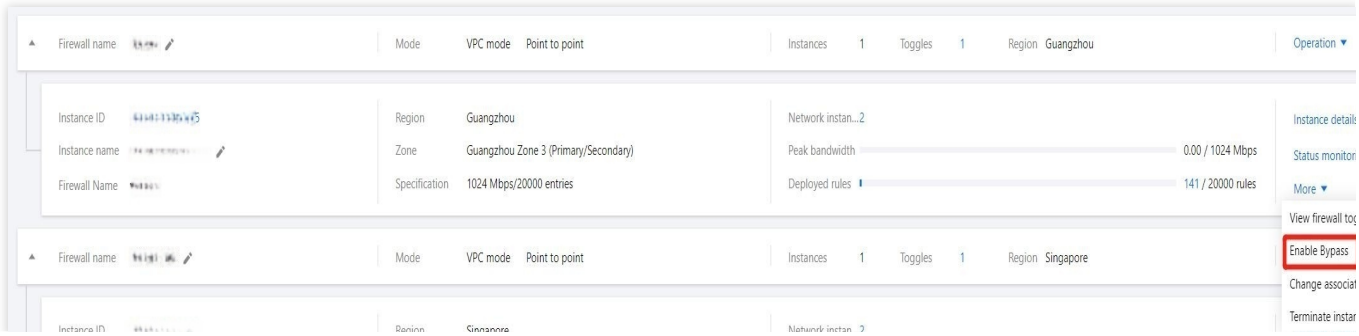
Bypass Mode

Inter-VPC firewalls provide Bypass mode that allows instance traffic to bypass your firewall. **Use this mode only for debugging**.

On the firewall instance page, click **More** > **Enable Bypass** / **Disable Bypass**.

Important

Disable Bypass mode once the debugging completes.


Firewall name
Mode
VPC mode
Point to point
Instances
1
Toggles
1
Region
Guangzhou
Operation
Instance ID
Instance name
Firewall Name
Region
Guangzhou
Zone
Guangzhou Zone 3 (Primary/Secondary)
Specification
1024 Mbps/20000 entries
Network instan...2
Peak bandwidth
0.00 / 1024 Mbps
Deployed rules
141 / 20000 rules
Instance details
Status monitor
More
Firewall name
Mode
VPC mode
Point to point
Instances
1
Toggles
1
Region
Singapore
View firewall tog
Enable Bypass
Change associat
Terminate instar

Managing Firewall Toggles

Last updated：2023-11-28 20:51:48

On the Firewall Toggles page, you can control traffic between VPCs through inter-VPC firewall toggles. You don't need to adjust the firewall settings when there is an asset change, as CFW can automatically sync assets in a short time.

Important

Enabling/Disabling firewall toggles involves switching networks and routes. This can cause a short network jitter and interruption.

Route Modes

There are four route modes available for firewall toggles.

Point-to-point mode: A firewall toggle is set for one pair of interconnected VPCs. A pair of interconnected VPCs is enabled by one peering connection or CCN instance.

Point to multipoint mode: A firewall toggle is set for one VPC and controls all traffic entering or leaving this VPC. Traffic exchanges between two VPCs go through two separate firewall toggles.

Fullmesh mode: A firewall toggle is set for all associated VPCs.

Custom route: Only associated VPCs are displayed.

Changes made to a VPC peering connection or CCN instance are synced to firewall toggles, which must be disabled to avoid any business interruption.

Important:

Though CFW cannot connect to the classic network, firewall toggles can be automatically created based on reachable routes. If there is no toggle, check whether there is a peering connection or CCN instance.

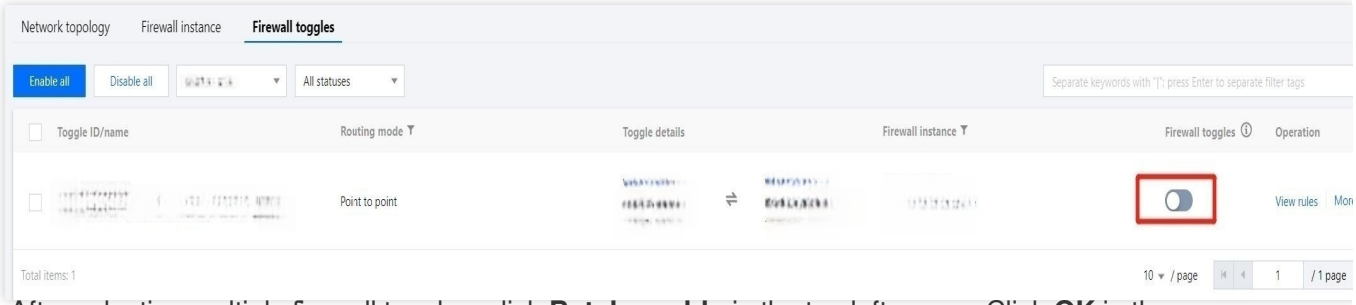
Enabling Firewall Toggles

After the toggle is turned on, the system automatically modifies the routing policy of the relevant route table. The traffic between the local network and the peer network, which are associated with the firewall toggle, is directed to the inter-VPC firewall.

1. On the Inter-VPC toggle page, firewall toggles can be turned on in the following ways.

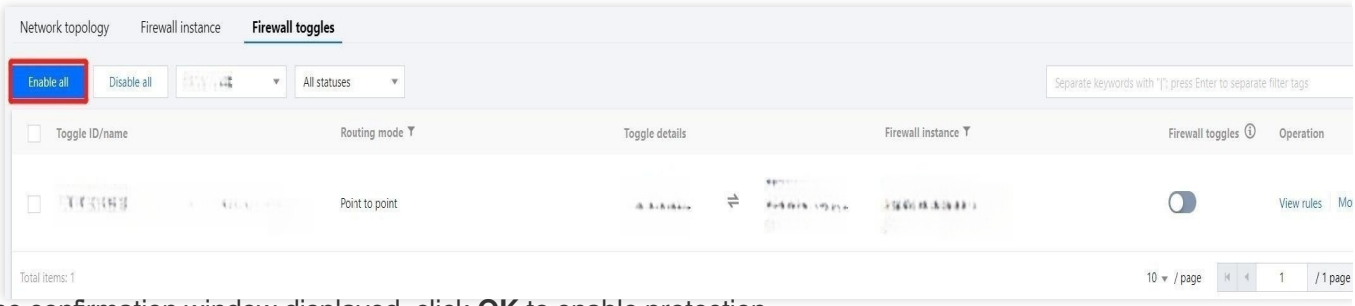
Single: Select a firewall toggle and click the

icon in the **Firewall toggle** column. Click **OK** in the pop-up confirmation window.



Batch: After selecting multiple firewall toggles, click **Batch enable** in the top left corner. Click **OK** in the pop-up confirmation window.

All: Click **Enable all** in the top left corner.



2. In the confirmation window displayed, click **OK** to enable protection.

Important

If the VPC peering connection or CCN instance is not correctly configured, the firewall cannot be enabled.

When the firewall toggle is on, don't change the corresponding routes manually in the VPC console. Otherwise, the network gets interrupted due to the missing routes.

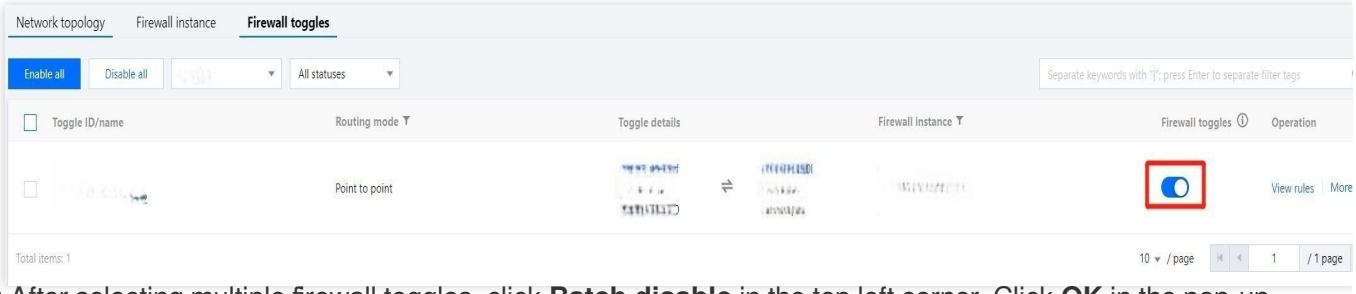
Disabling Firewall Toggles

When the firewall is disabled, the original route policies are restored. The traffic between the local network and peer network goes through the original path instead of the inter-VPC firewall.

1. On the Inter-VPC toggle page, click **Firewall toggle**. You can turn off firewall toggles individually, in a batch, or all of them.

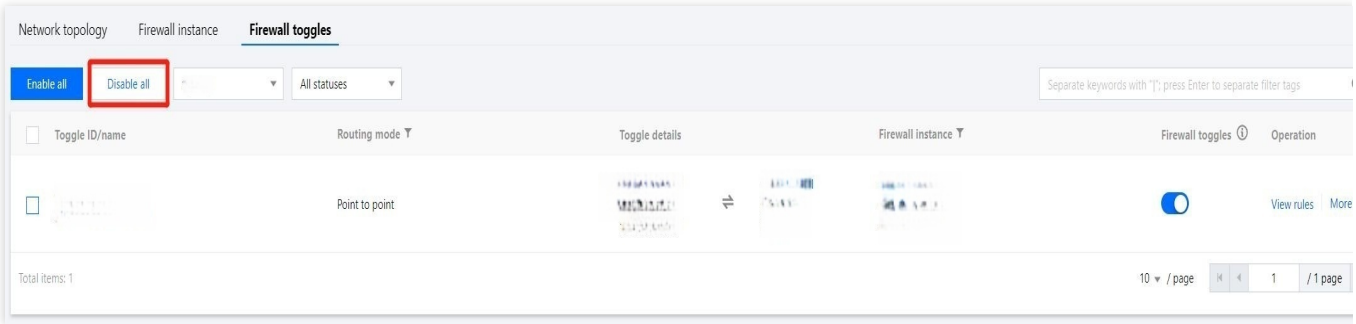
Single: Select a firewall and click the

icon in the **Firewall toggle** column. Click **OK** in the pop-up window to disable it.



Batch: After selecting multiple firewall toggles, click **Batch disable** in the top left corner. Click **OK** in the pop-up confirmation window.

All: Click **Disable all** in the top left corner.



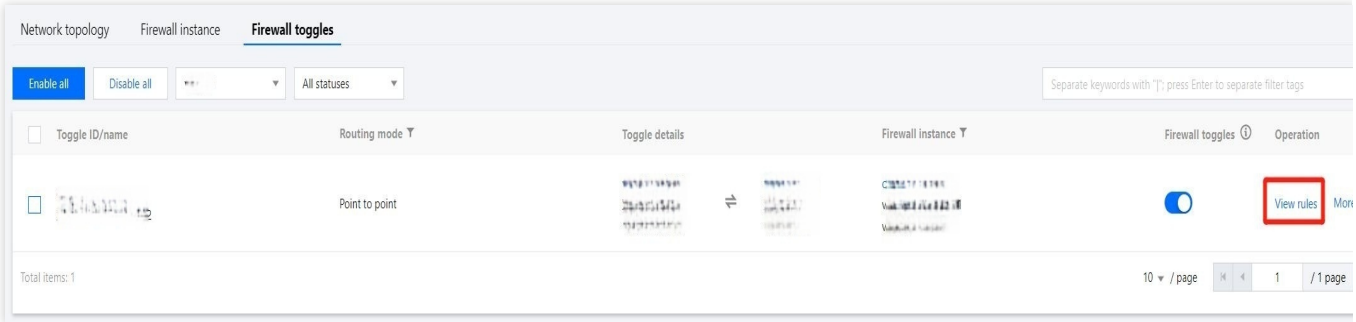
2. In the confirmation window displayed, click **OK** to disable the protection.

Important

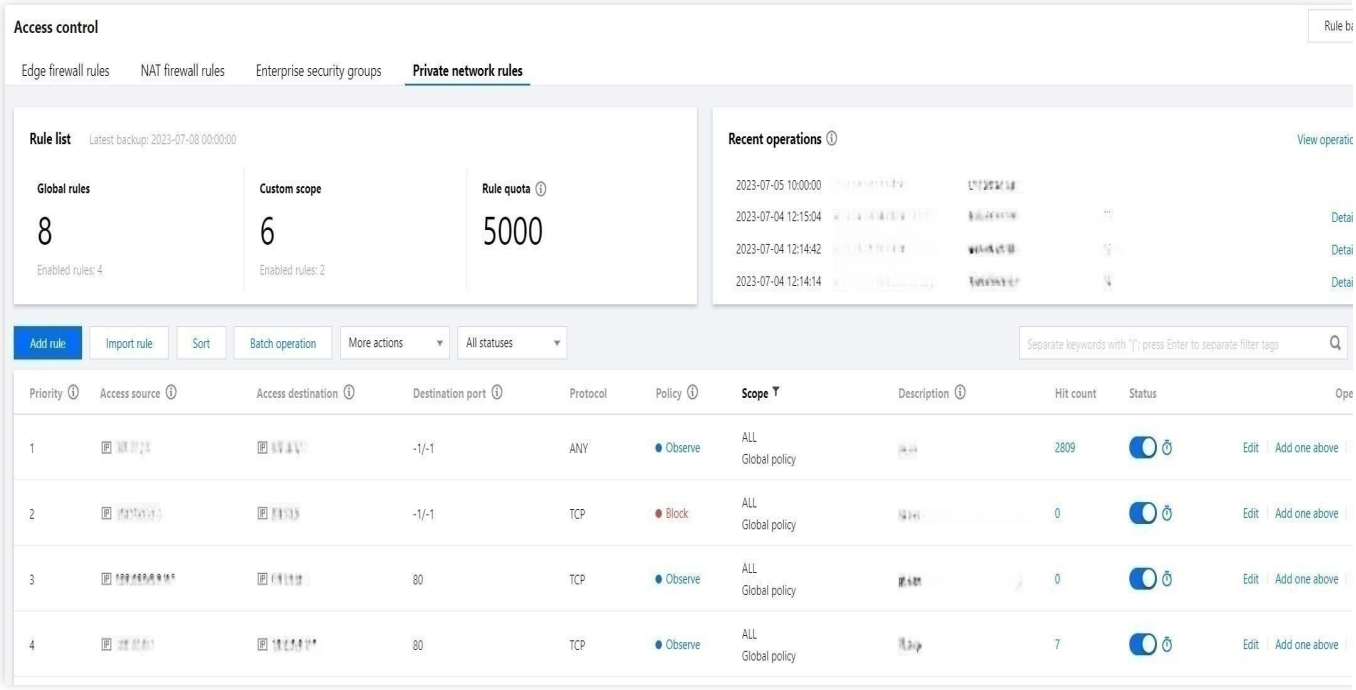
After the firewall toggle is disabled, you can switch the VPC routes as needed. Do not manually enable the firewall routes, otherwise this will cause network interruptions and firewall toggle failure.

Viewing Rules

1. On the Inter-VPC toggle page, click **Firewall toggle**.
2. On the **Firewall toggle** page, click **View rules** on the right of the target firewall toggle.



3. On the **Private network rules** page, view and edit the rules as needed.



Viewing Logs

1. On the Inter-VPC toggle page, click **Firewall toggle**.
2. On the page that appears, select **More** > **View logs** to view access control logs or traffic logs.

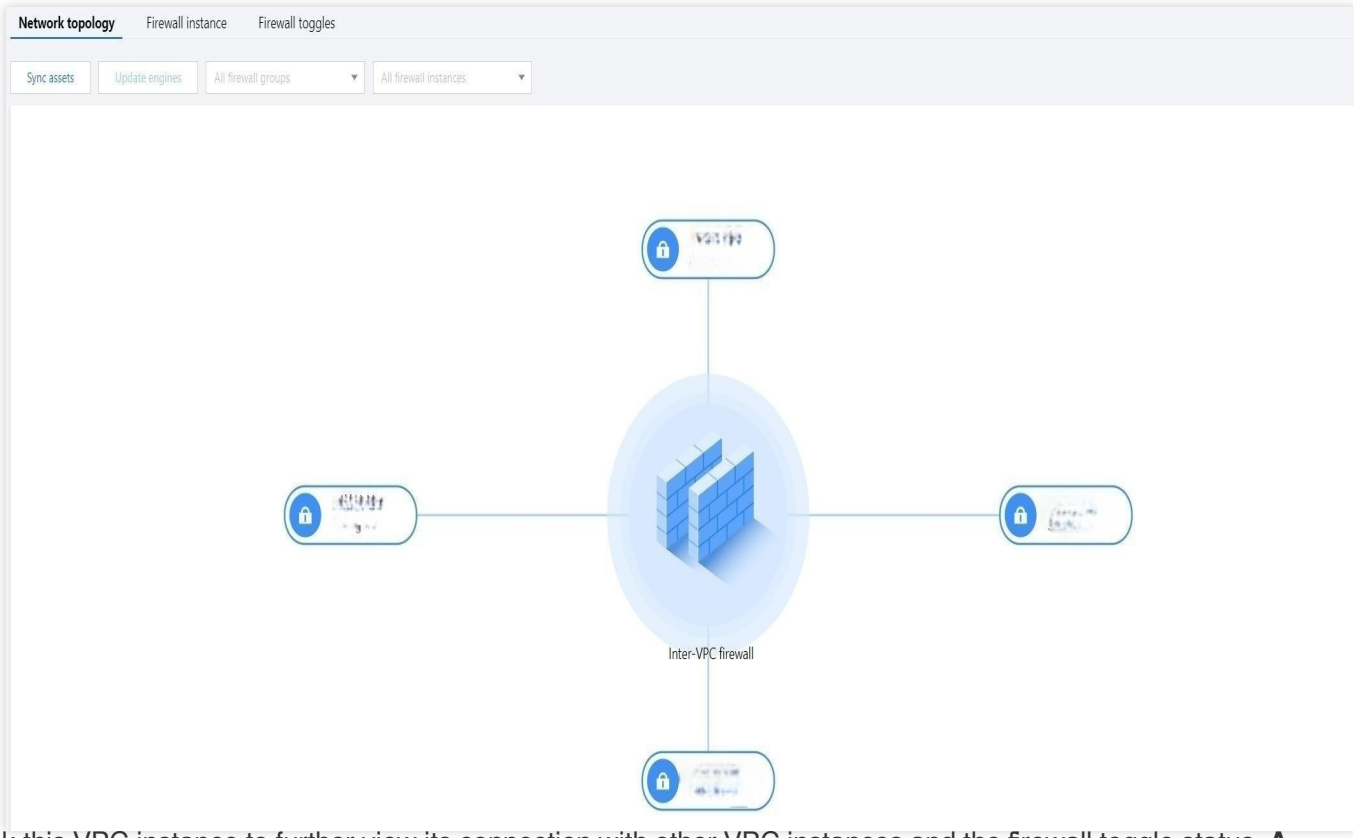
Using Network Topologies

Last updated：2023-11-28 20:54:48

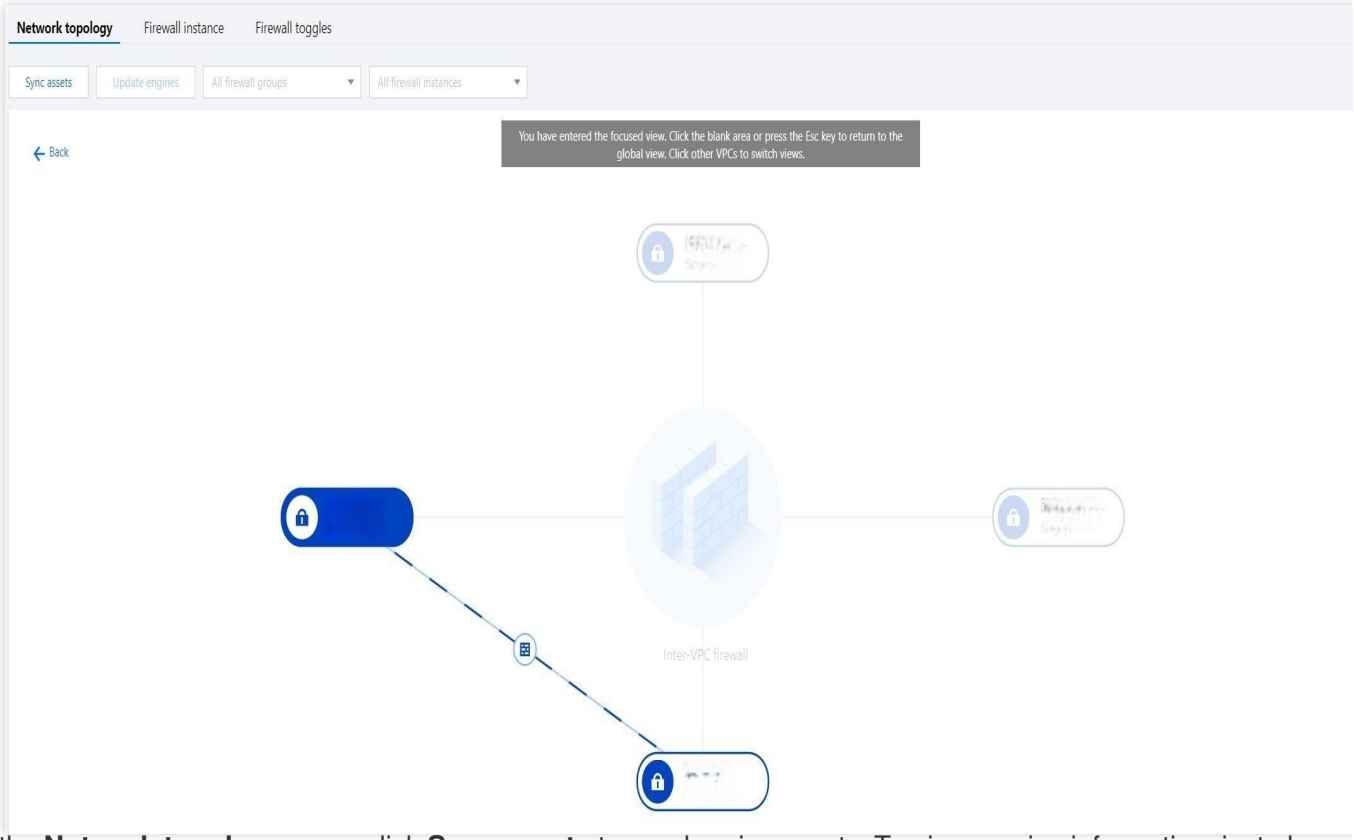
Viewing Network Topologies

Cloud Firewall provides a dashboard displaying the access relation between VPC assets.

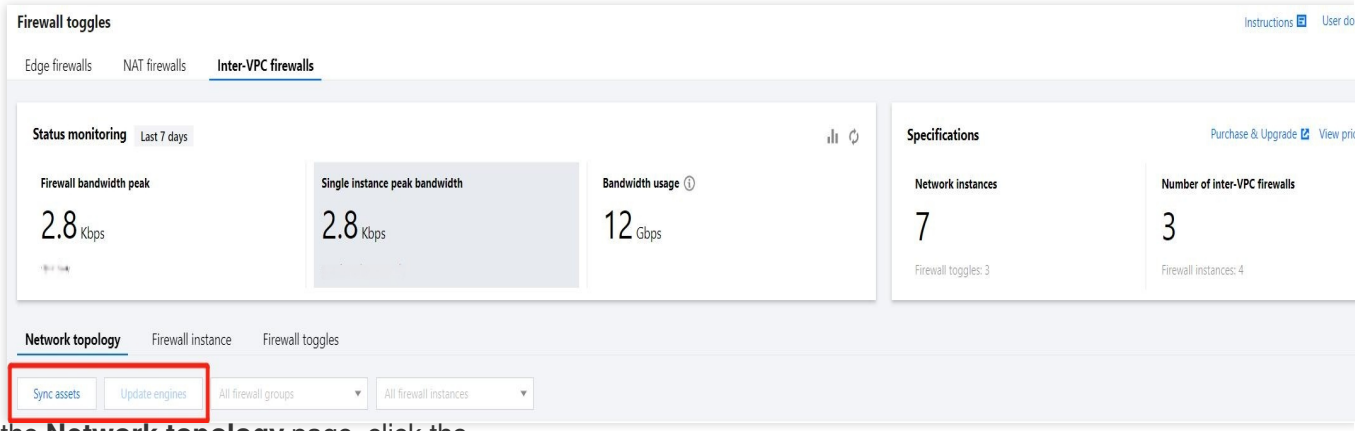
1. Log in to the Cloud Firewall console, and select **Firewall toggle** > **Inter-VPC toggle** in the left sidebar.
2. On the **Inter-VPC toggle** page, click **Network topology** to view associated VPC instances.
3. On the **Network topology** page, place the mouse over a VPC instance to show details.



4. Click this VPC instance to further view its connection with other VPC instances and the firewall toggle status. **A dark blue firewall toggle means it is turned on and a gray firewall toggle means it is turned off**.



5. On the **Network topology** page, click **Sync assets** to synchronize assets. To view version information, just place the mouse over **Update engines**.



6. On the **Network topology** page, click the

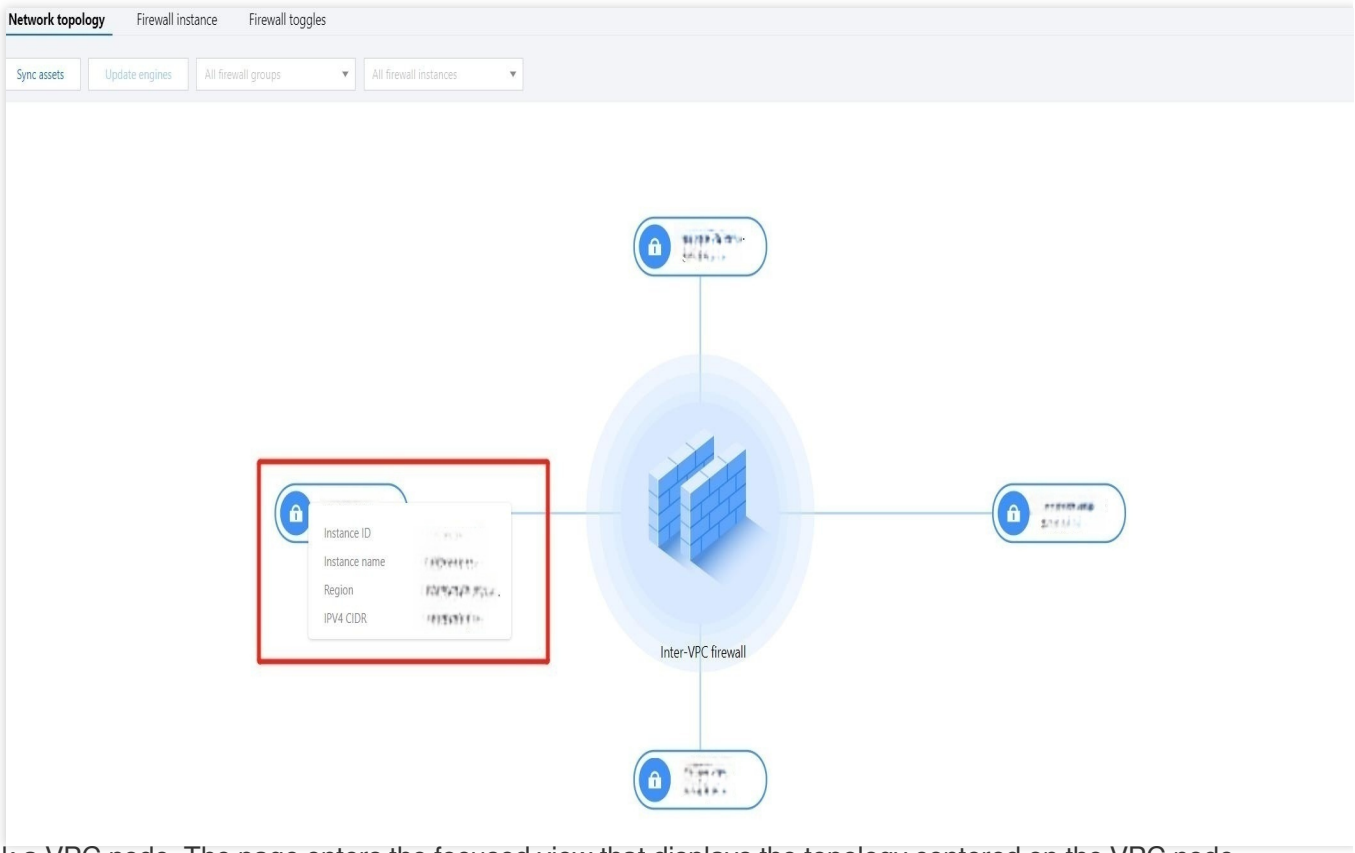
icon in the top right corner to view the operation guide, or click the

icon to refresh the network topology.

Viewing the Access Relation Between VPCs

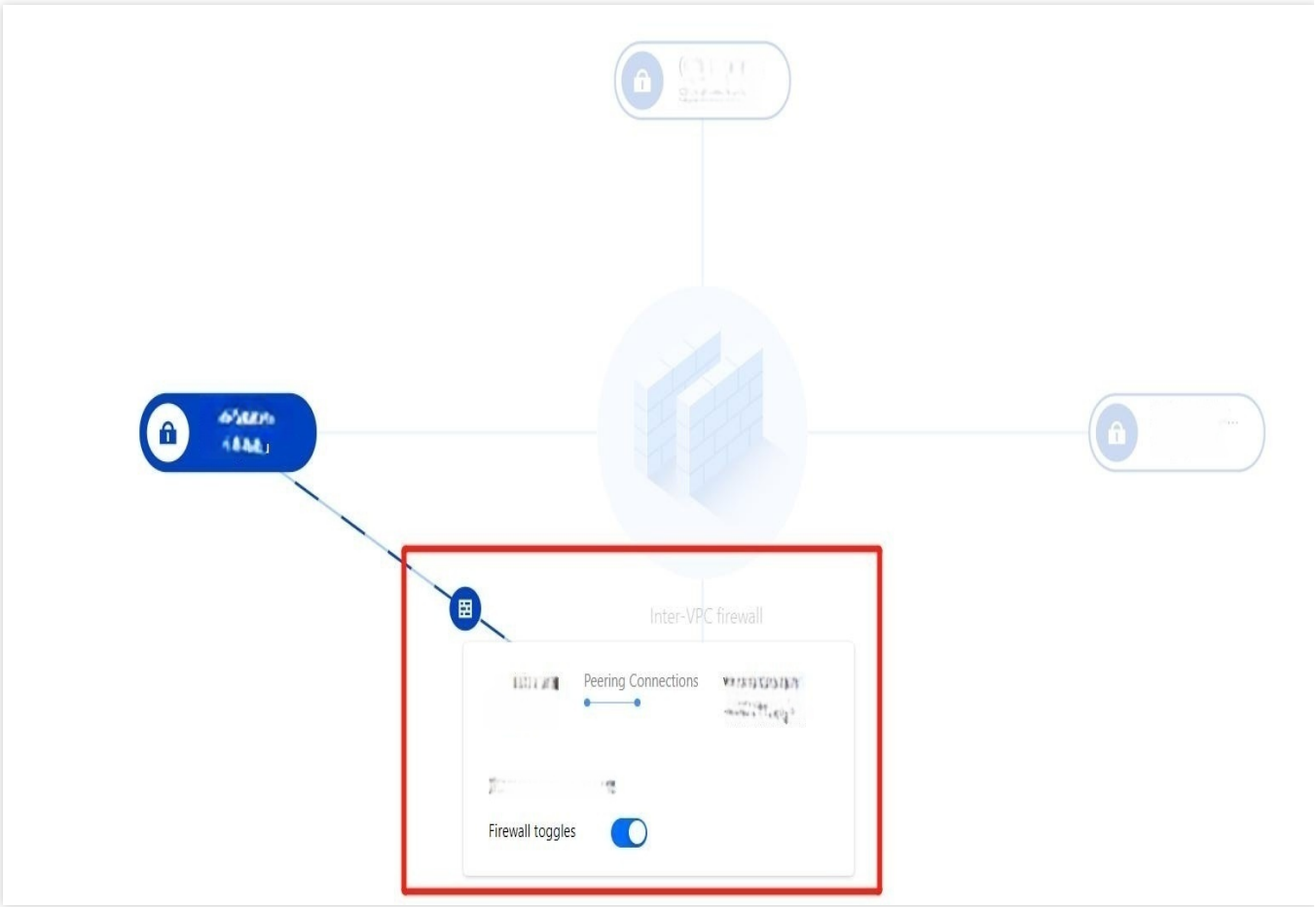
Cloud Firewall provides a dashboard displaying the access relation between VPC assets. In the VPC visualization view, each node represents a VPC instance protected by the inter-VPC firewall, which is a centralized device for inter-VPC firewall toggles. Each toggle controls different routes. Traffic between VPCs with firewall toggles turned on is directed to the firewall for filtering and protection.

1. Log in to the Cloud Firewall console, and select **Firewall toggle** > **Inter-VPC toggle** in the left sidebar.
2. On the **Inter-VPC toggle** page, click **Network topology** to view associated VPC instances.
3. Hover the mouse over a VPC node to view its brief details. All VPC nodes interconnected to it will light up. Click the **VPC ID** and the VPC details page opens.



4. Click a VPC node. The page enters the focused view that displays the topology centered on the VPC node.
5. Interconnected VPCs are linked via a connection line, with a firewall toggle lying in the middle that can be managed as needed. You can click the

icon to go to the page for configuring access control rules.



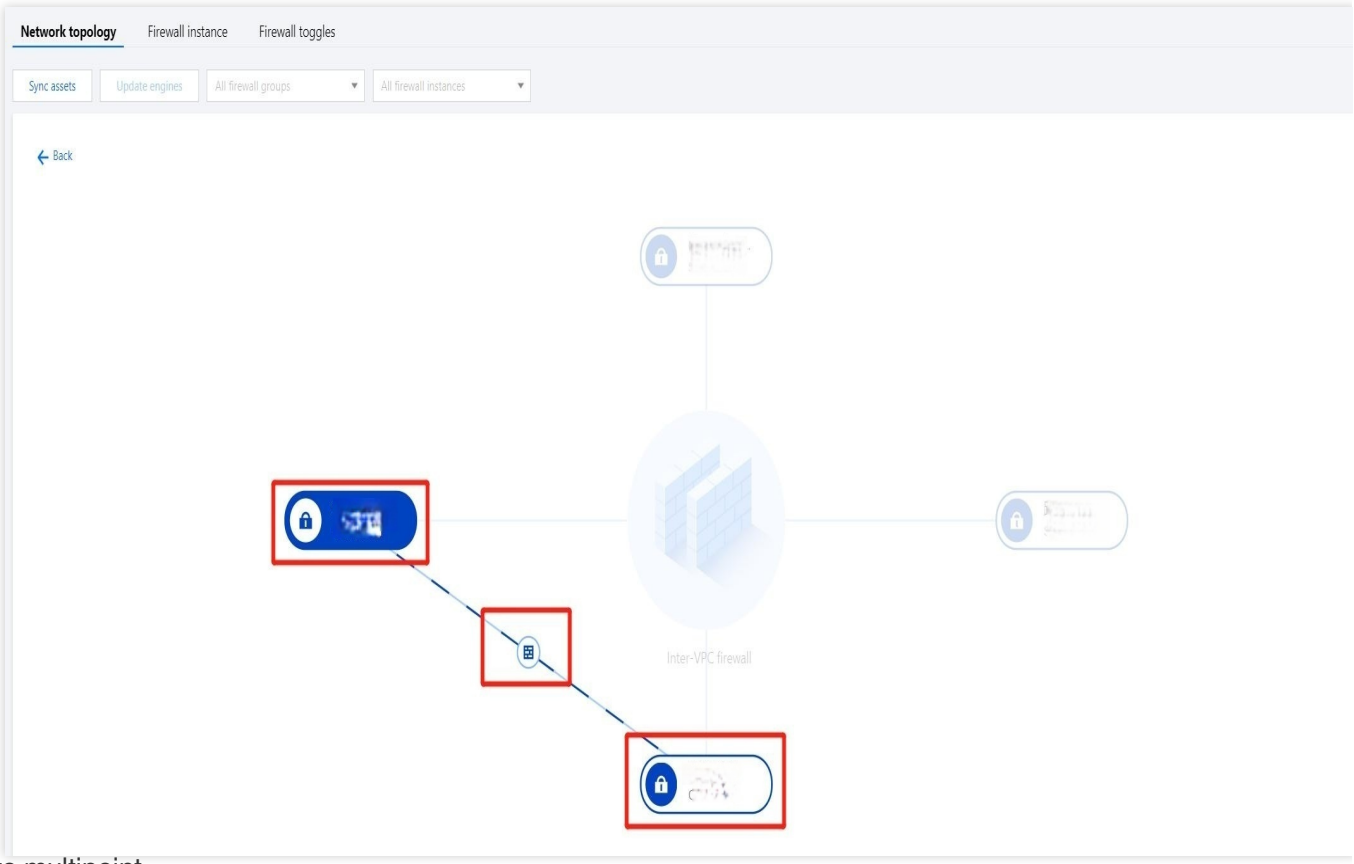
Important

In the "Point to point" mode, each pair of interconnected VPCs has only one firewall toggle.

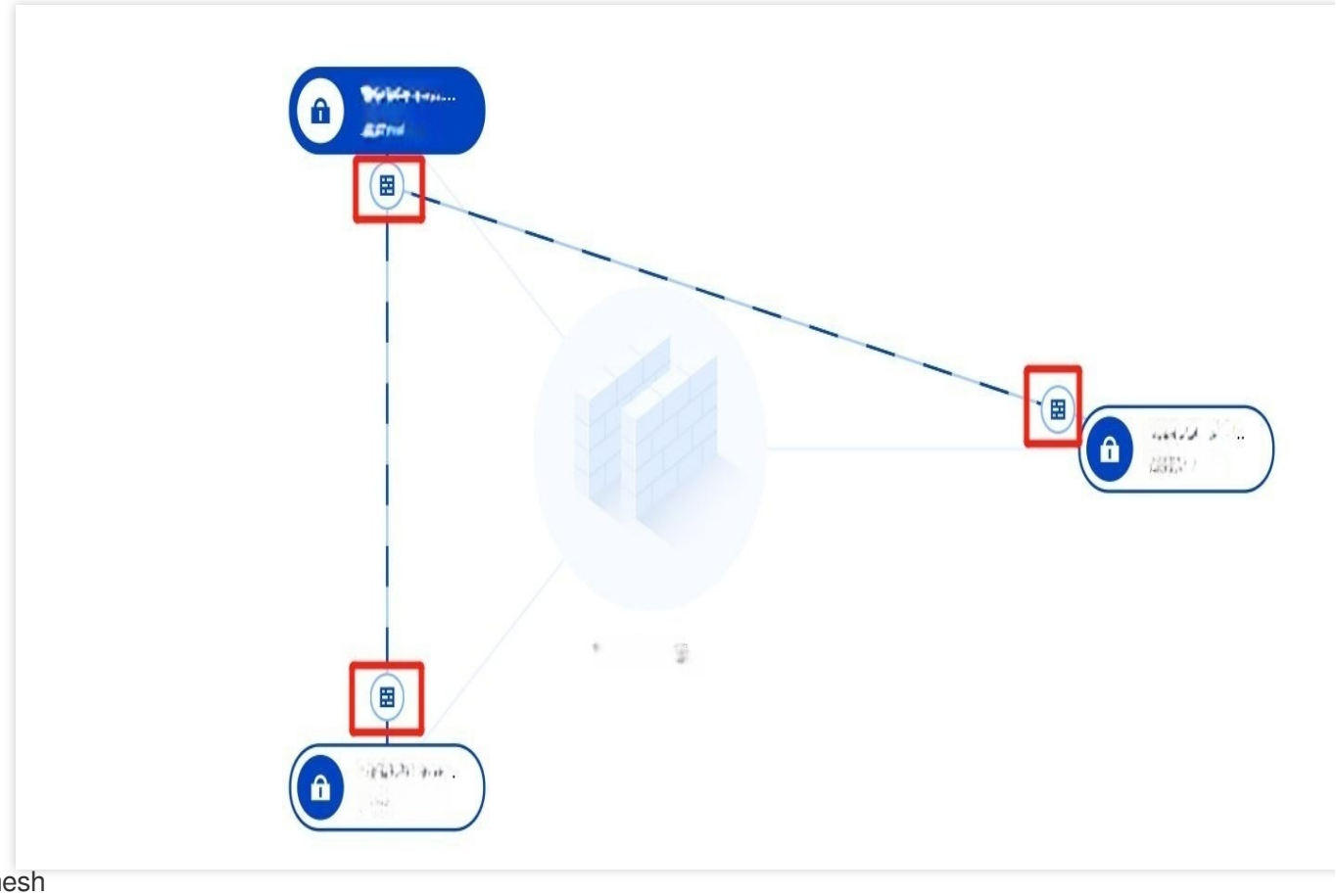
In the "Point to multipoint" mode, each VPC has one firewall toggle.

In the "Fullmesh" mode, all VPCs has only one firewall toggle.

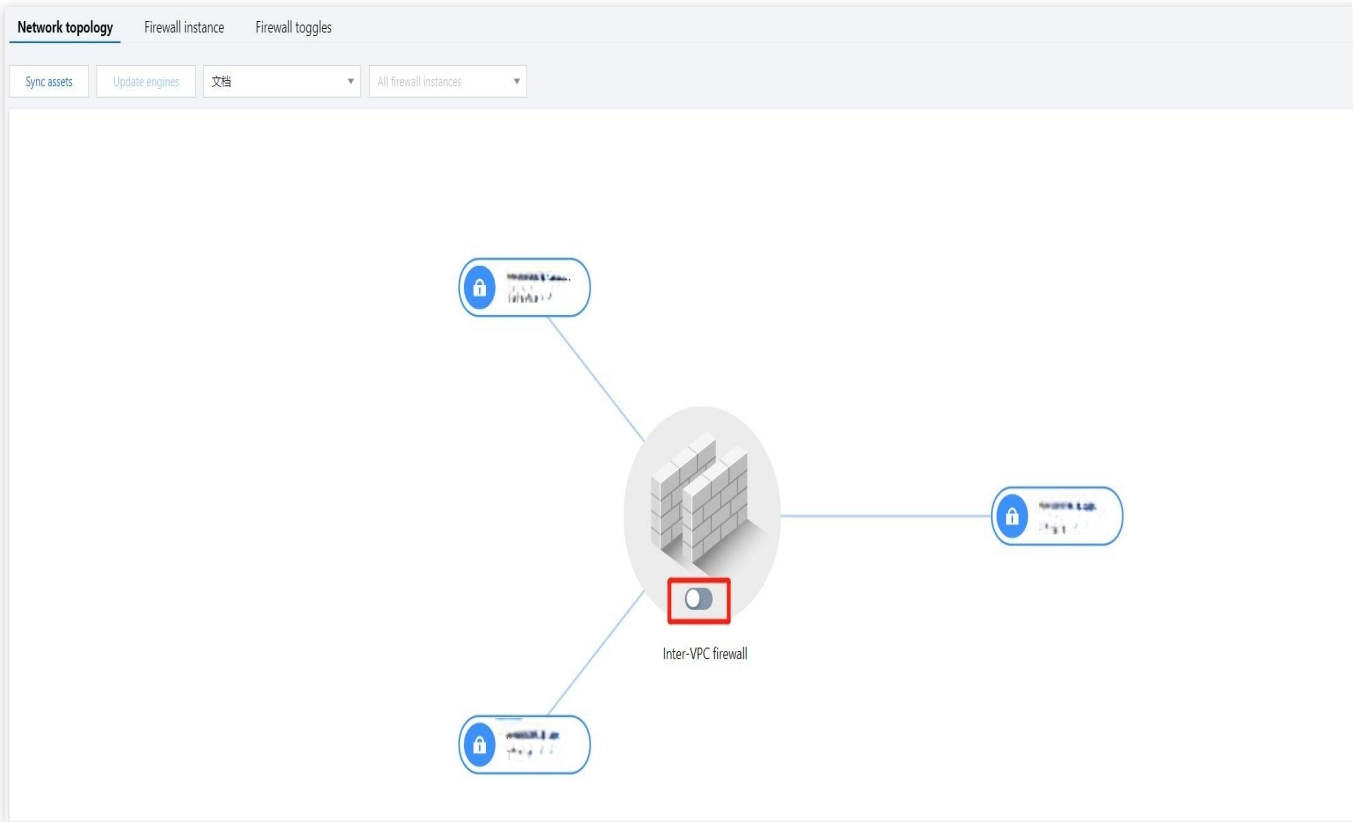
Point to point



Point to multipoint



Fullmesh


Network topology
Firewall instance
Firewall toggles
Sync assets
Update engines
文档
All firewall instances
Inter-VPC firewall

Configuring Custom Routes

Overview

Last updated：2023-11-28 20:23:18

When an inter-VPC firewall is set to **Custom route**, a custom route can be created to suit your needs.

Important:

Before using this mode, make sure that CFW has been connected to the classic network through peering connections or CCN instances.

Concepts

Firewall instance

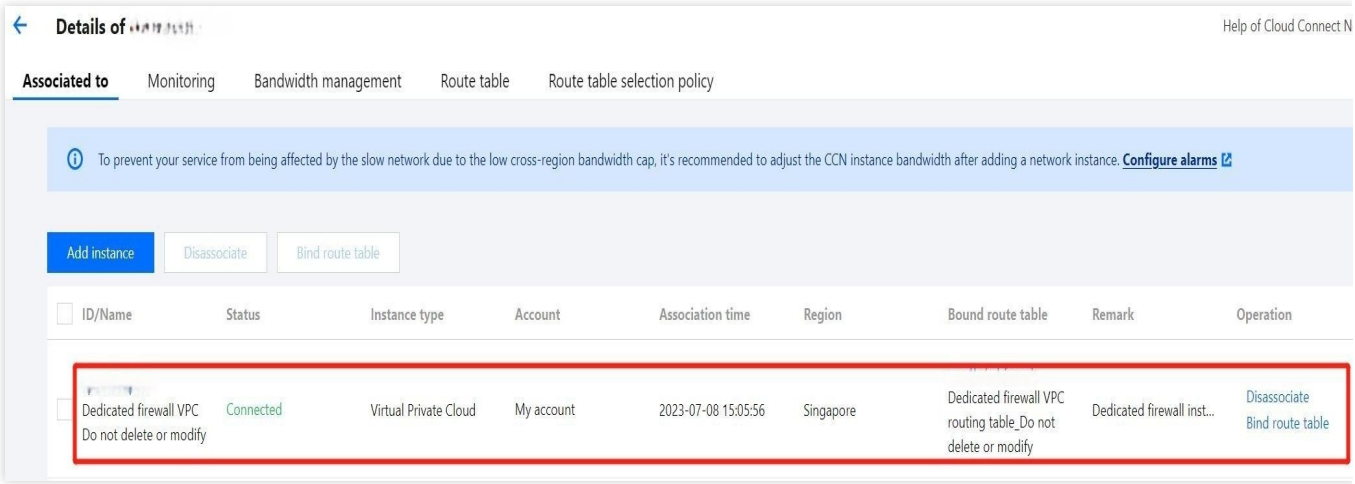
Similar to CVM, it is a virtualized instance that can perform all features of a firewall. View more details in the CFW console.

Firewall VPC (CCN mode)

A VPC that is created by CFW in CCN can direct user network traffic to firewall instances, so as to enable protection. Such VPC is named "Firewall VPC_DO NOT MODIFY". Go to the CCN instance details page and view more details.

Notes

A firewall VPC will be created in each region to handle traffic. Please do not modify it.

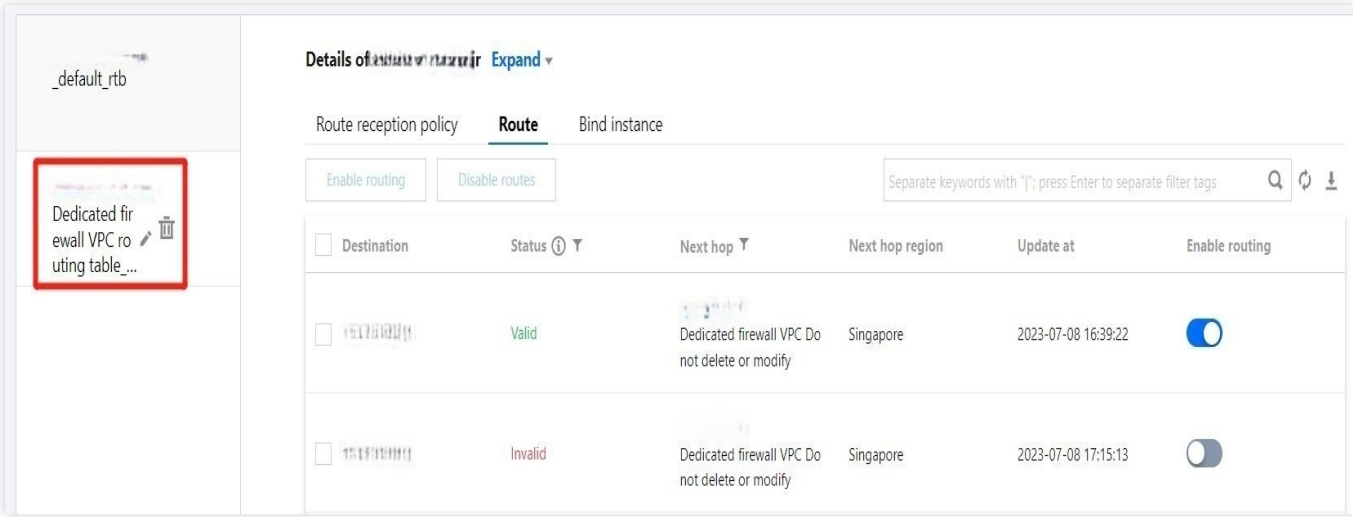


Firewall route table (CCN mode)

A route table that is automatically created by CFW can distribute traffic. Such route table is named "Firewall VPC route table_DO NOT MODIFY".

Important

A firewall route table will be created in each region. Please do not modify it.

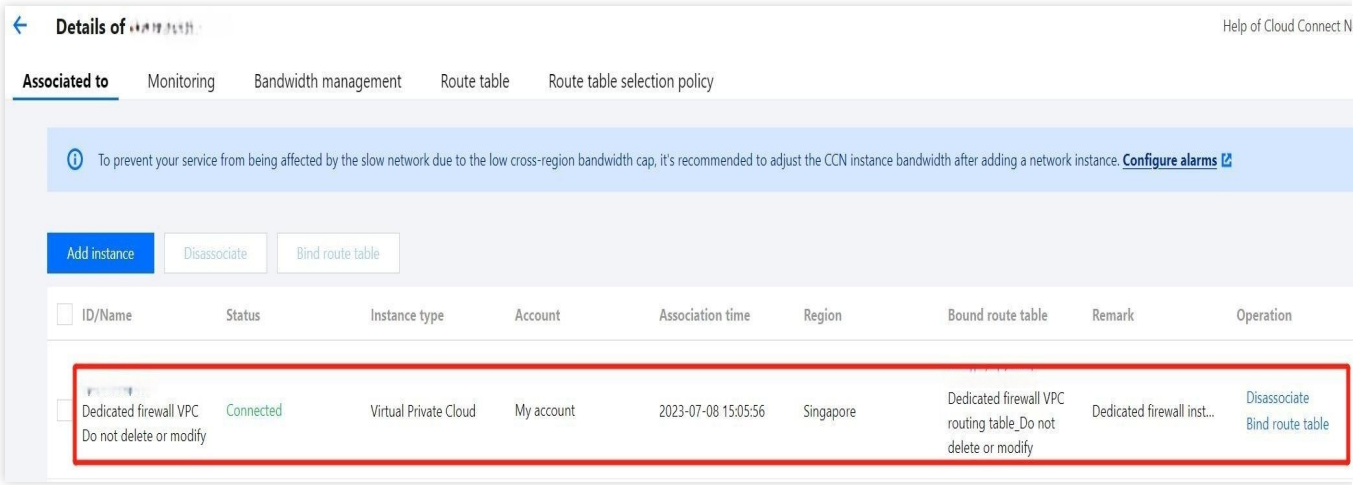


Firewall VPC

A VPC that is created by CFW in CCN can direct user network traffic to firewall instances, so as to enable protection. Such VPC is named "Firewall VPC_DO NOT MODIFY". Go to the CCN instance details page and view more details.

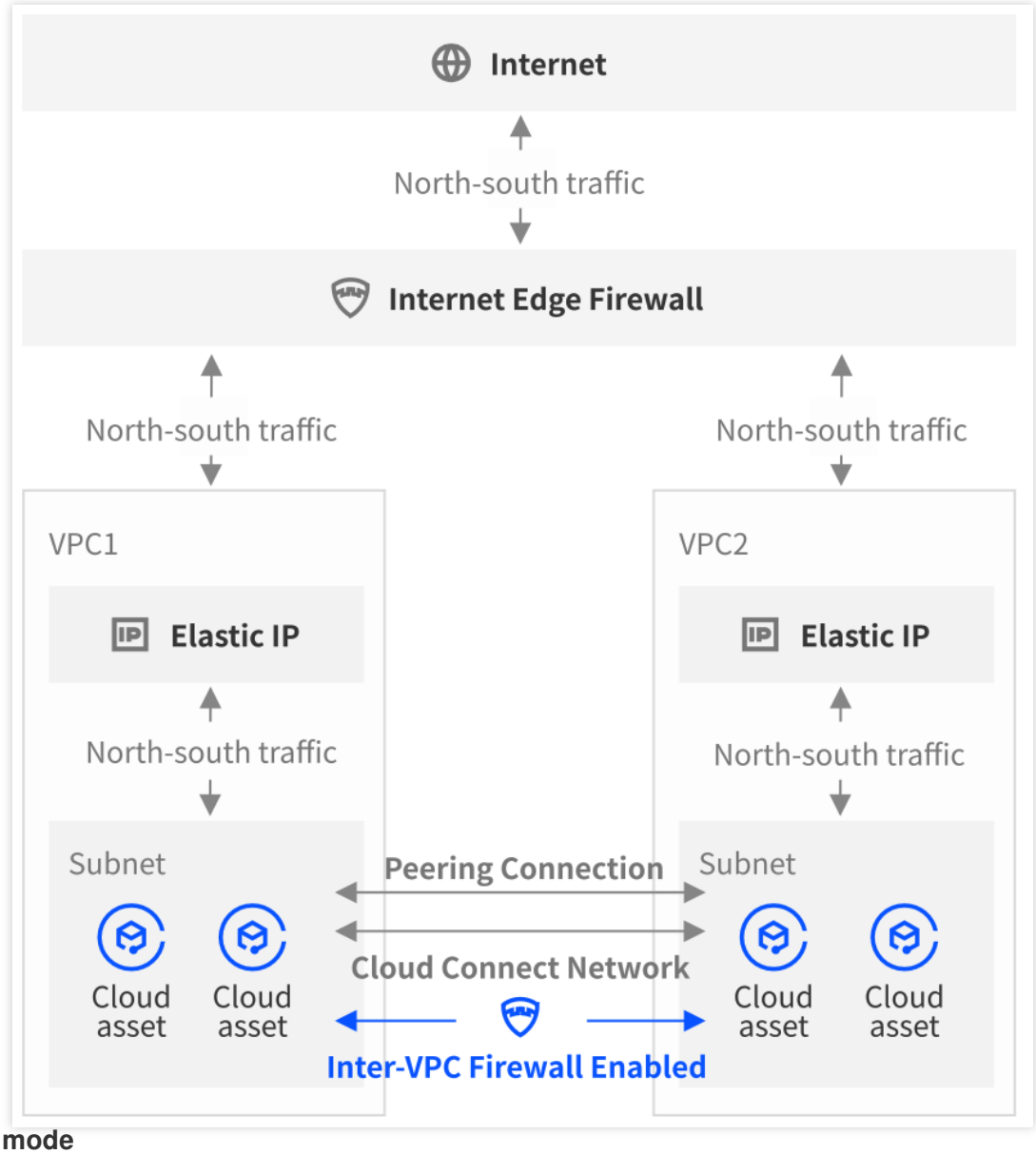
Notes

A firewall VPC will be created in each region to handle traffic. Please do not modify it.



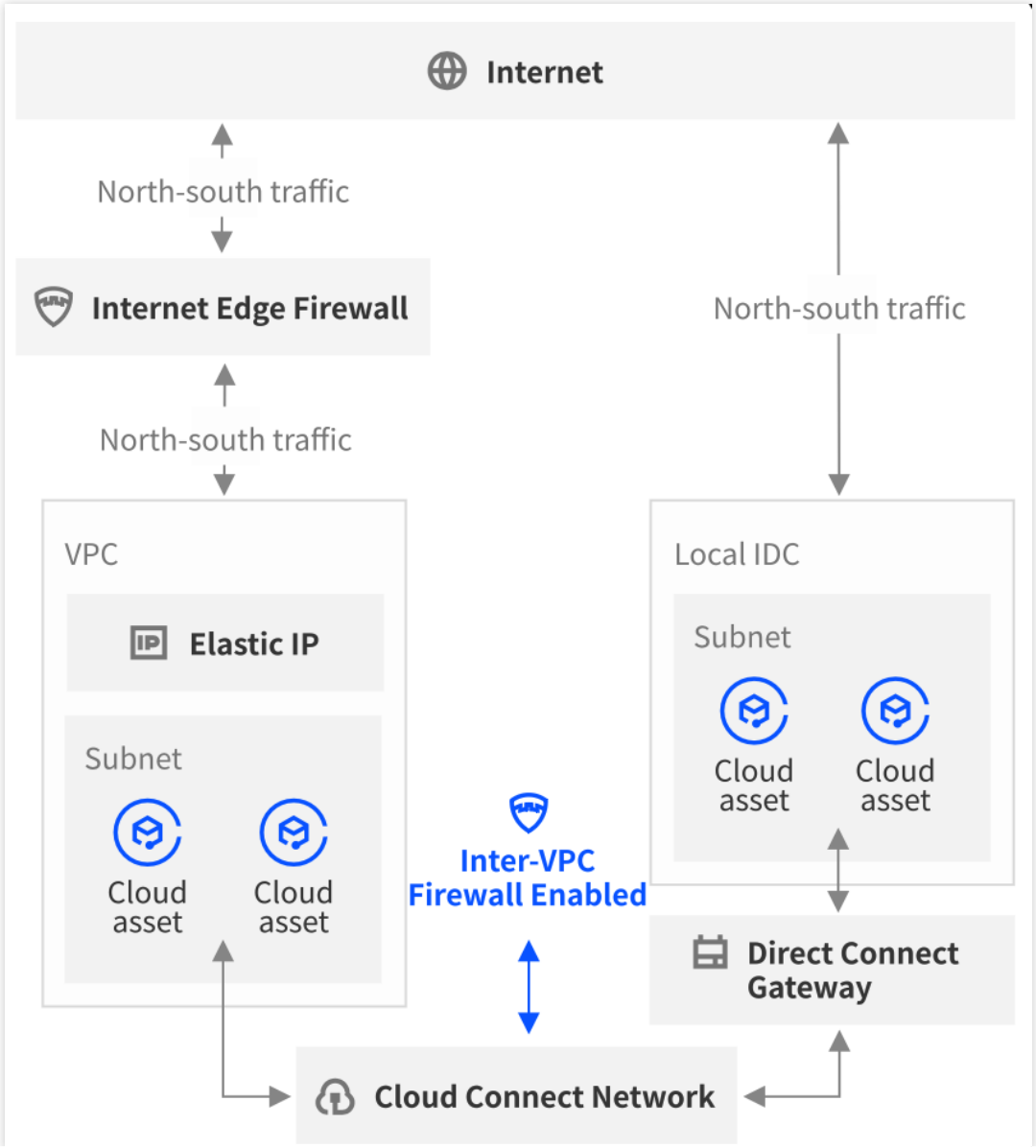
Working Mode

VPC mode



CCN mode

In this mode where the inter-VPC firewall and all service VPCs are connected to the same CCN instances, service traffic is directed via a firewall VPC subnet.


Internet
North-south traffic
Internet Edge Firewall
North-south traffic
North-south traffic
VPC
Elastic IP
Subnet
Cloud asset
Cloud asset
Inter-VPC Firewall Enabled
Local IDC
Subnet
Cloud asset
Cloud asset
Direct Connect Gateway
Cloud Connect Network

VPC Mode

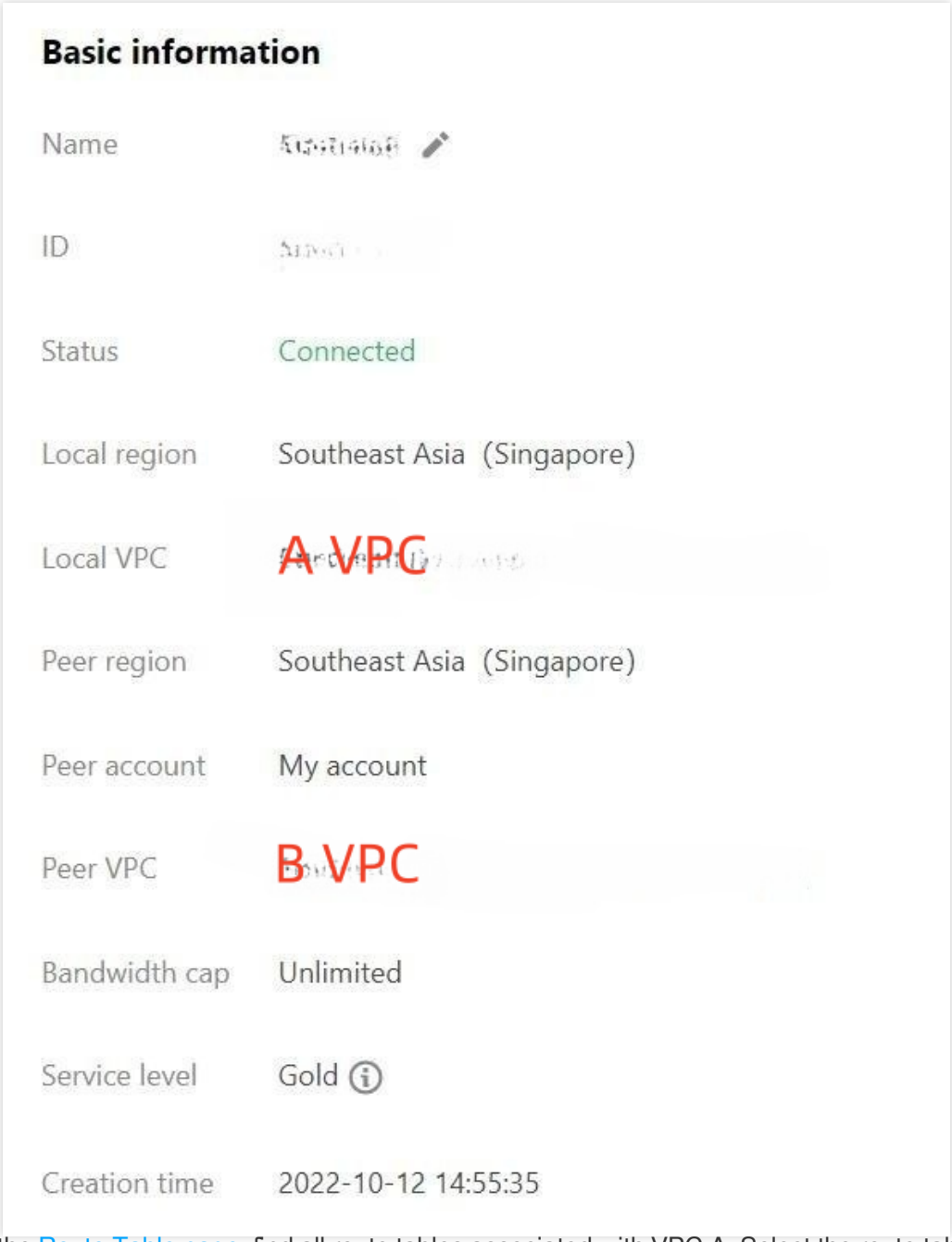
Last updated：2023-11-28 20:25:44

Step 1. Creating an Instance with Custom Route

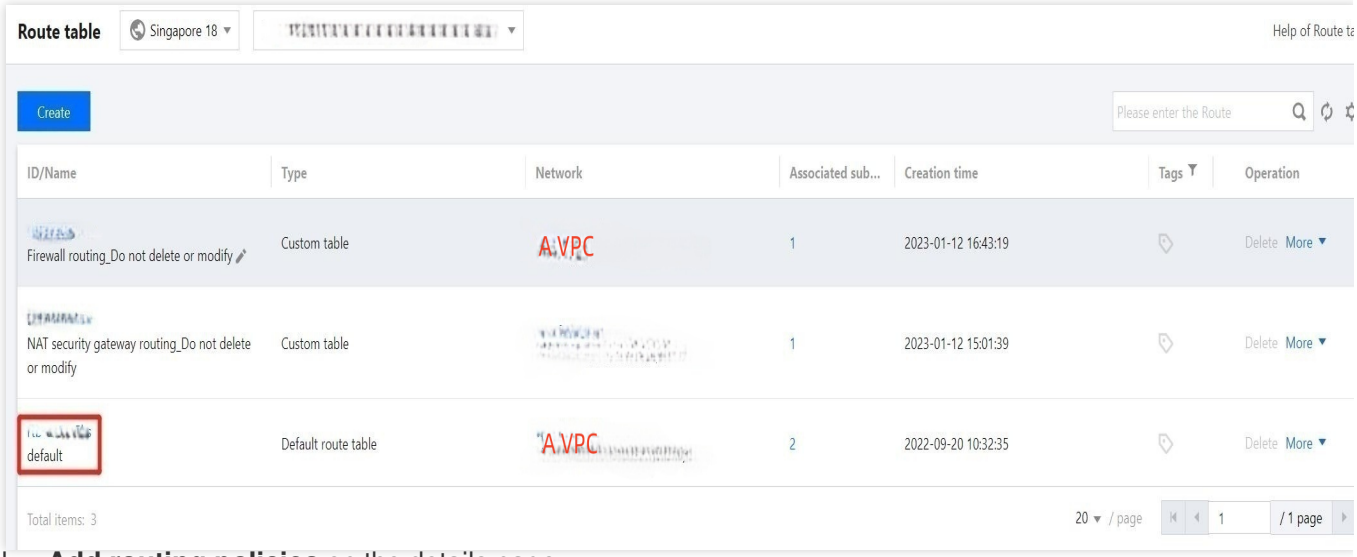
Create an instance as instructed by Creating Inter-VPC Firewalls. Select **Custom route** for the route mode.

Step 2. Configuring the Forwarding Route

1. View the two peered VPCs, namely VPC A and VPC B.

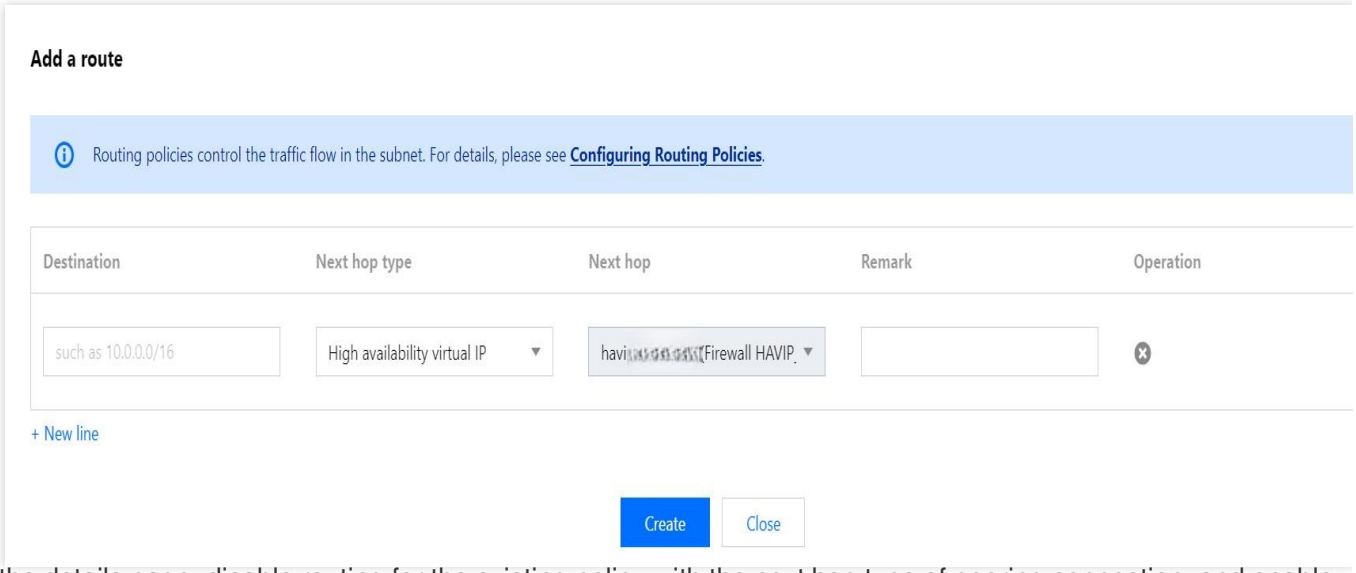


2. On the Route Table page, find all route tables associated with VPC A. Select the route table named "default" by clicking its ID.



3. Click **+ Add routing policies** on the details page.

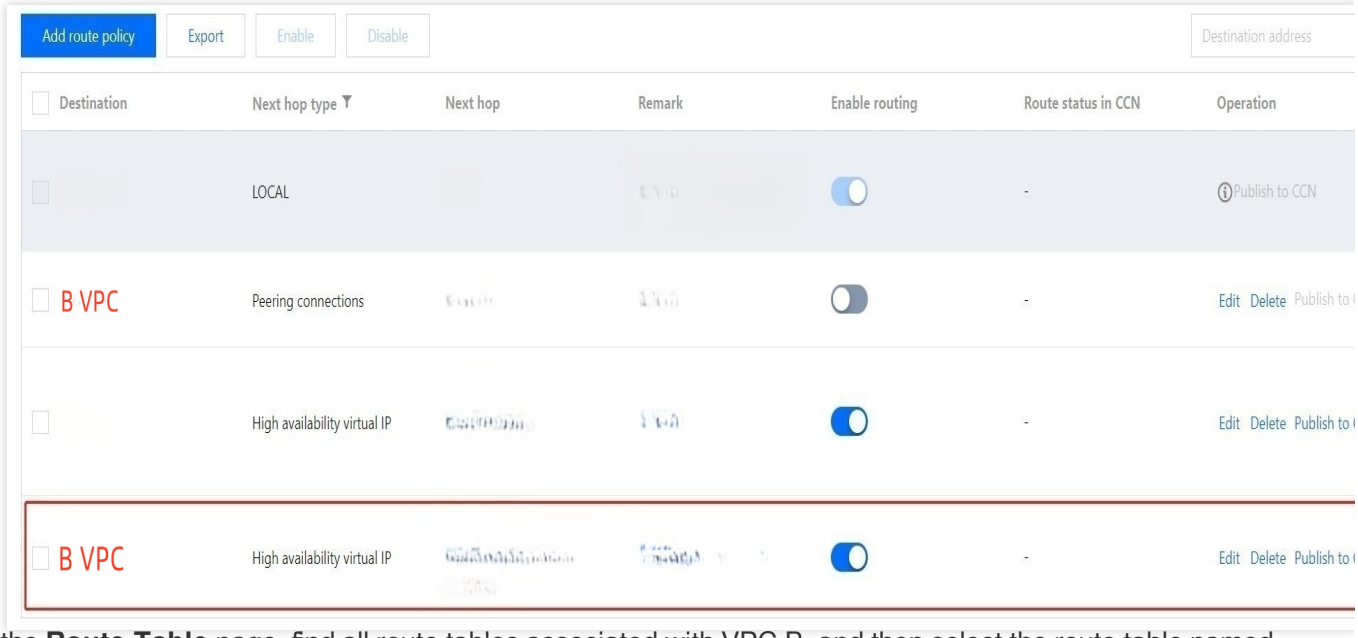
4. In the pop-up window, enter the subnet of VPC B for **Destination**, select **HAVIP** for **Next hop type**, and click **Create**.



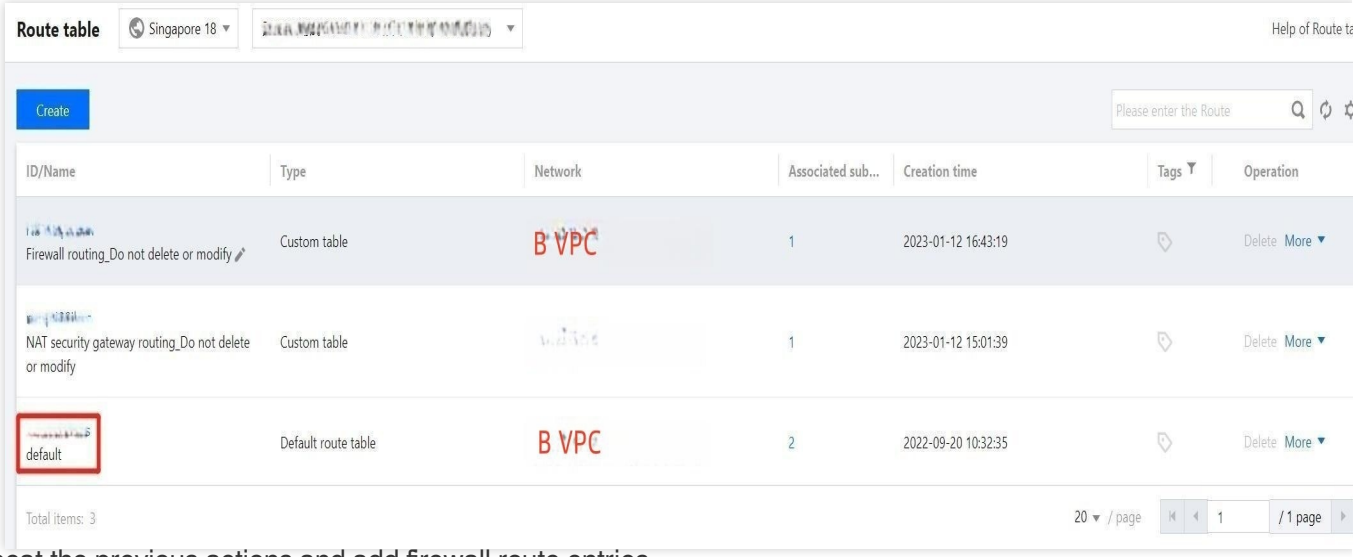
5. On the details page, disable routing for the existing policy with the next hop type of peering connection, and enable routing for the new policy.

Important

Switching routes may cause network interruptions. It is recommended to operate during off-peak hours.



6. On the **Route Table** page, find all route tables associated with VPC B, and then select the route table named "default" by clicking its ID.



7. Repeat the previous actions and add firewall route entries.

Step 3. Verifying the Firewall

1. For information about accessing traffic logs, see Log Audit.
2. For information about verifying the intrusion defense configuration, see Log Audit.
3. Configure private network rules and ensure they are hit normally.

Now the firewall should work properly. For detailed route solutions, or if you have any other questions, please submit a ticket.

CCN Mode

Last updated：2023-11-28 20:27:56

Step 1. Creating an Instance with Custom Route

Create an instance as instructed by Creating Inter-VPC Firewalls. Select **Custom route** for the route mode.

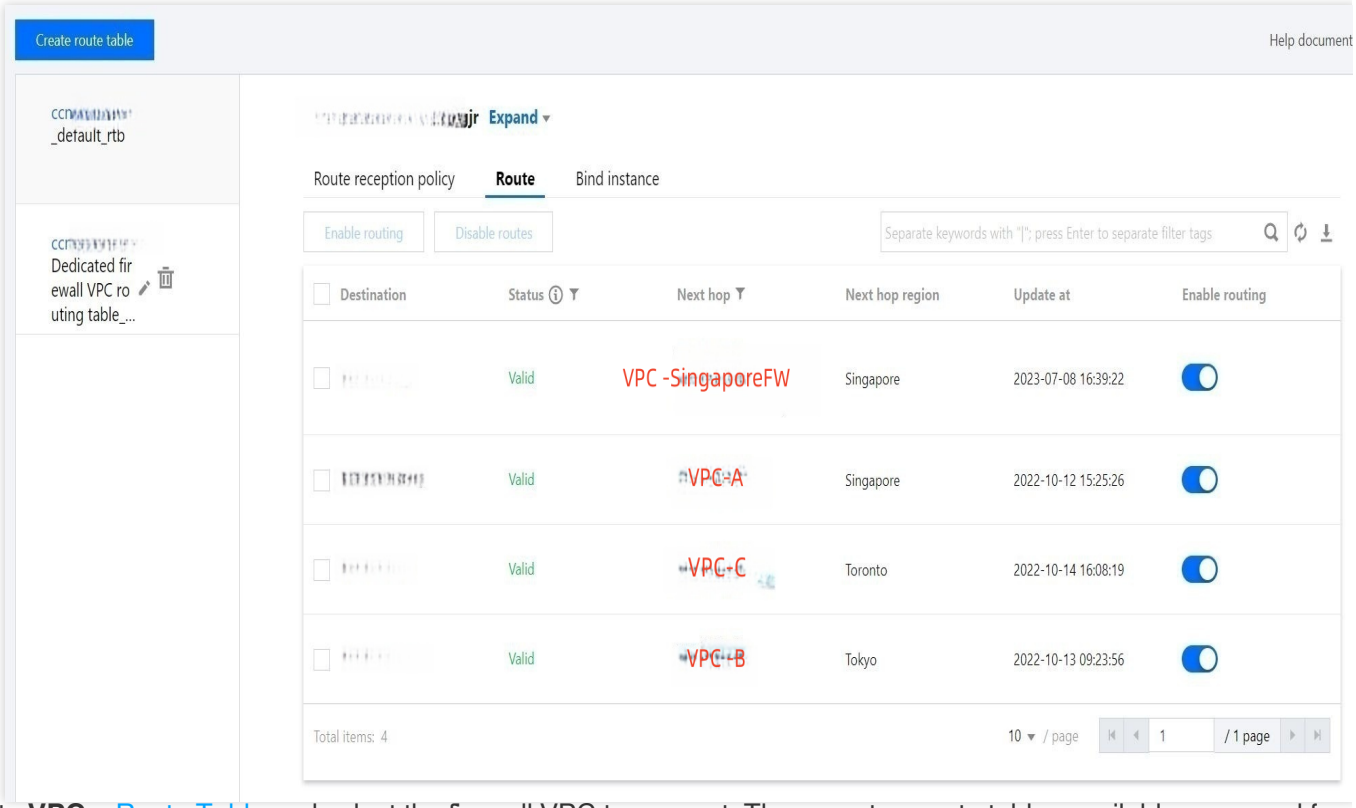
Step 2. Configuring the Forwarding Route

This is to forward the traffic going to the VPC where the customer service is deployed to the firewall instance through the firewall gate.

1. Go to the console where you associate a CCN instance to the created inter-VPC firewall instance and view the CCN instance details.
2. Make sure that the firewall VPC and related route tables have been created. If not, wait until they are prepared or submit a ticket.
3. Open the route table page and select the service VPC and firewall VPC to connect.

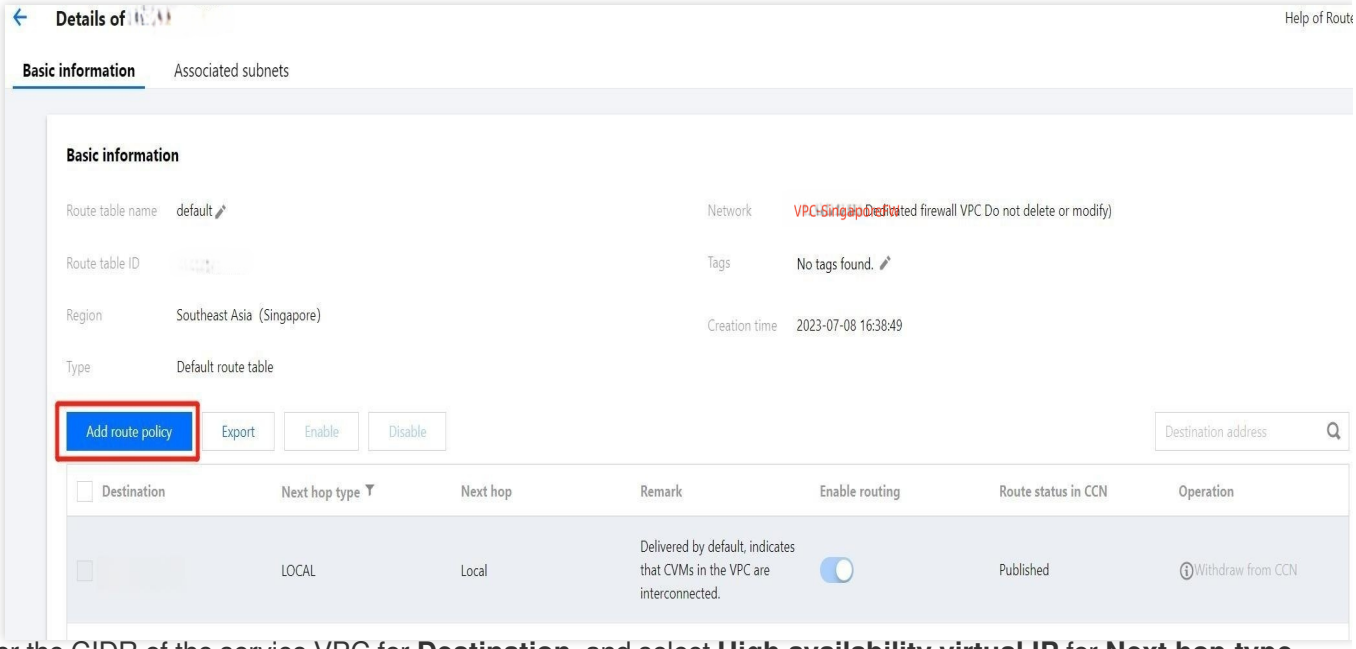
Notes

To give a clear illustration, take Beijing-based service VPC-A, Chongqing-based service VPC-B and Beijing-based firewall VPC-BJFW as examples.

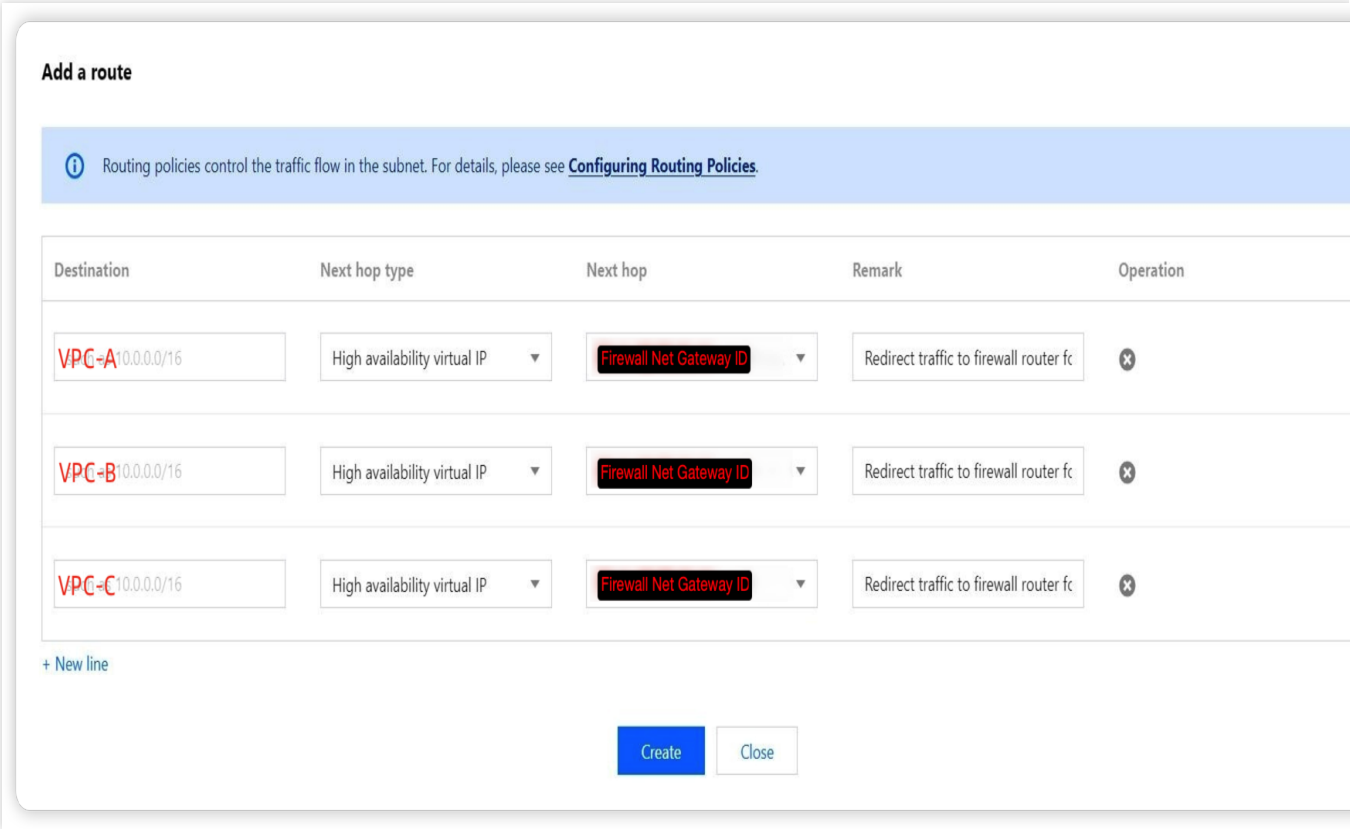


4. Go to **VPC** > Route Table and select the firewall VPC to connect. There are two route tables available, one used for the firewall VPC and that cannot be modified, the other named "default". Select the route table named "default" to edit.

5. Click **Add routing policies**. The policies you add can direct the next hop of the service VPC to the firewall.



6. Enter the CIDR of the service VPC for **Destination**, and select **High availability virtual IP** for **Next hop type**, and **Firewall gateway ID** for **Next hop**. **Notes** is optional.



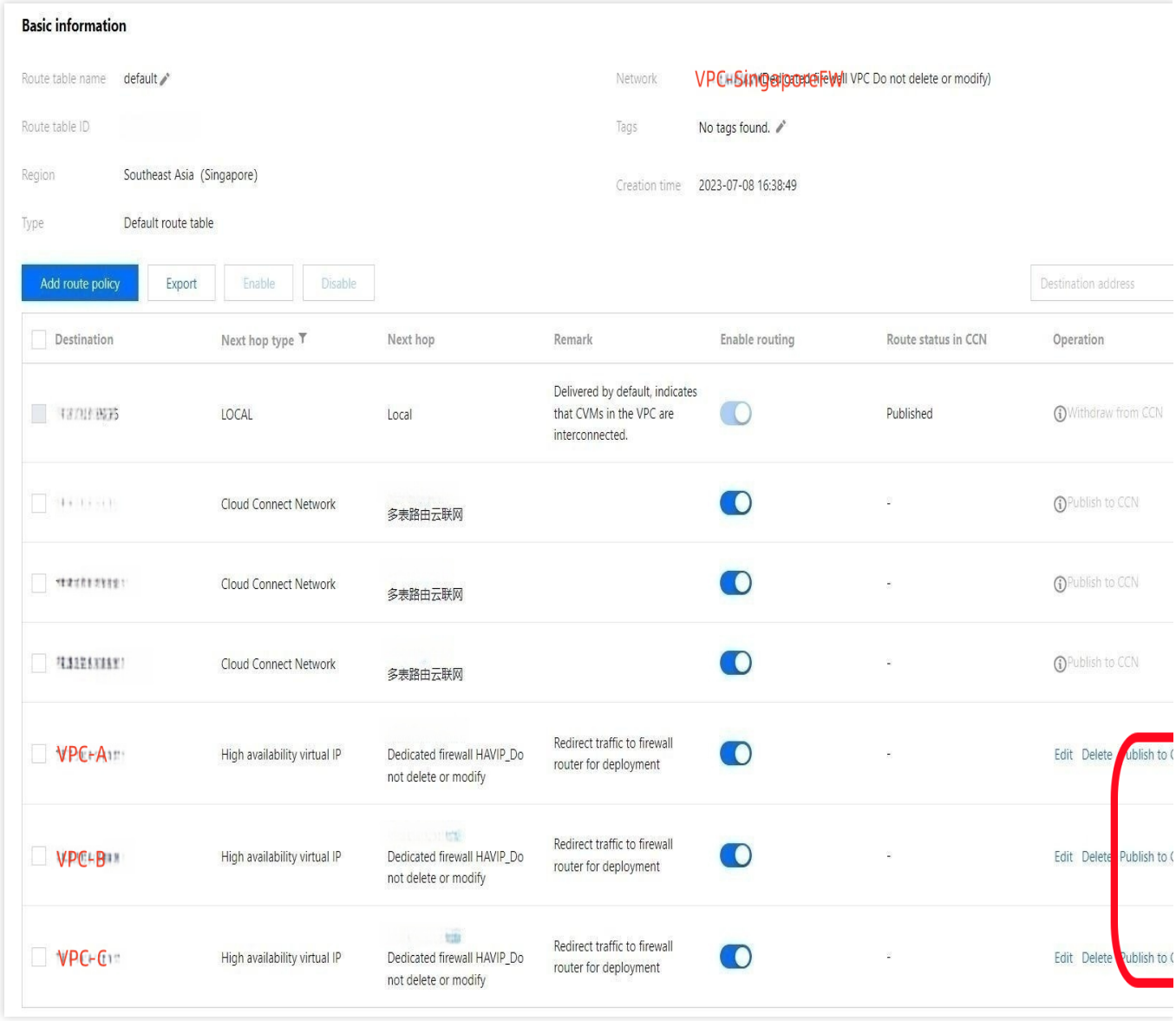
Notes

If you see the message "The specified CIDR forms ECMP", disable related routes in the default route table first.

7. Publish the newly added routing policies to CCN. For more details, see Managing Routing Policies. After that, these policies can be viewed in the default routing table in the corresponding CCN instance.

Notes

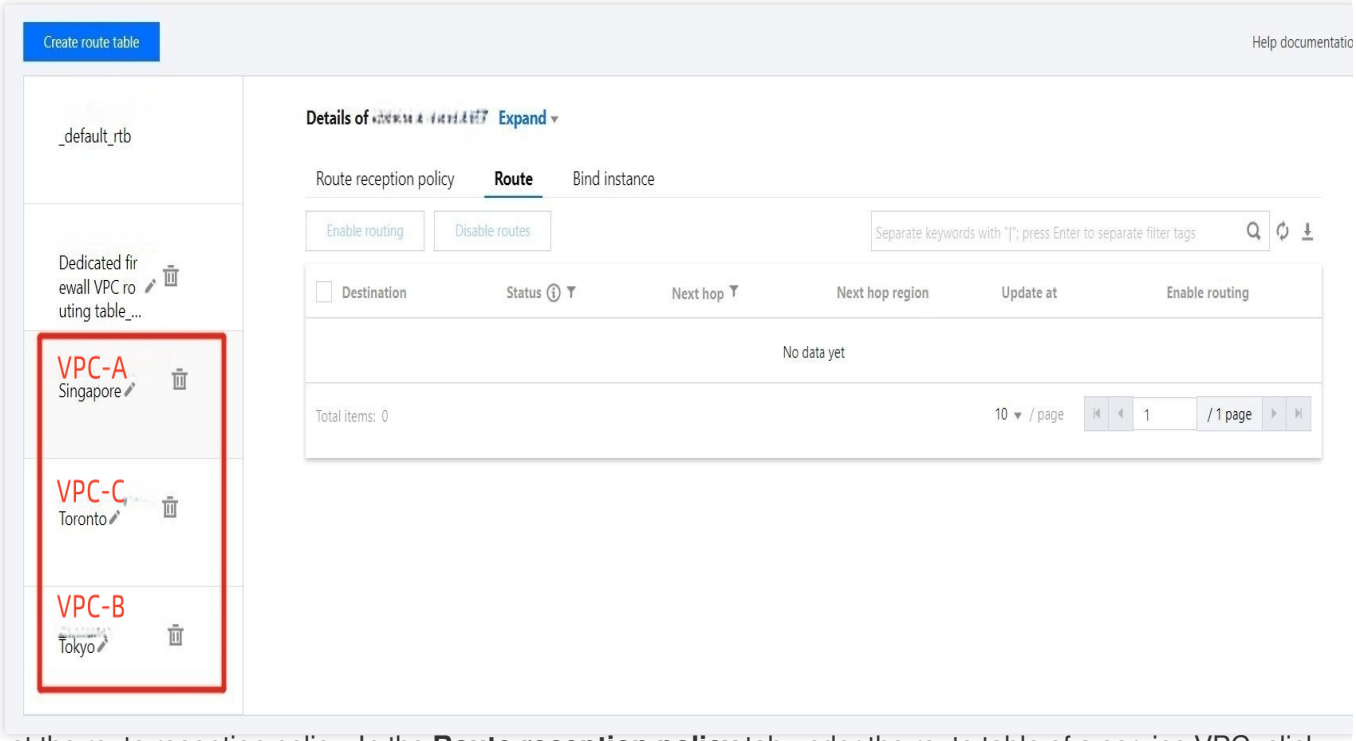
A new routing policy will override the original one.



Step 3. Creating a Route Table to Connect Service VPCs

The purpose is to build connectivity between firewall networks and customer networks.

1. On the CCN page, create a route table for each service VPC.

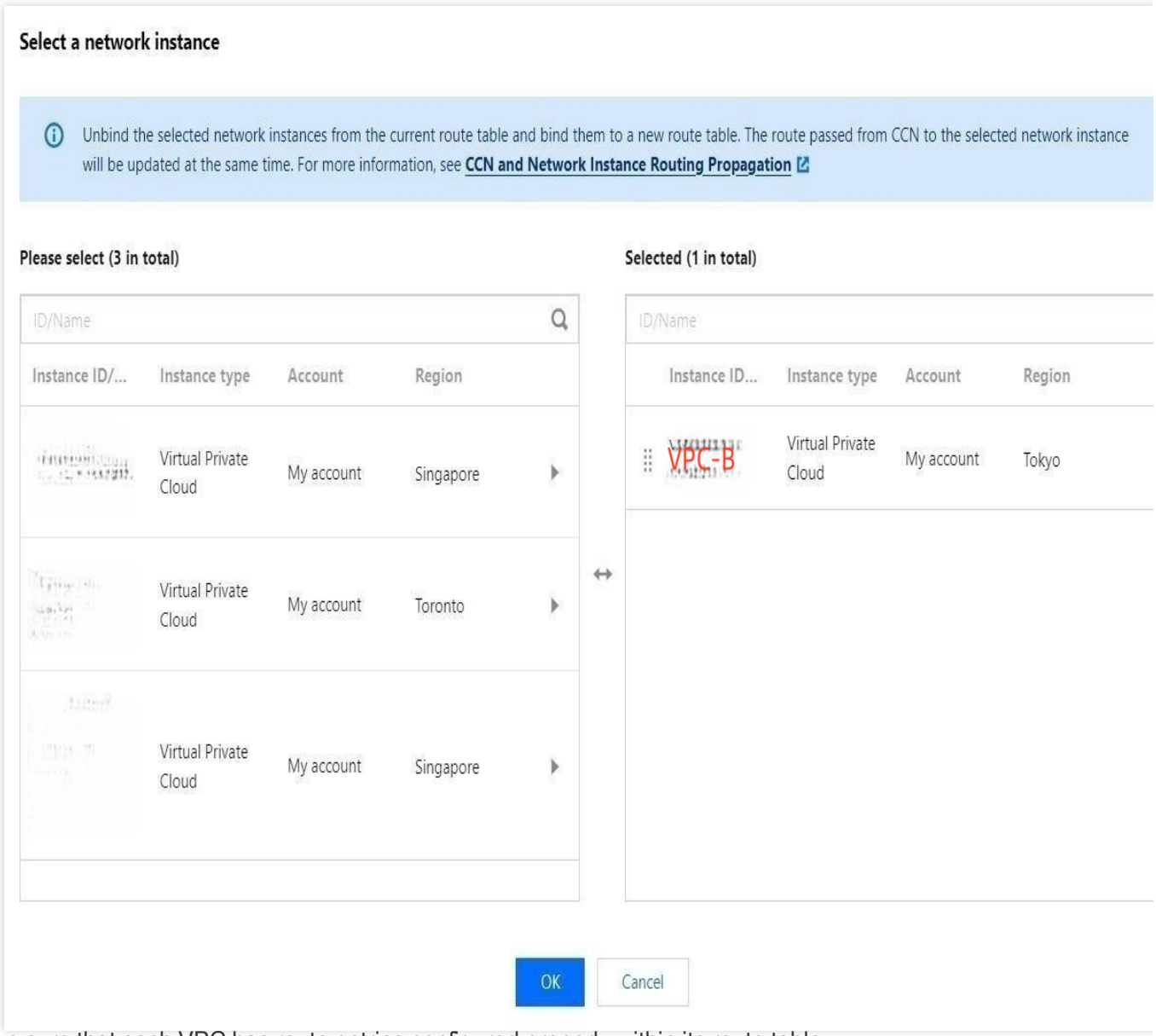


2. Adjust the route reception policy. In the **Route reception policy** tab under the route table of a service VPC, click **Add network instance** to add its associated VPC instance and interconnected VPC instance.

Important

VPC instances associated with route tables and those unprotected by the firewall must be added first.

Example: Assuming that VPC-C is the service VPC unprotected by the firewall instance, you should first add VPC-A and VPC-C to the route table of VPC-A. Repeat the above operations and then add VPC -BJFW.



3. Make sure that each VPC has route entries configured properly within its route table.

4. Bind network instances. In the **Bind instance** tab under the route table of a service VPC, click **Bind network instance** to bind network instances to the route table. After that, the network traffic will be directed to the firewall.

Important

Be sure to set the routes properly before binding the route table.

Step 4. Verifying the Firewall

1. For information about accessing traffic logs, see Log Audit.

2. For information about checking intrusion defense, see Log Audit.

Important

In the **Custom route** mode, the protection mode set in Intrusion Defense cannot be adjusted individually.

3. Configure internal rules and check whether they are hit normally.

Now the firewall should work properly. If your network structure is too complex or involves the application of Direct Connect, get a route solution by submitting a ticket. For further questions, contact us in the same way.

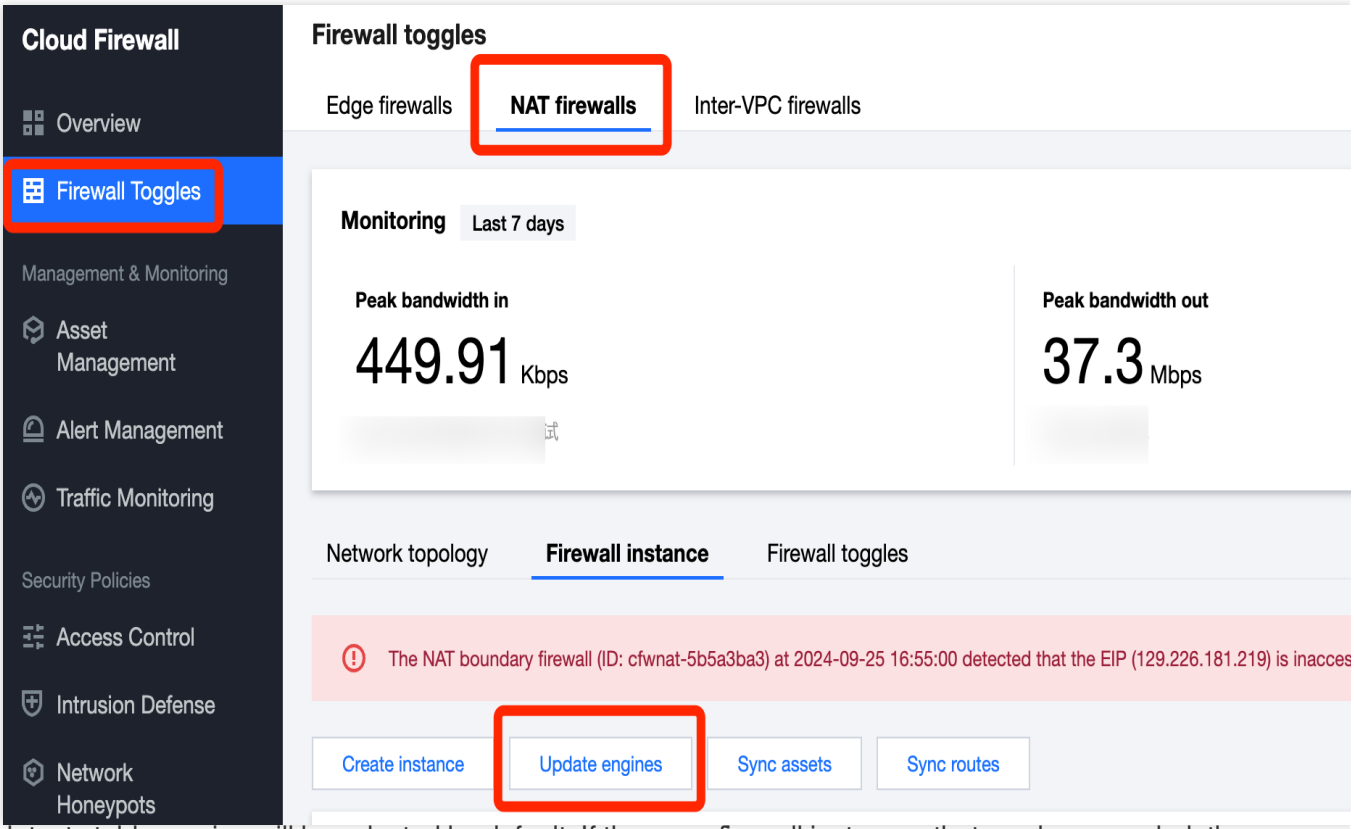
Firewall Engine Upgrade

Last updated：2024-11-01 10:37:54

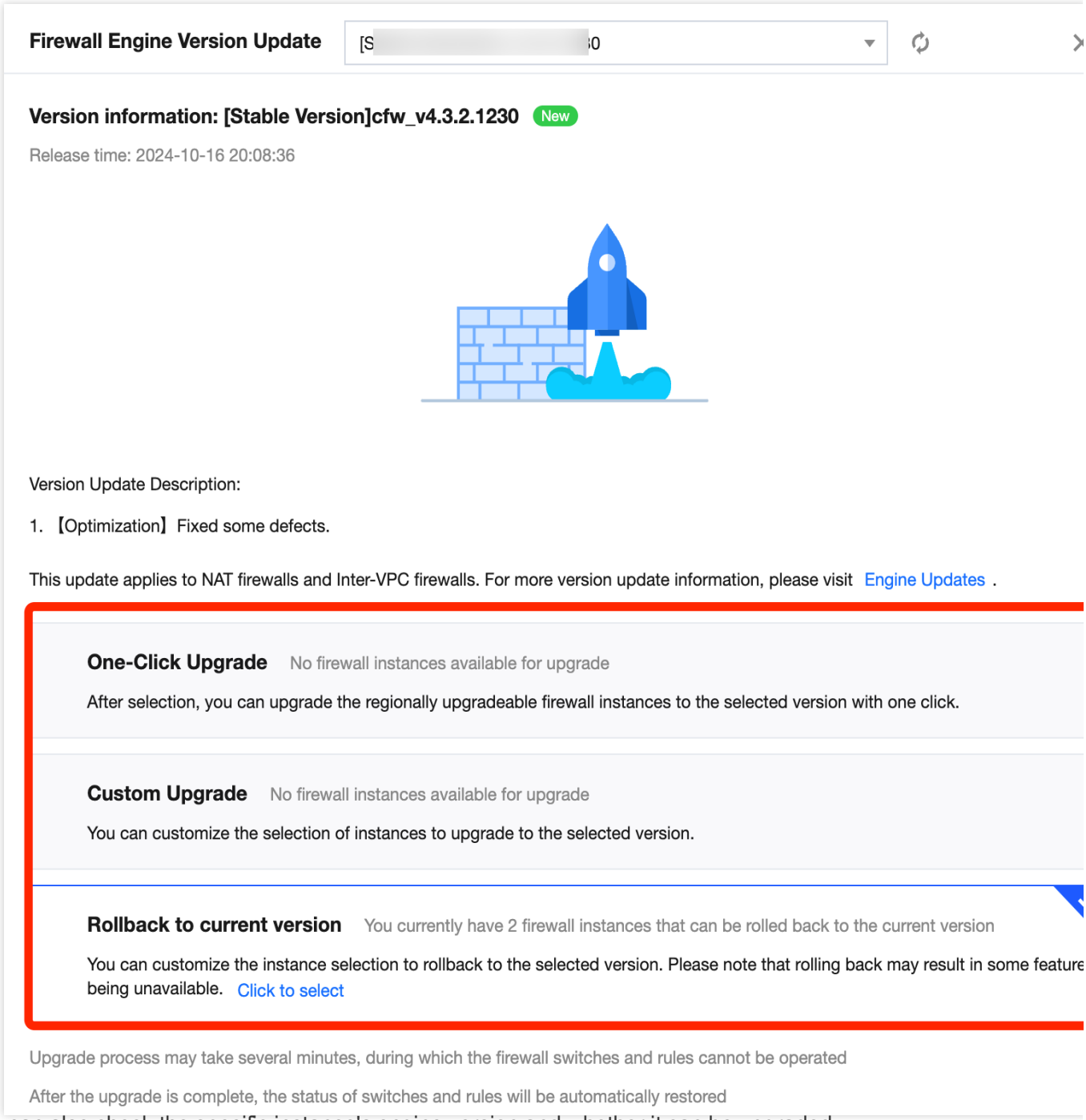
The NAT Firewall and the Inter-VPC Firewall are privately deployed, with their engines exclusively owned by tenants. Therefore, users need to manually update engines. The following is the upgrade operation guide.

Querying the Firewall Instances That Can Be Upgraded

1. Log in to the CFW Console, and choose **Firewall Toggles** > **NAT firewalls**/**Inter-VPC firewalls** in the left sidebar.
2. On the firewall instance page, click Engine Update to check the latest version of the engine and the instances that can be upgraded.

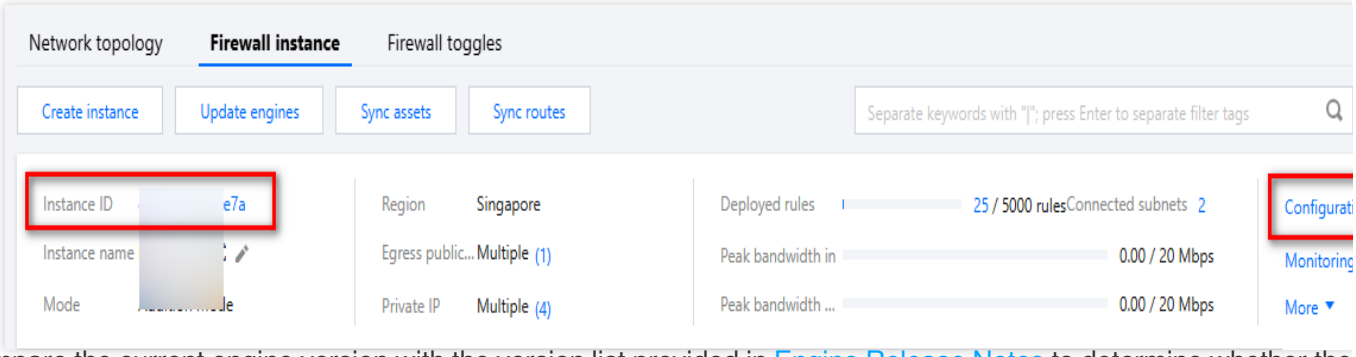


3. The latest stable version will be selected by default. If there are firewall instances that can be upgraded, the upgrade options below will become available.



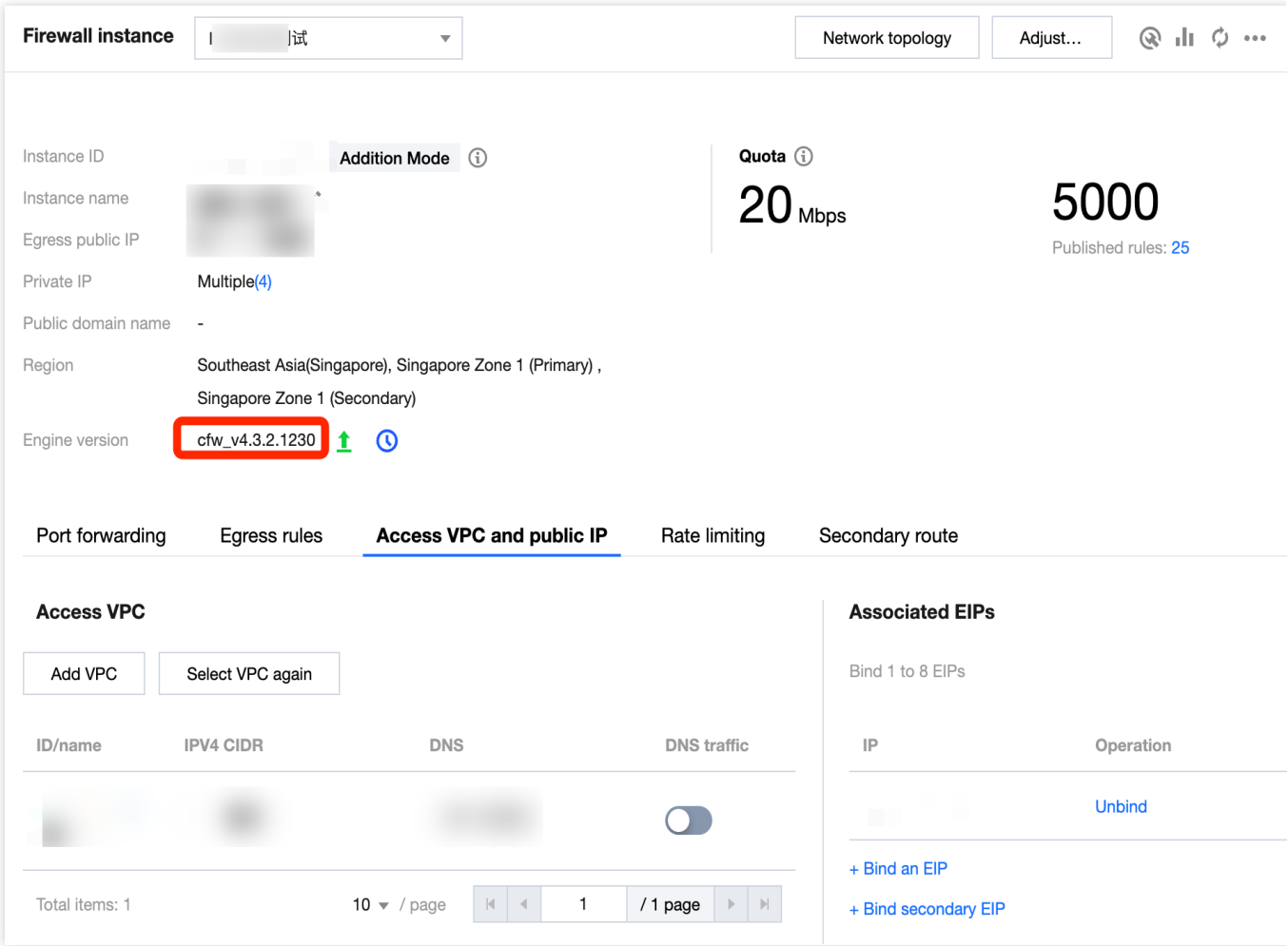
4. You can also check the specific instance's engine version and whether it can be upgraded.

Click **Instance ID** or **Configuration** of the target firewall to enter the firewall instance details page.



5. Compare the current engine version with the version list provided in Engine Release Notes to determine whether the upgrade is available. If the upgrade is available, a

mark will appear on the right side of the engine version.



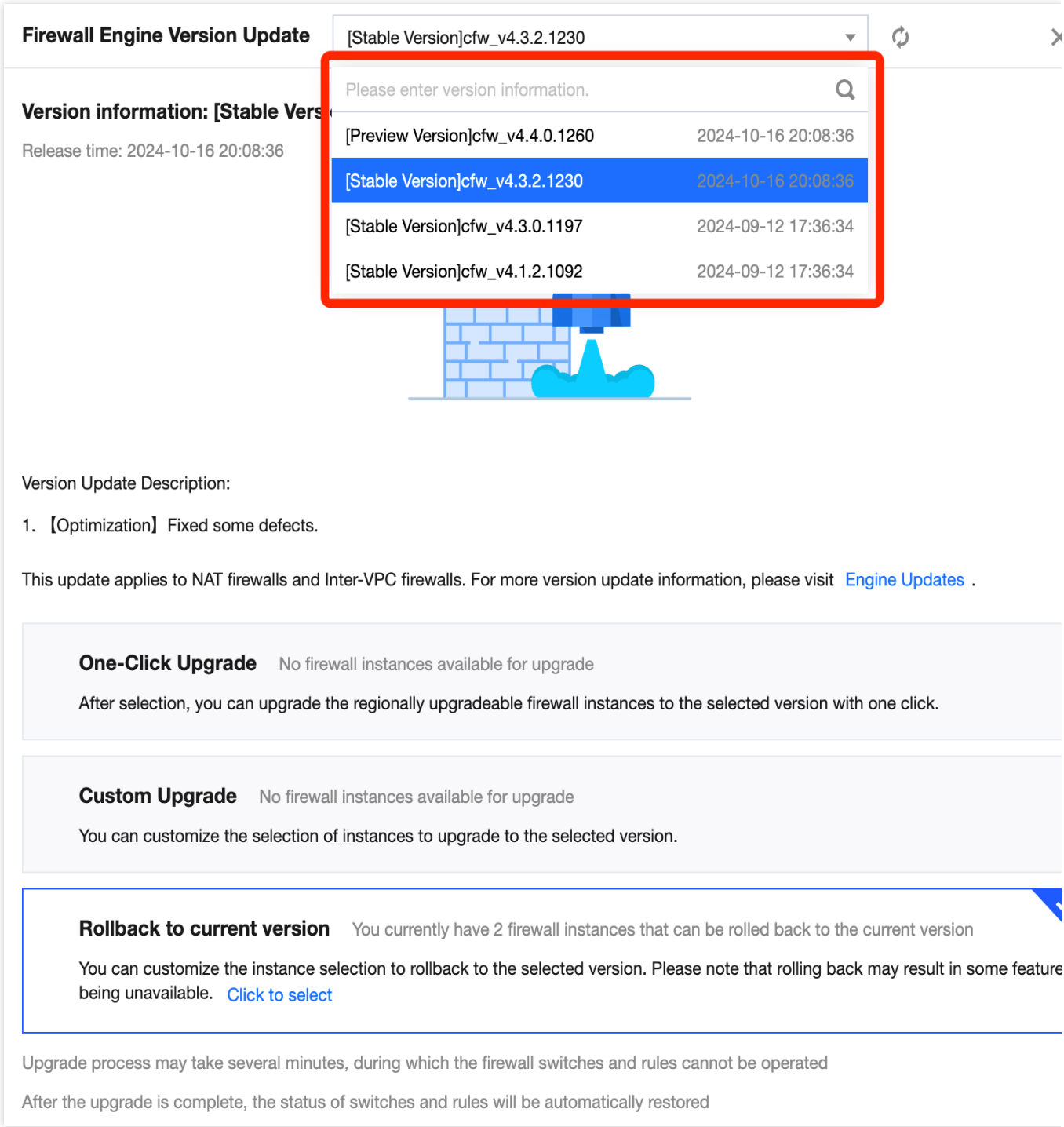
Upgrading the Firewall Engine Version

1. See the previous section to enter the engine upgrade page, and select the engine version you want to upgrade at the indicated location.

Note:

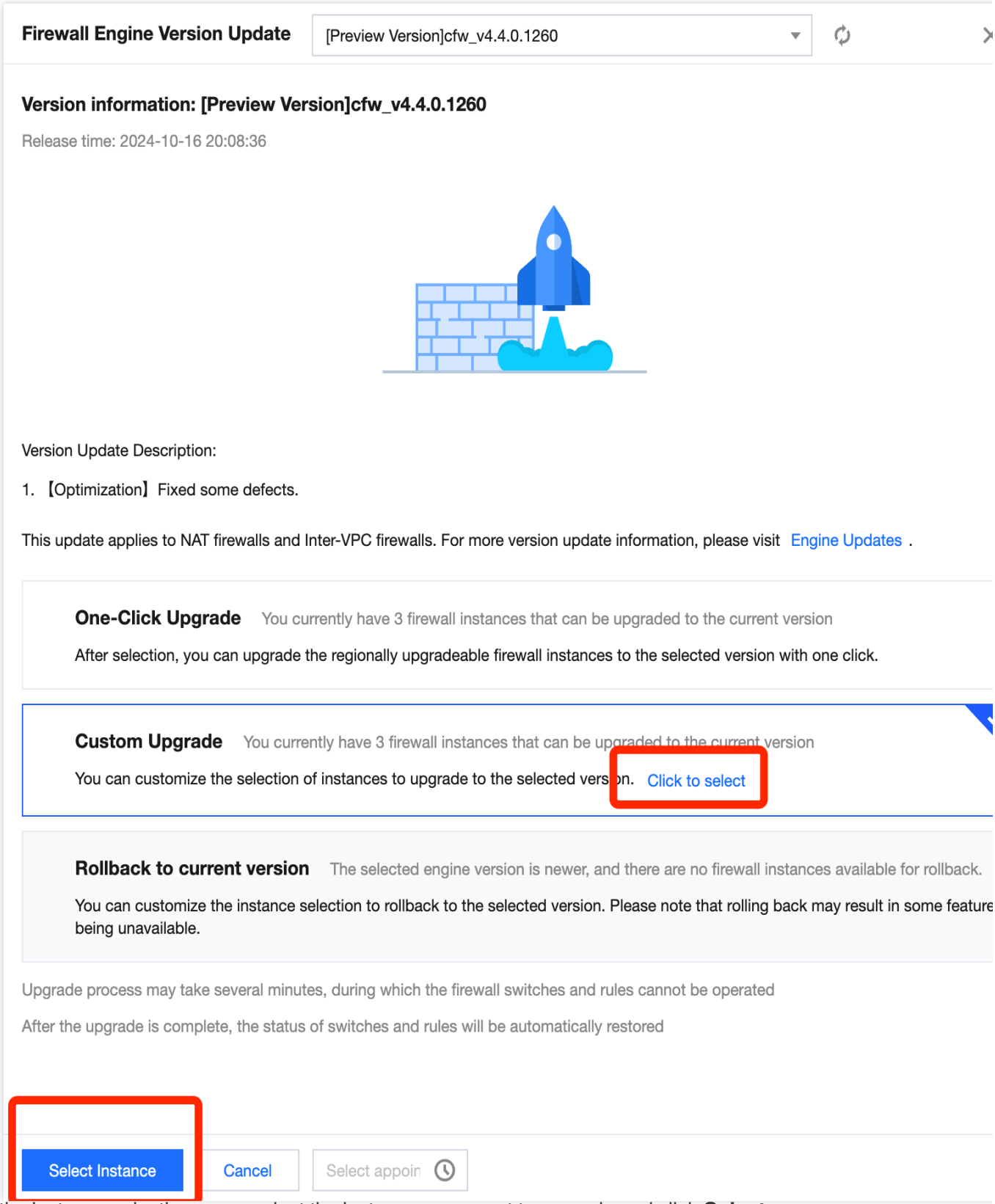
The preview version is the latest engine version, which includes the latest features and bug fixes. The stable version has been verified for long-term stability in the production environment and generally lags behind the preview version by one major version.

We recommend that you promptly update the engine to the latest stable version. For details about the version, see Engine Release Notes.

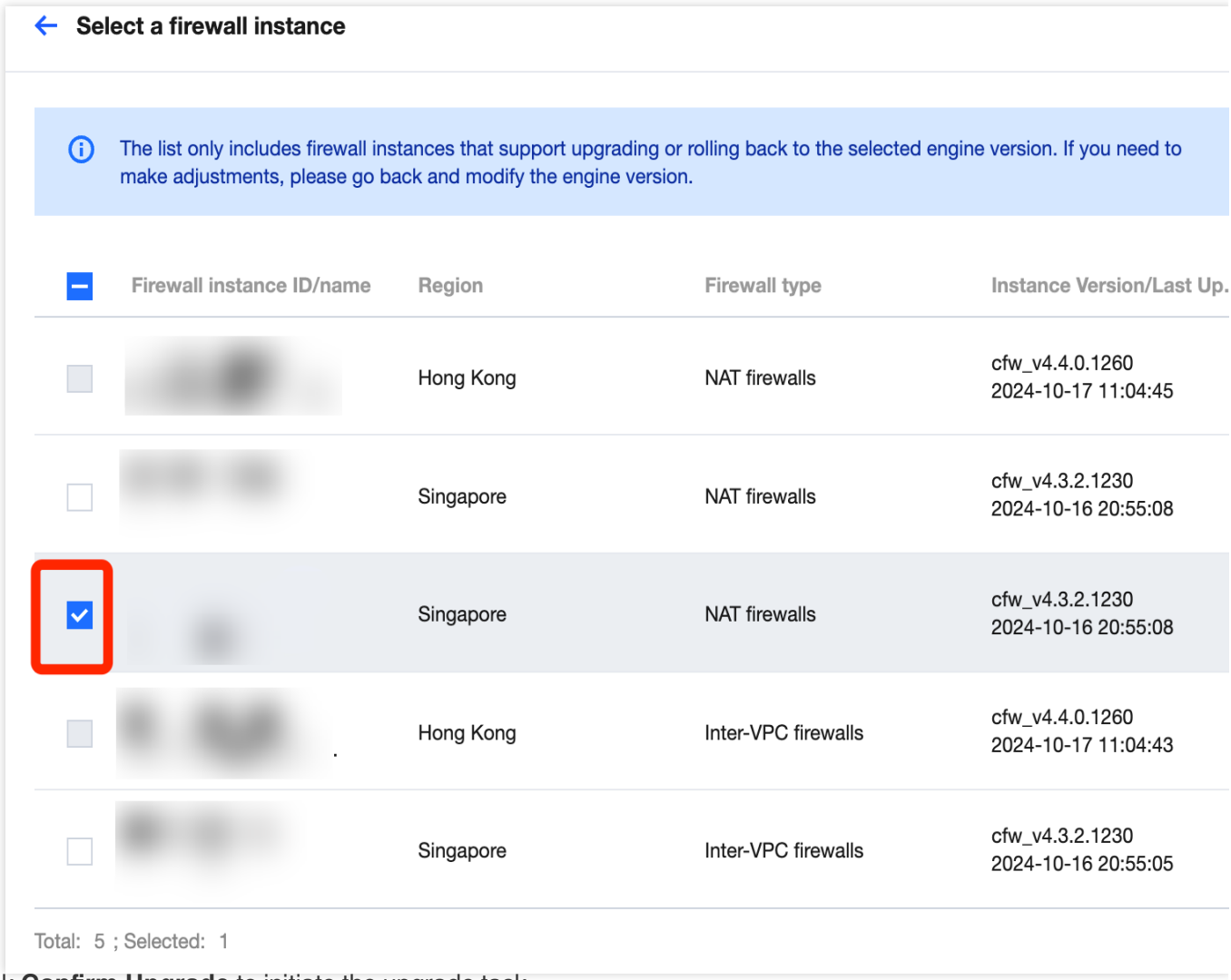


2. Select the engine instances that need to be upgraded.

One-Click Upgrade: After you select this option, firewall engine instances of the current version in all regions will be automatically identified and upgraded to the selected version.
Custom upgrade: You can manually select instances you want to upgrade. Click **Click to****Select/Select Instance** to enter the instance selection page.



3. On the instance selection page, select the instances you want to upgrade and click **Select**.



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

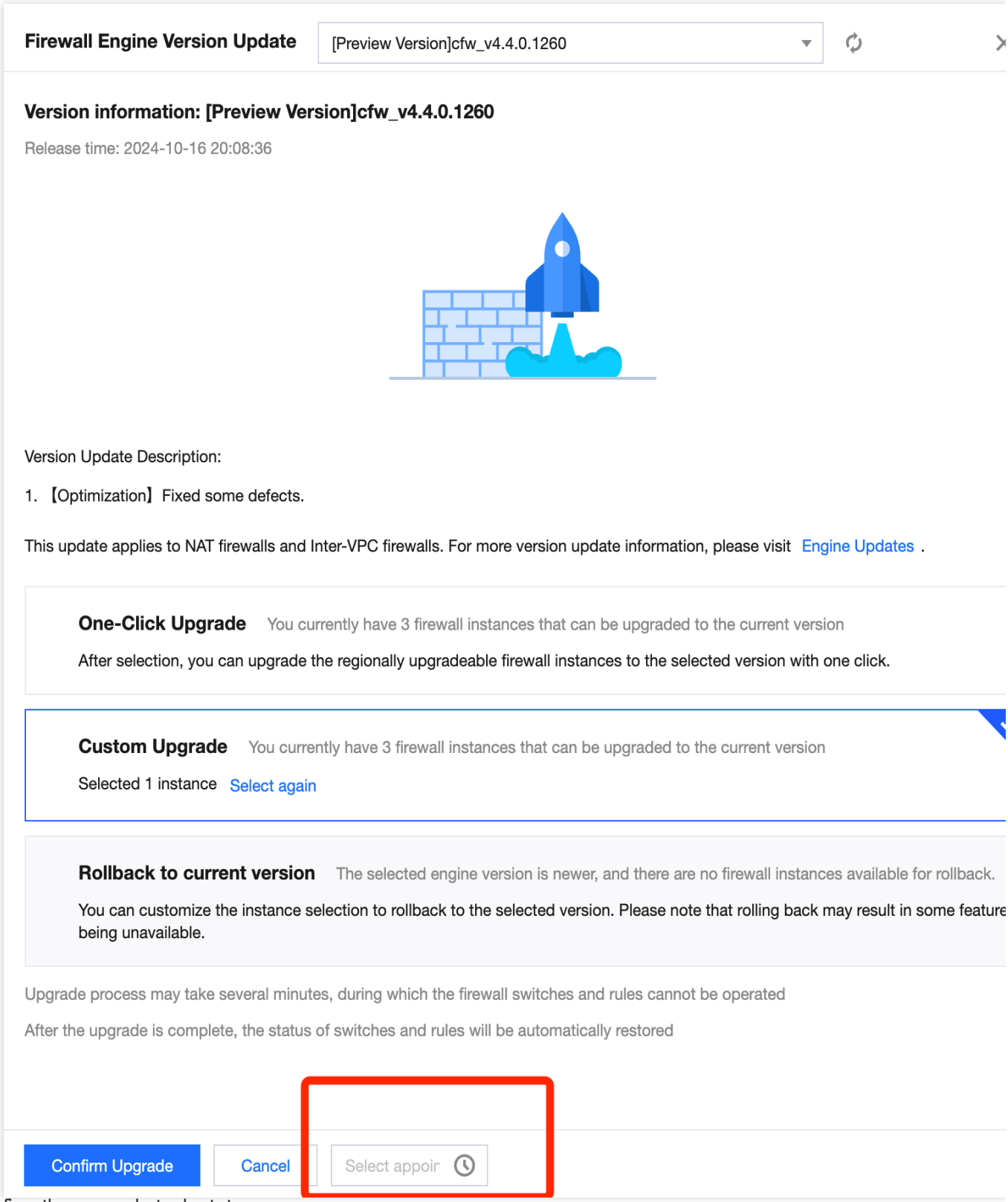
Note:

The upgrade may take several minutes during which the firewall switch and rules cannot be configured. After the upgrade is completed, the status of the switch and rules will be automatically recovered.

During the upgrade, the secondary machine will be upgraded first, followed by the primary machine. In addition, a primary-secondary switch operation will be triggered, which may cause slight network jitter, but the service will not be interrupted.

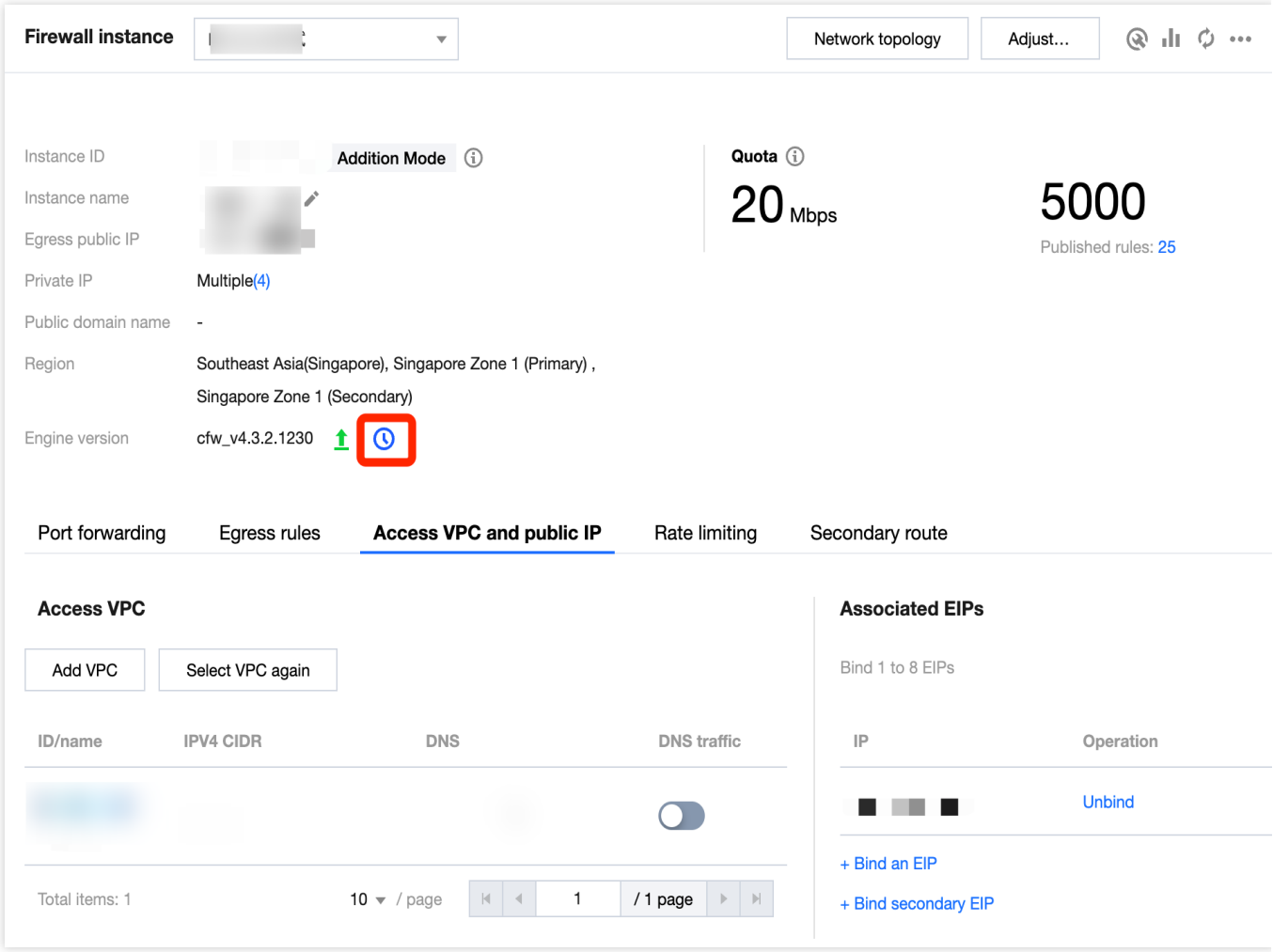
Scheduling the Upgrade Time

1. After Steps 1 and 2 in the previous section are completed, click **Select appoir** at the indicated location.



2. Confirm the upgrade task status.

Enter the corresponding firewall instance page, where you can view the scheduled upgrade task in the indicated engine version area. You can click **Cancel appoir** or re-execute the engine upgrade operation to cancel the schedule.


Firewall instance
Network topology
Adjust...
Instance ID
Addition Mode
Instance name
Egress public IP
Private IP
Multiple(4)
Public domain name
-
Region
Southeast Asia(Singapore), Singapore Zone 1 (Primary) ,
Singapore Zone 1 (Secondary)
Engine version
cfw_v4.3.2.1230
Quota
20 Mbps
5000
Published rules: 25
Port forwarding
Egress rules
Access VPC and public IP
Rate limiting
Secondary route
Access VPC
Add VPC
Select VPC again
ID/name
IPV4 CIDR
DNS
DNS traffic
Total items: 1
10 / page
1
/ 1 page
Associated EIPs
Bind 1 to 8 EIPs
IP
Operation
Unbind
+ Bind an EIP
+ Bind secondary EIP

Alert Management
Features
Overview

Last updated：2024-01-24 15:48:25

Alarm management presents the data of cyber attacks and risk events detected by the **Intrusion defense** and **Security baseline** modules. The data is divided into **Attack alerts**, **Blocked attacks**, and **Honeypot events** based on the action taken by CFW.

Attack alerts: all detected cyber attacks and risk events, which need to be blocked or ignored manually by users.

Blocked attacks: all detected cyber attacks and risk events that are automatically blocked by the system. The data is used for subsequent audits and troubleshooting.

Honeypot events: all detected cyber attacks and risk events against probes and honeypots. You can set the system to block or allow such attacks and events.

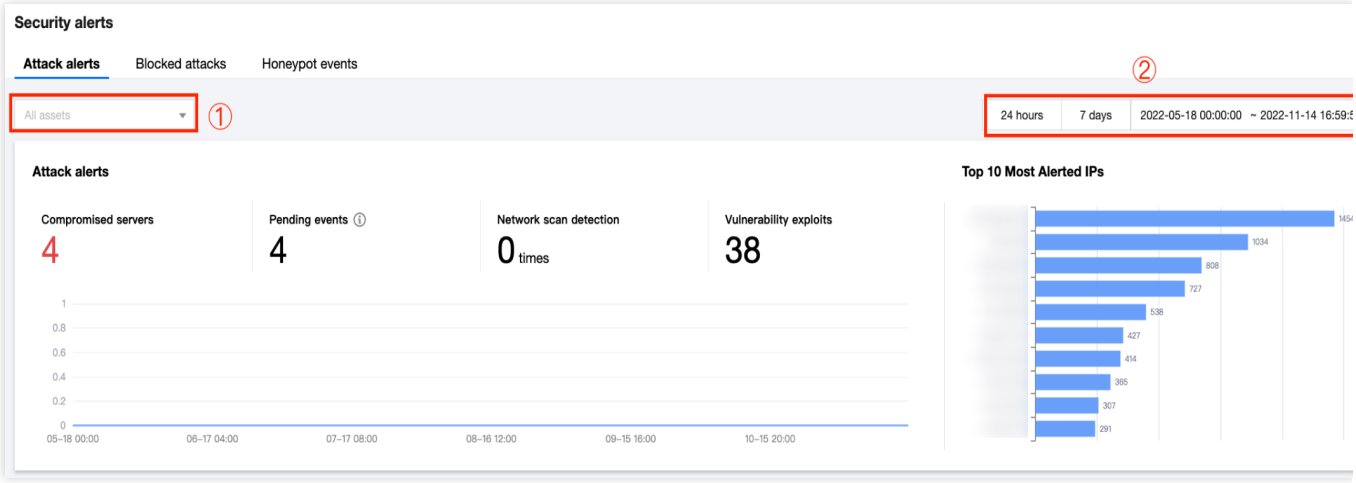
Attack Alerts

Last updated：2024-01-24 15:48:25

The **Attack alerts** module displays all monitored risk events and allows you to analyze and resolve all events detected by CFW.

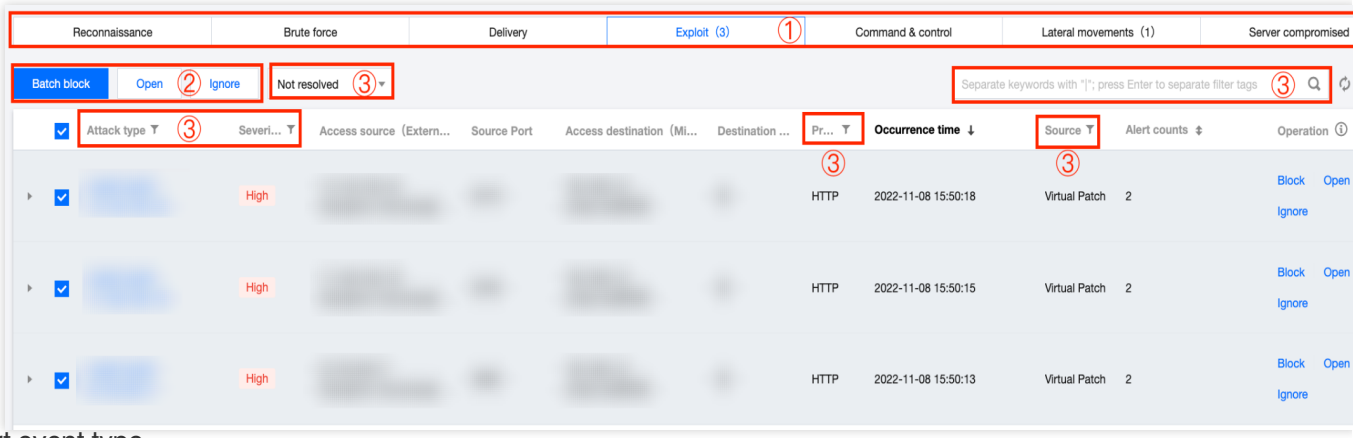
Visual representation of attack alerts

1. Log in to the Cloud Firewall console. In the left navigation pane, click **Alert Management** -> **Attack alerts** to open the **Attack alerts** page.
2. In this module, you can analyze existing security alert events by ①**personal assets** and ②**time range** (24 hours, 7 days, or a custom time range) with a graph. The left section displays the trend curve of recent security events, with the x-axis indicating time and the y-axis indicating the number of alerts at each point in time. In addition, you can view the statistics about compromised servers, pending events, network scans, and exploit attacks. The right section displays the list of the top 10 IPs with the most attack alerts so that you can take early action to prevent attacks of those IPs.



Attack alert list

In this module, you can analyze alert events under different ① **event types**, ② **batch resolve events**, ③ **filter events by conditions**, and ④ **specify custom keywords**.



① Alert event type

② Batch resolve events

③ Filter events by conditions

④ Specify custom keywords

Click the tabs in the area marked "①" to view the details of the alerts of different types.

Note

The relevant security event types are displayed only after you configure the security policies required by CFW in Intrusion defense, and Security baseline.

You can click **Block all** for all selected events, or **Allow** or **Ignore** them in batch mode.

Note

These buttons are only available when one or more events are selected.

Select values from the drop-down lists marked "③" to filter the alert events. The following capabilities are supported:

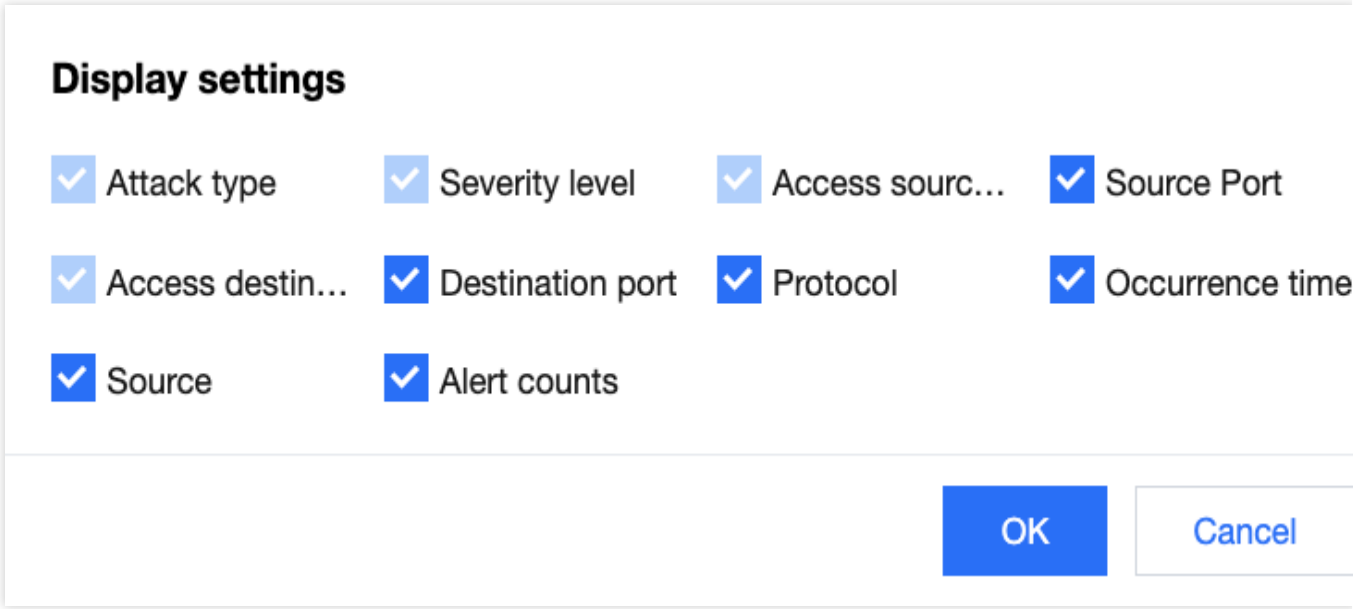
View the information of unresolved, blocked, allowed, and ignored alert events.

Filter alert events by severity.

Filter alert events by security event type, protocol, and source.

Filter events by keywords.

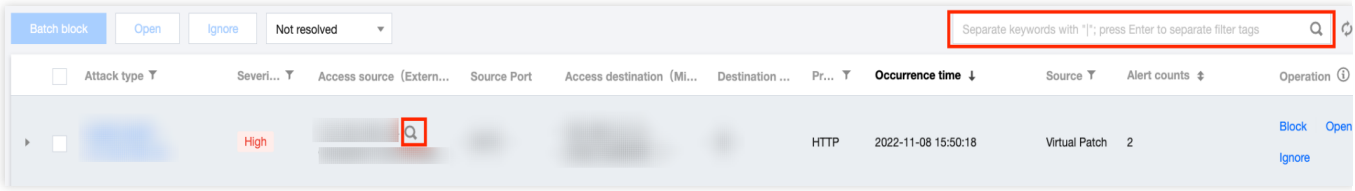
Click the icon marked "④" to specify custom keywords. A maximum of 10 keywords are allowed.



Event details

Click

next to a malicious IP to filter out all security events of that IP under the current type.

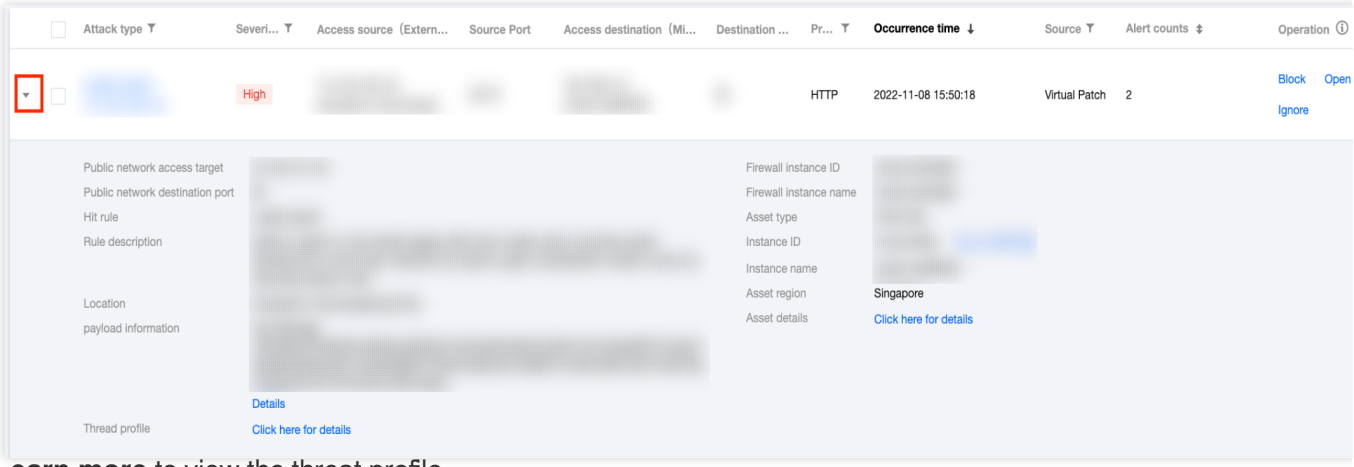


Click

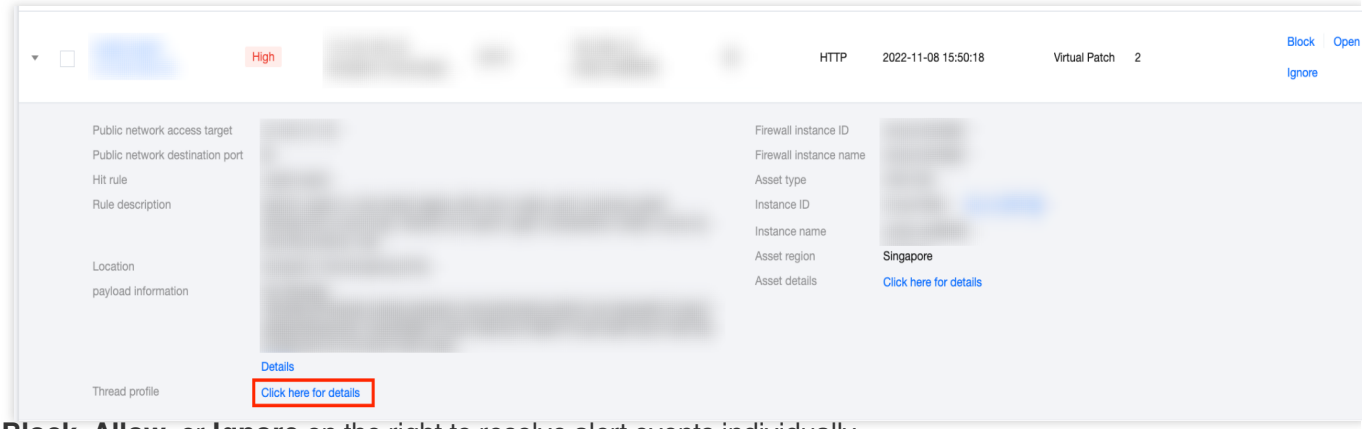
on the left to view the details of an event.

Note

You need to purchase CWPP to use the enhanced detection features of CWPP.



Click **Learn more** to view the threat profile.

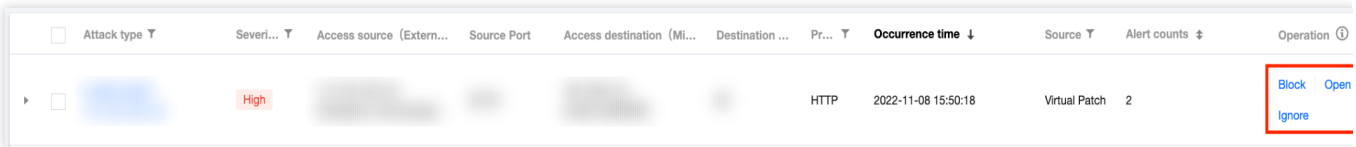


Click **Block**, **Allow**, or **Ignore** on the right to resolve alert events individually.

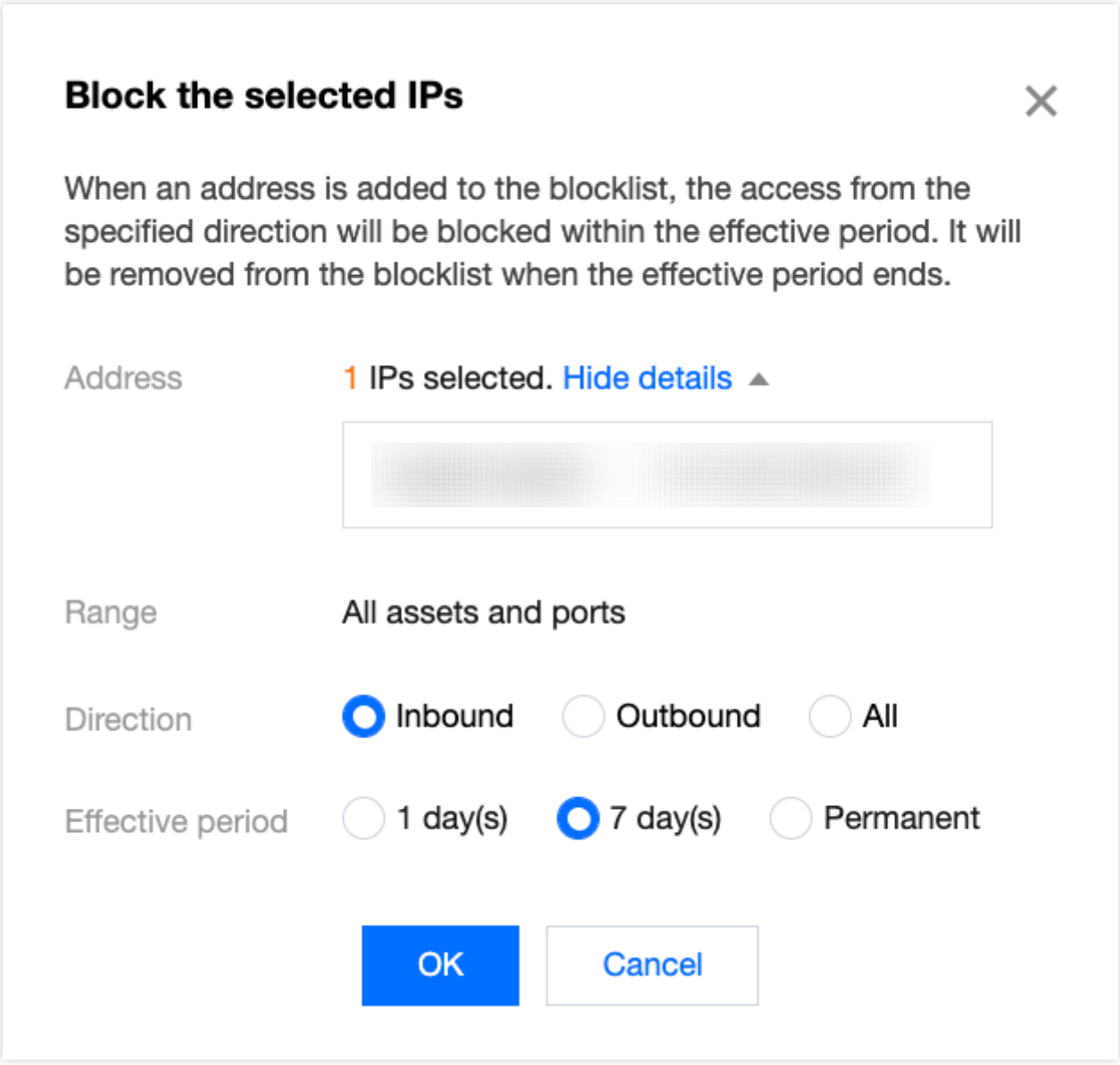
Note

The following operations also apply to batch processing and events for other types of IPs.

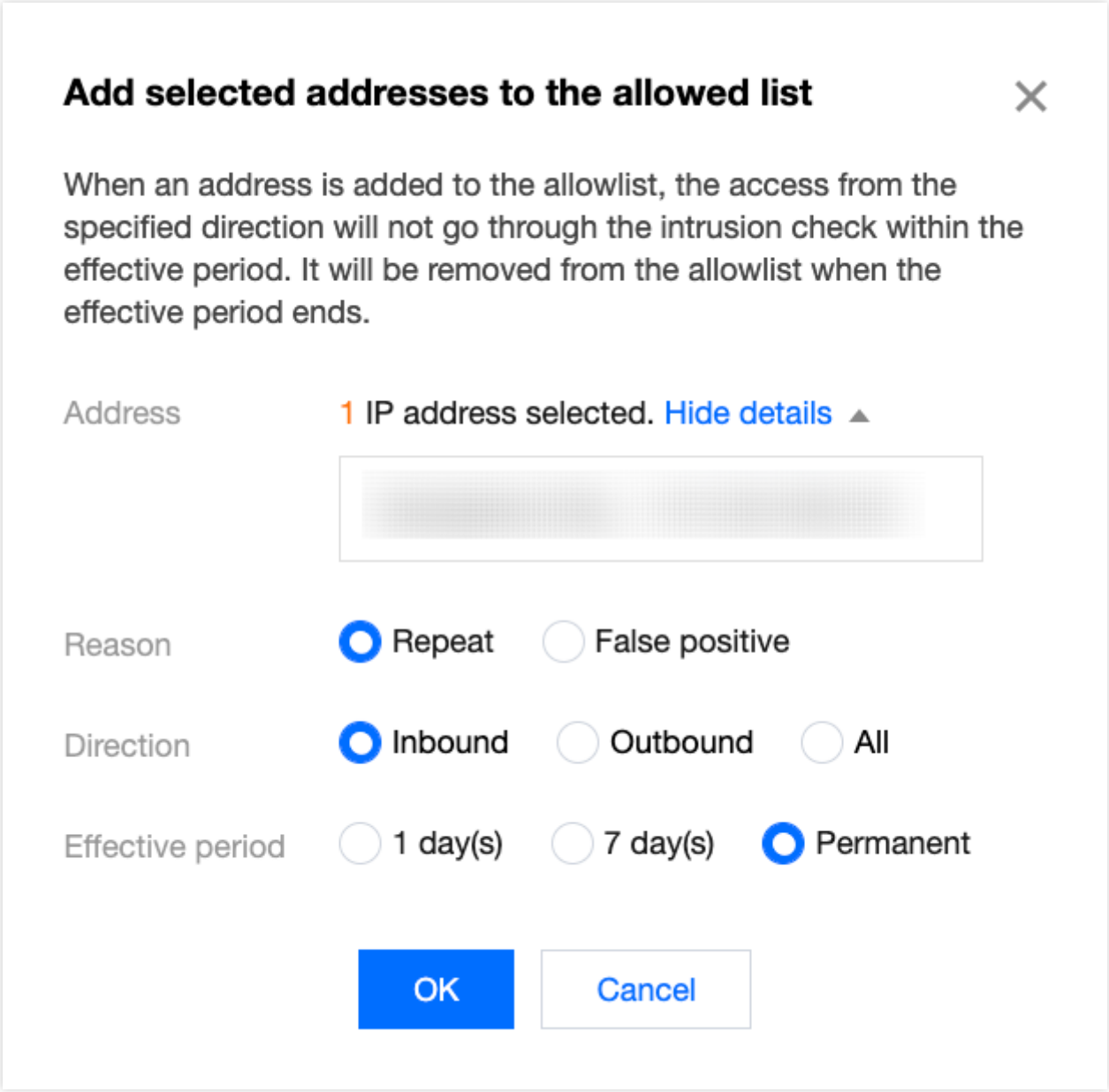
To modify your operation, undo the operation in **Intrusion defense** -> **Blocklist**.



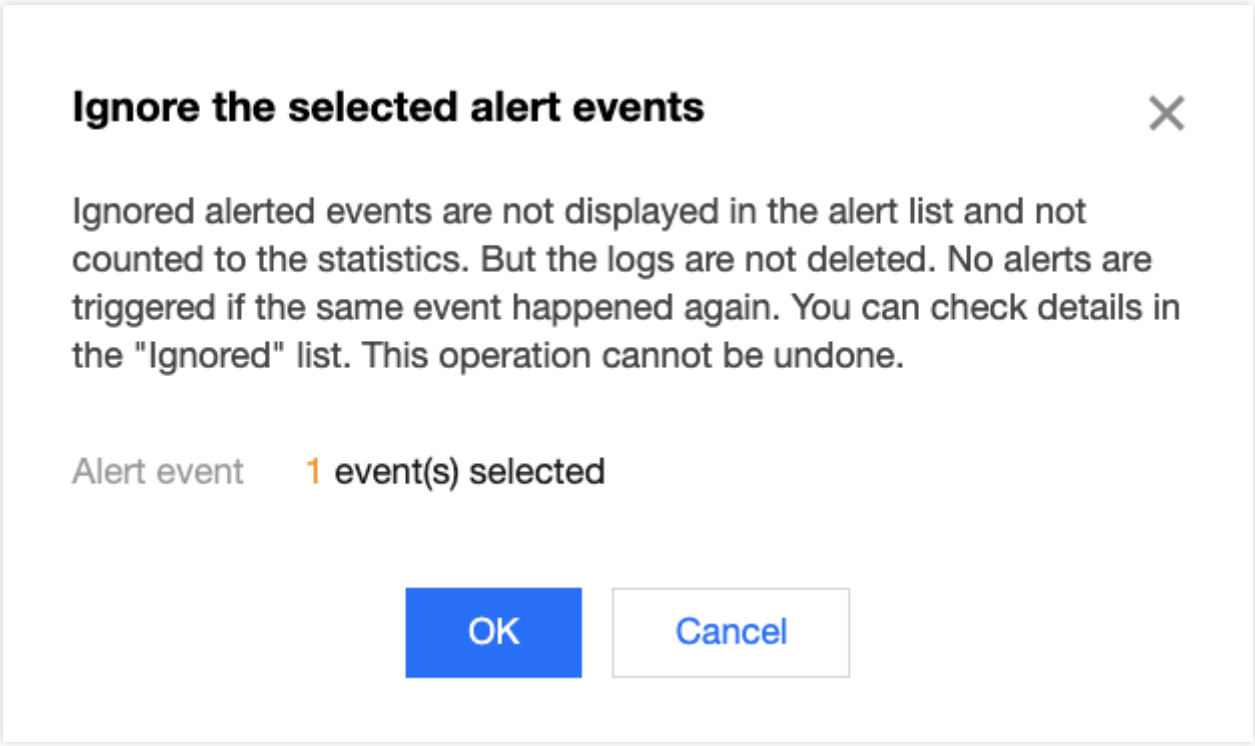
Block: For security events with a higher severity or a larger number of alerts, click **Block** to add the IP to the blocklist in Intrusion defense. CFW automatically blocks that IP from accessing all of your assets within the specified period.



Allow: For repeated or possible false alerts, you can click **Allow** to add the IP to the allowlist in Intrusion defense. CFW allows traffic from the IP by skipping attack detection for the IP in **Intrusion defense** within the specified period.



Ignore: If you do not want to take action on an alert, click **Ignore**. The log is not deleted. You can view the log in the list of ignored alerts.



Blocked Attacks

Last updated：2024-01-24 15:48:25

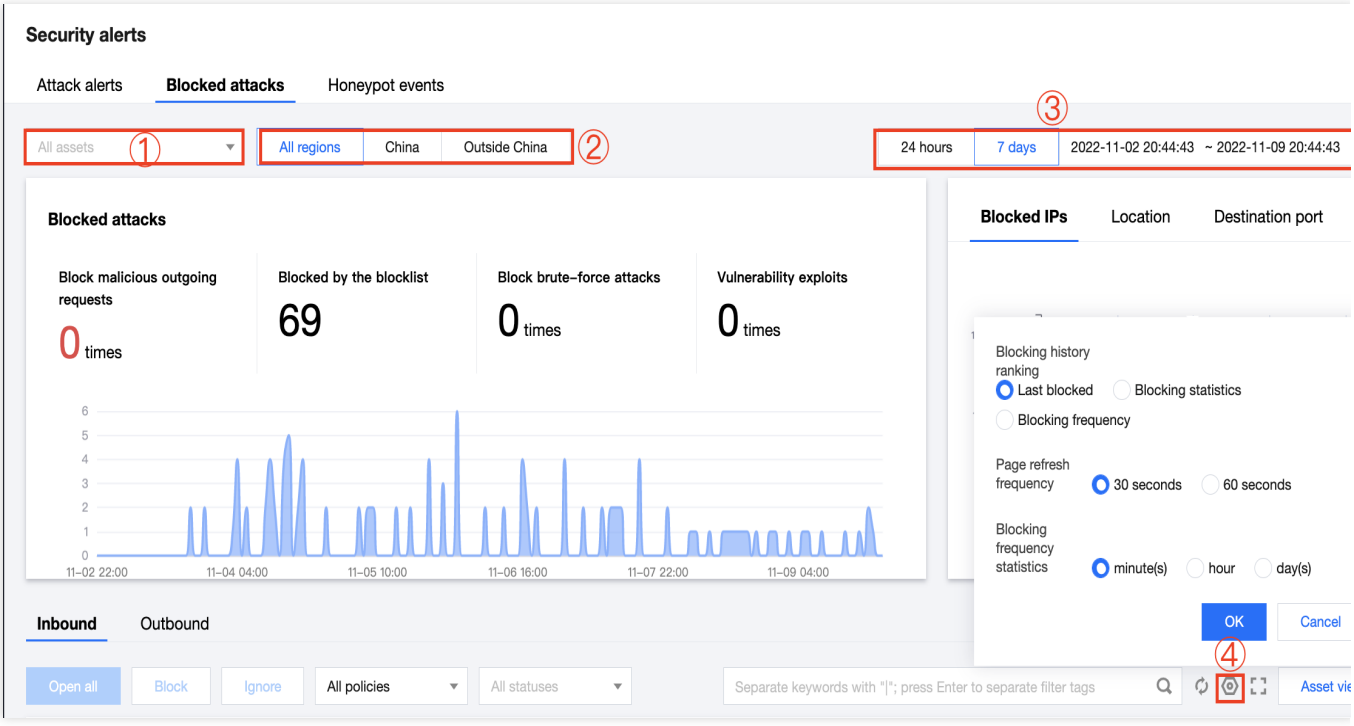
The **Blocked attacks** module presents all the security events blocked by CFW based on configured rules and threat intelligence, and allows you to analyze and resolve all blocked attacks.

Visual representation of blocked attacks

1. Log in to the Cloud Firewall console. In the left navigation pane, click **Alert Management** -> **Blocked attacks** to open the **Blocked attacks** page.
2. In this module, you can analyze existing security alert events by ① **personal assets**, ② **region**, and ③ **time range** (24 hours, 7 days, or a custom time range) with a graph. The left section displays the trend curve of recently blocked events, with the x-axis indicating time and the y-axis indicating the number of blocked attacks at each point in time. In addition, you can view the statistics about blocked malicious outgoing access, attacks blocked by blocklist, blocked brute-force attacks, and exploit attacks. On the right, you can view the ranking of blocked events by blocked IP, geographic location, and destination port.

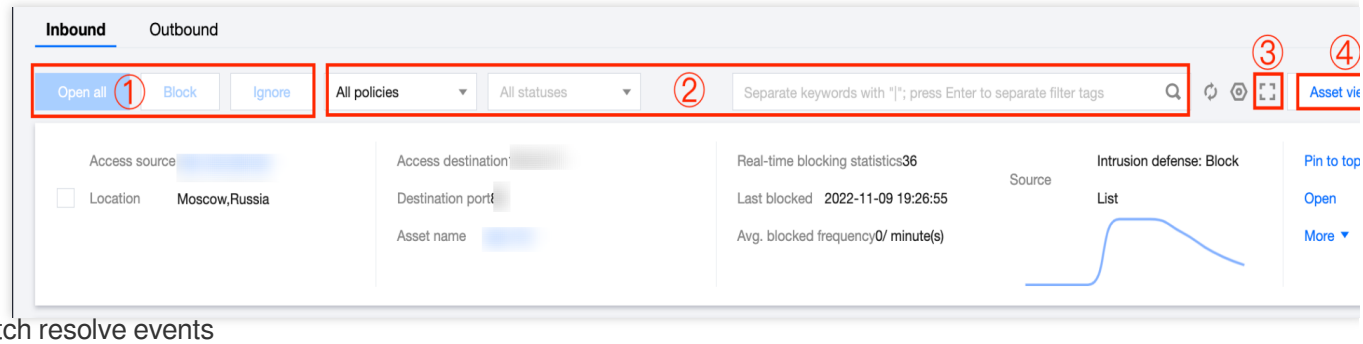
Note

This page is automatically refreshed at an interval. You can set ④**Auto refresh rate** to **30s** or **60s**.



List of blocked attacks

Blocked events are divided into **Inbound**, **Lateral movements**, and **Outbound** based on the traffic direction.



① Batch resolve events

② Filter events by conditions

③ Full-screen display

④ Switch view

You can click **Block all**, **Block**, or **Ignore** for selected events.

Note

These buttons are only available when one or more events are selected.

Select values from the drop-down lists marked "②" to filter blocked events. The following capabilities are supported:

Display blocked events by intrusion defense policy and resolution status.

Sort blocked events by blocking time, blocking statistics, and average blocking frequency.

Record blocked events at a frequency of minutes, hours, or days.

Filter events by keywords.

Click

to switch to the full-screen display mode.

Click

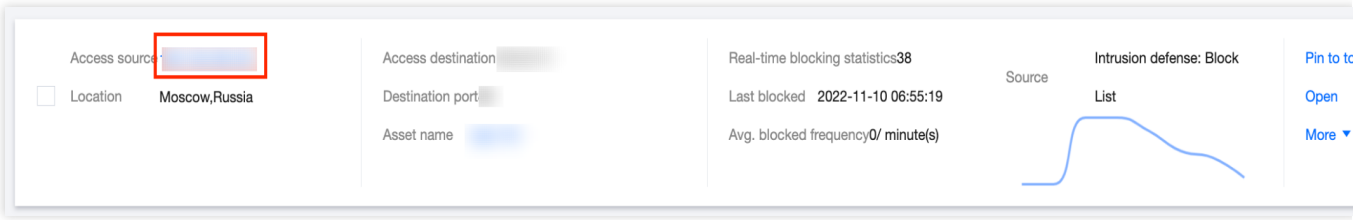
to switch back to the original display mode.

Click **Asset view** or **Event view** to switch between the two views.

Asset view

In this view, the blocked events from the same access source are displayed based on attacker assets.

You can click the IP of the access source on the left to view the threat profile.



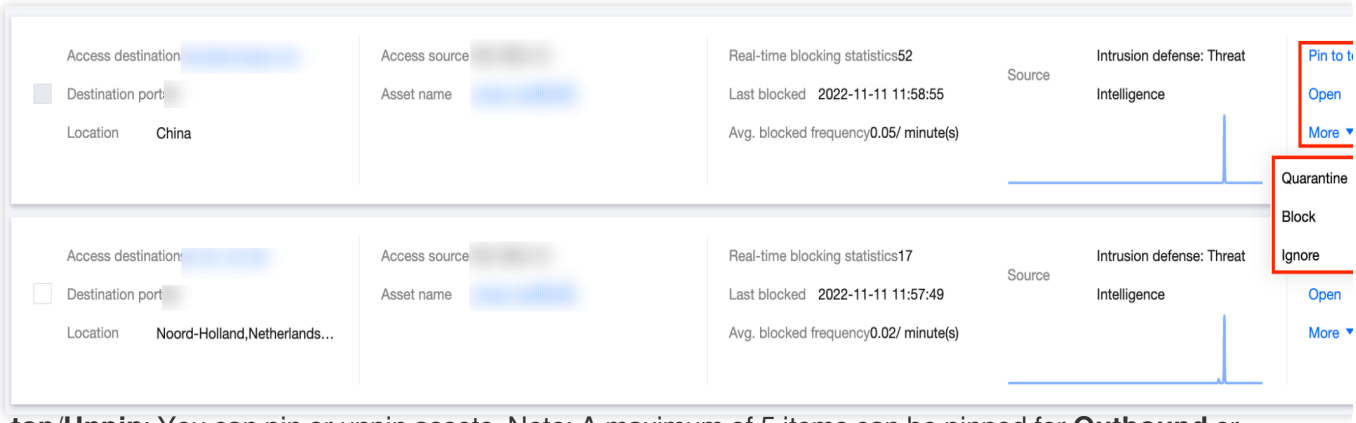
Click **Pin to top** or **Allow**, or click **More** -> **Quarantine**/**Block**/**Ignore** on the right to pin, allow, quarantine, block, or ignore an IP.

Note

The available buttons on the right vary depending on the state of the assets.

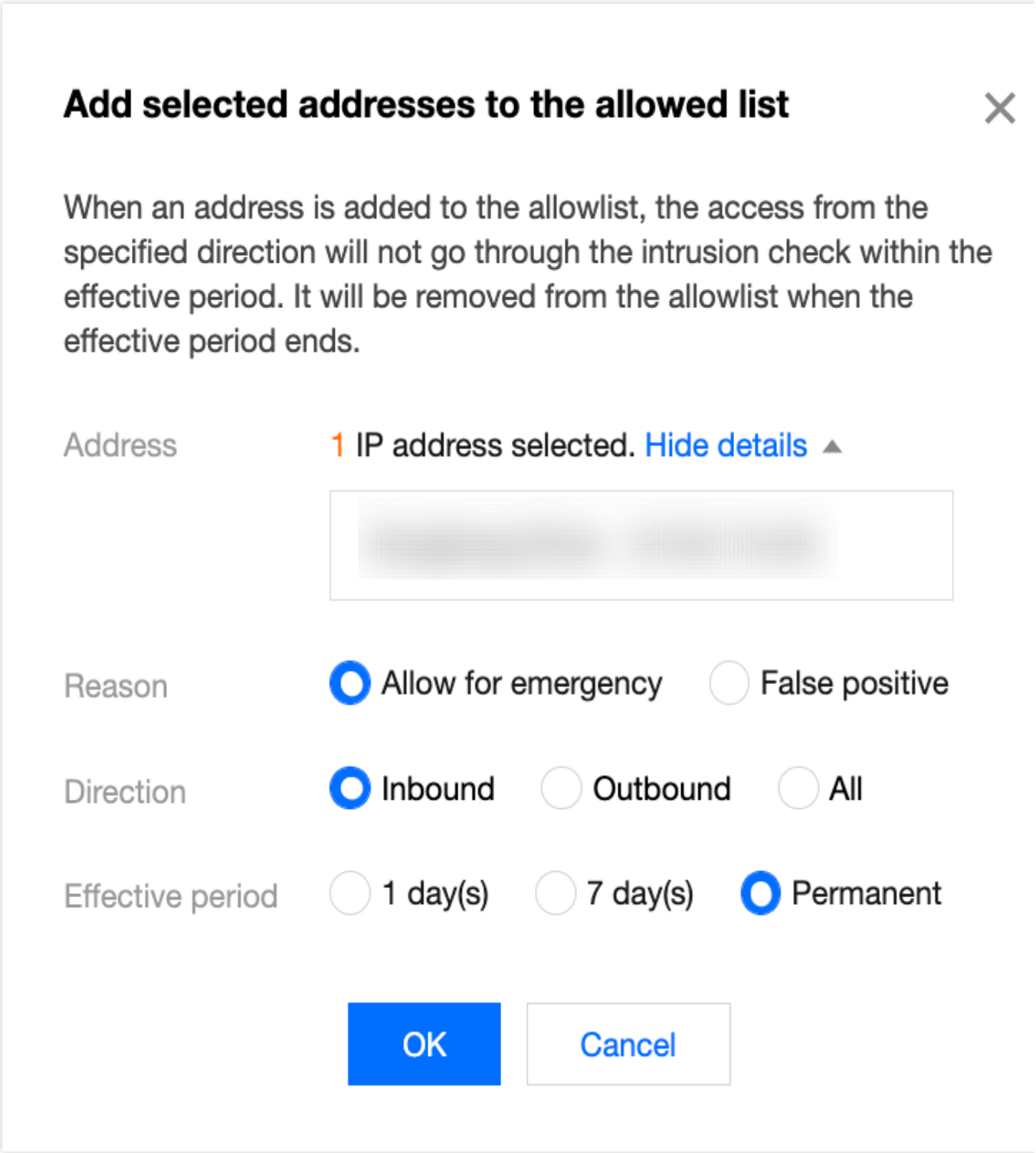
The following operations also apply to batch processing and event view.

To modify your operation, undo the operation in **Intrusion defense** -> **Blocklist**.

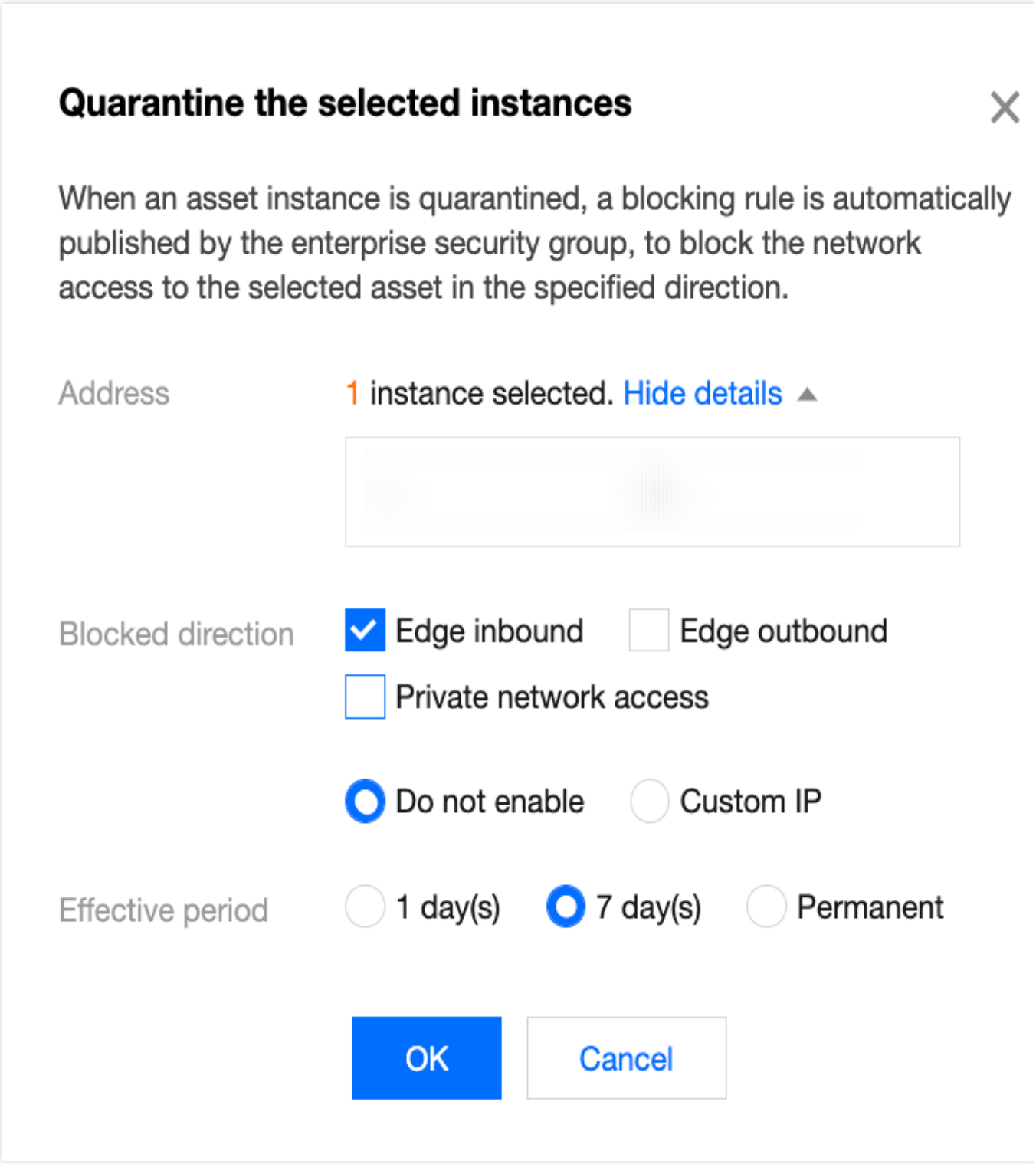


Pin to top/**Unpin**: You can pin or unpin assets. Note: A maximum of 5 items can be pinned for **Outbound** or **Inbound**.

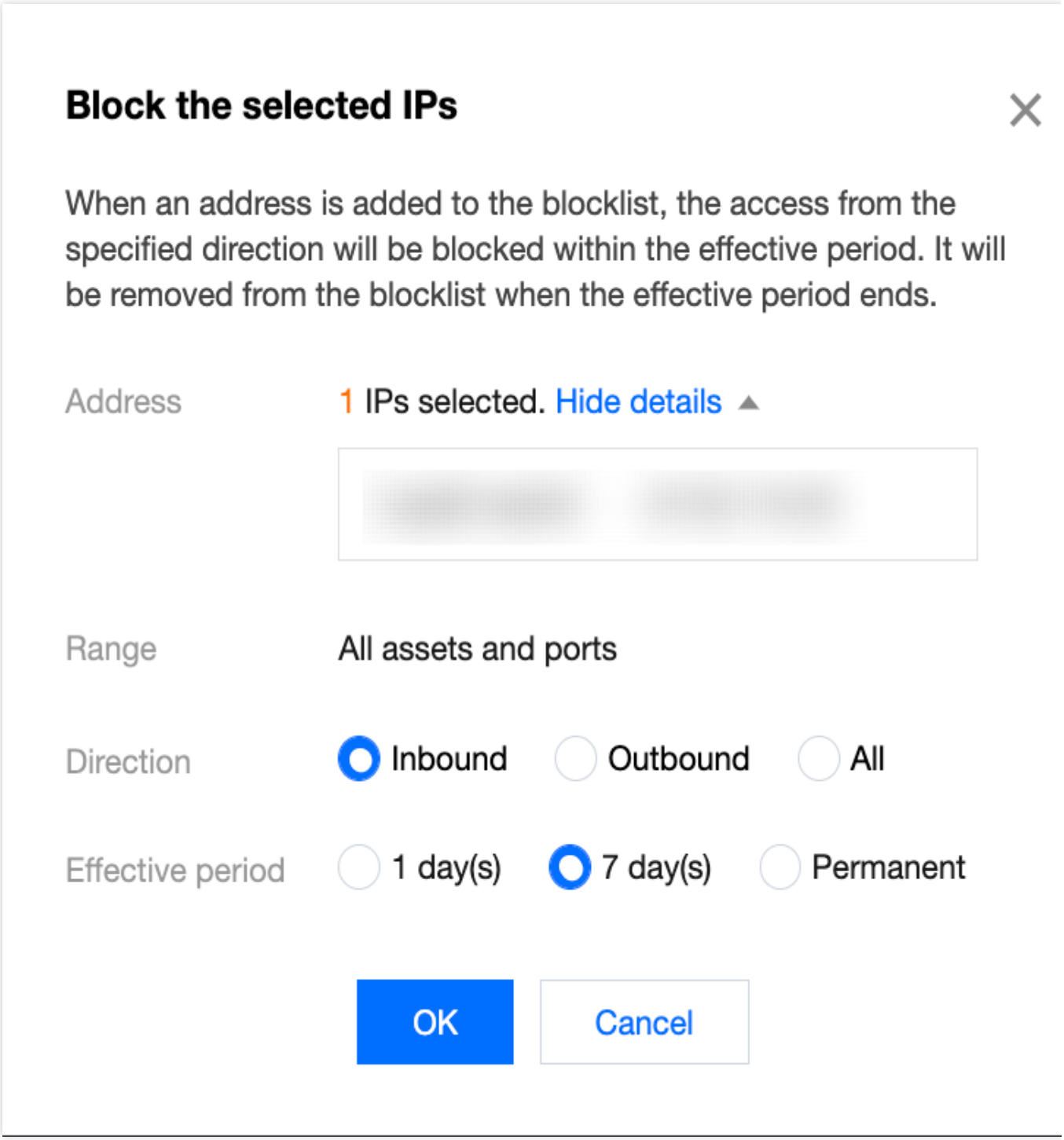
Allow: Click **Allow** for an IP that does not need to be blocked. Then, select **Reason** and **Validity**. Within the selected validity period, the IP is in the access control allowlist and is not blocked. If you are not certain about whether the reason is "false positive", you can select **Allow for emergency**, and modify it later if necessary.



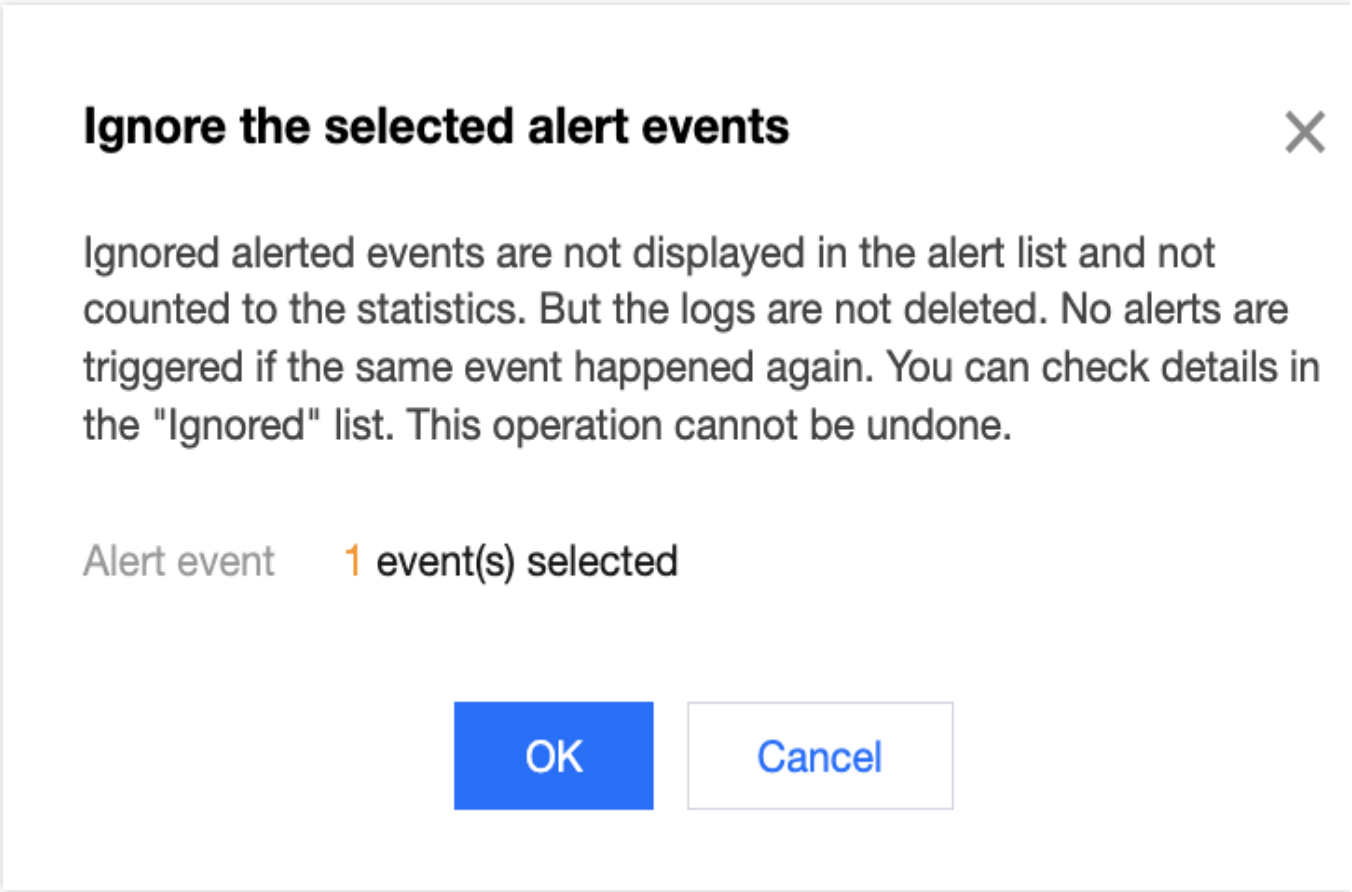
Quarantine: Click **Quarantine**. When an asset instance is quarantined, the system automatically publishes the blocking rule for enterprise security groups to block network access to the selected asset in the specified blocking direction. This makes the subsequent troubleshooting easy and prevents the asset from being attacked.



Block: For assets with a high threat level, click **Block**. Then, specify a validity period to add the IP to the blocklist in Intrusion defense. CFW automatically blocks that IP from accessing all of your assets within the specified period.



Ignore: For repeated or possible false alerts, you can click **Ignore**. The ignored alert events are not included in the alert list and statistics, but their logs are retained. You are no longer notified of the ignored alert events when they trigger alerts again. You can select **Ignored** in the list to view all the ignored events. **The "Ignore" operation is irreversible.**



Event view

For more information about operations in this view, please see Attack alerts - Event details.

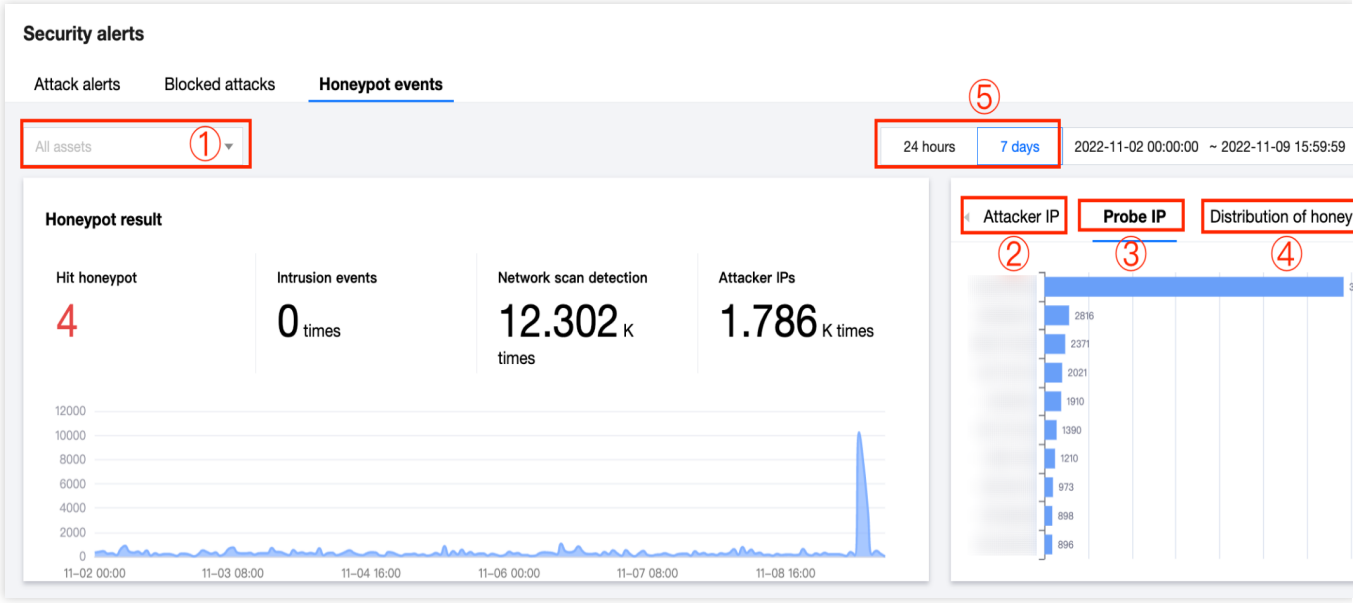
Honeypot Events

Last updated：2024-01-24 15:48:25

The **Honeypot events** page records the scans and attacks on all probes and honeypots and presents the data in a graph and list so that you can analyze and resolve all blocked events.

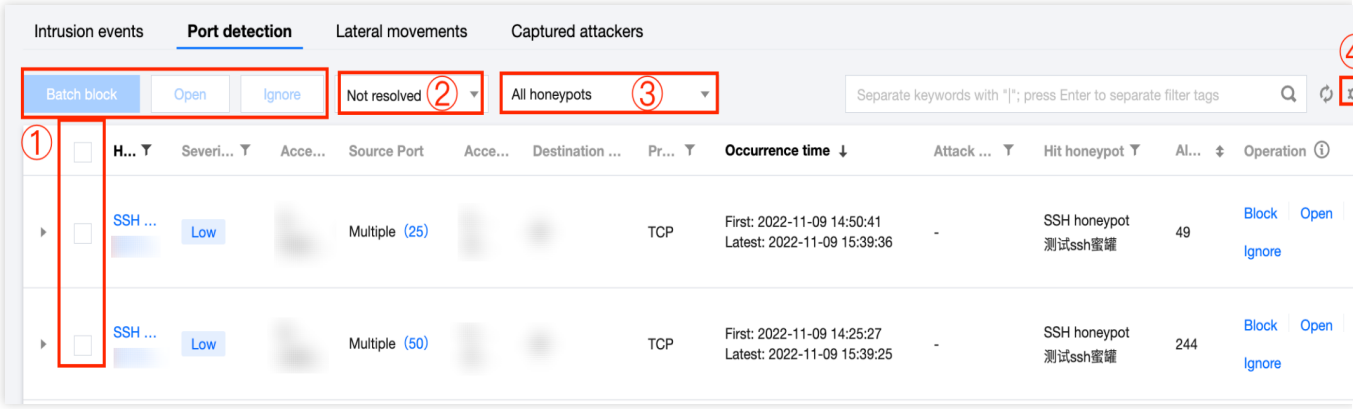
Visual representation of honeypot events

1. Log in to the Cloud Firewall console. In the left navigation pane, click **Alert Management** -> **Honeypot events** to open the **Honeypot events** page.
2. You can ① **select the probes to analyze**, and analyze the data of selected probes based on ②**Honeypot attacker IP**, ③**Probe scan IP**, ④ **Distribution of honeypot events** and ⑤**Time** (24 hours or 7 days). You can view the number of hit honeypots, the number of intrusion events, the number of network scans, and the number of attacker IPs for the selected or all probes within different periods.



List of honeypot events

1. Log in to the Cloud Firewall console. In the left navigation pane, click **Alert Management** -> **Honeypot events**.
2. On the **Honeypot events** page, honeypot events are divided into **Intrusion events** and **Port detection**, depending on whether the honeypots are attacked.



You can perform the following operations in the list:

① Select **Block all** or **Allow all** for selected events. (The buttons are available only when one or more events are selected.)

②Filter events based on the event status (whether the events have been resolved).

③Filter events based on the honeypot type.

④Specify custom keywords (4 to 10 keywords are allowed).

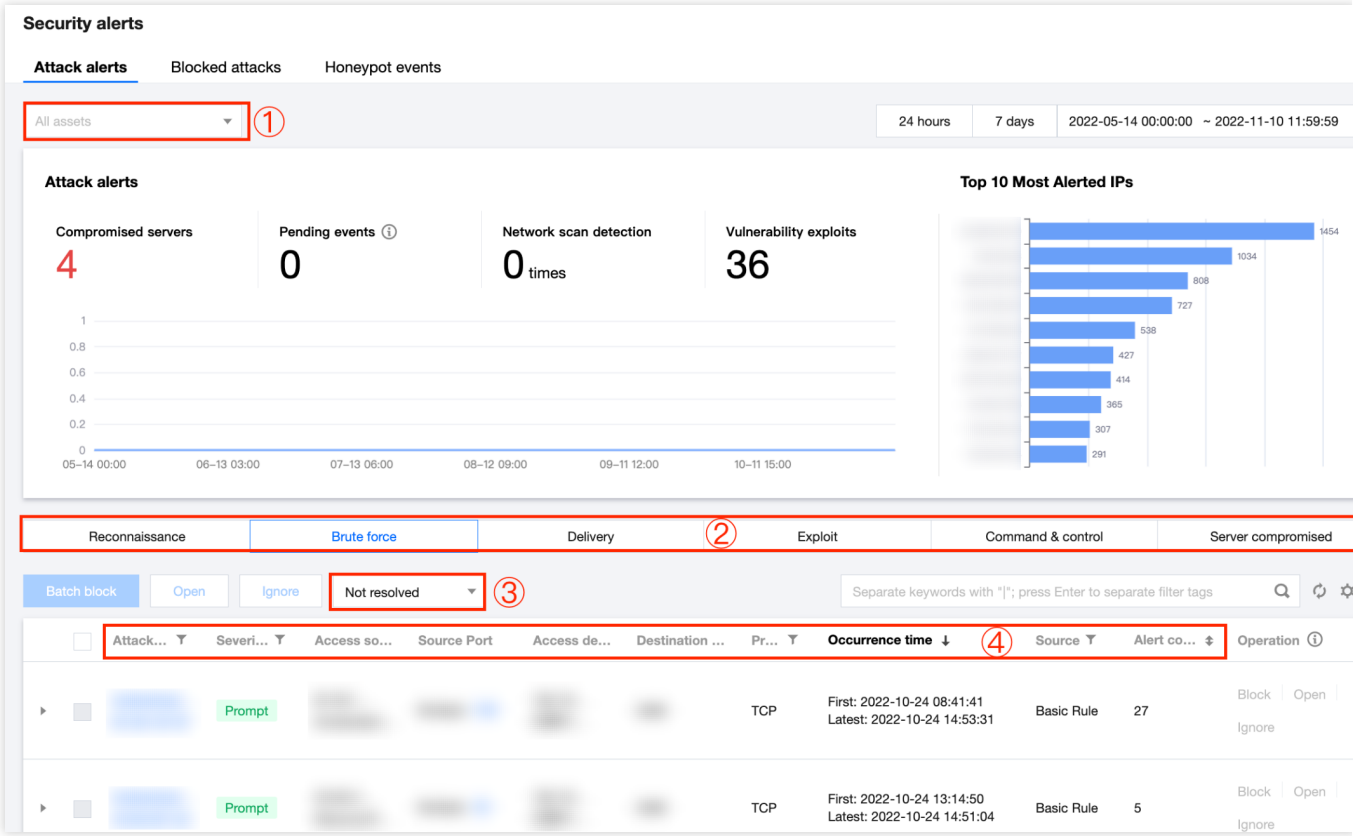
Operation Guide
Alert Analysis and Handling

Last updated：2024-01-24 15:48:25

This topic describes the operations in **Alert Management**. Log in to the Cloud Firewall console and open the Alert Management page, and then click **Attack alerts** to go to the **Attack alerts** page. On this page, you can view the trend chart of security events and the number of recent security events, and then adjust your defense policies to prevent attacks.

Filtering alert events

This section describes how to locate the alert events you want to view through filtering.
① Select the assets for which you want to view the alert events;
② Select the type of alert events.
③ Select whether to view unresolved events or resolved events;
④ Sort events in the order of occurrence time and the number of occurrences, or filter events by attack event type, severity, protocol, and source.



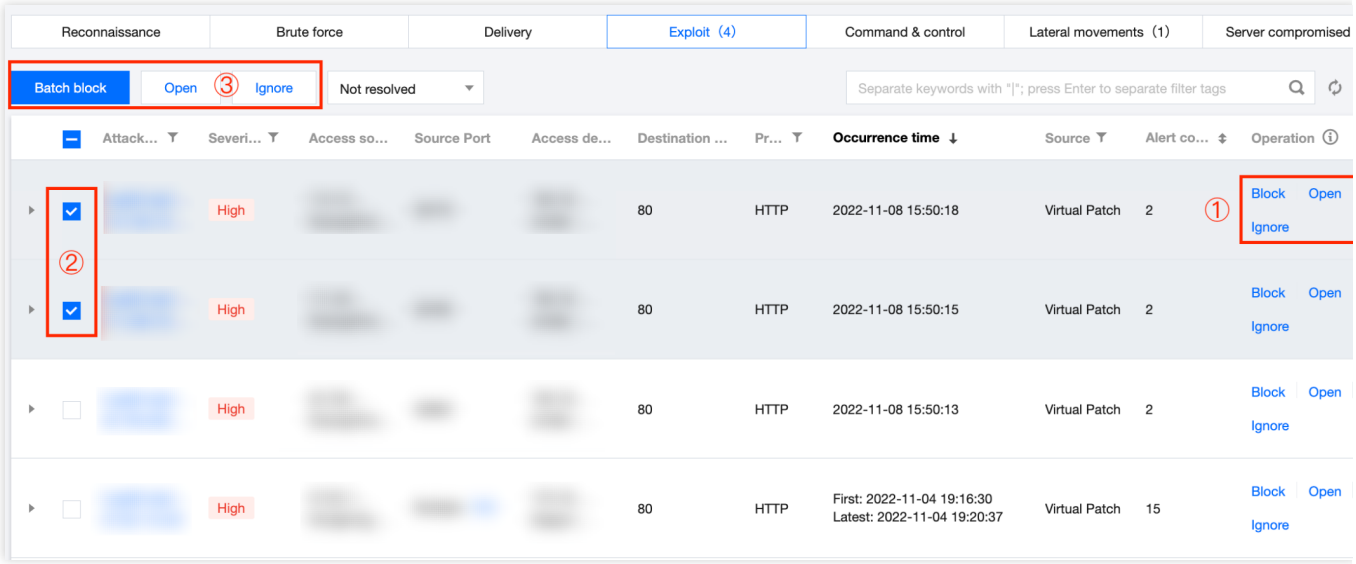
Note

To view all critical or high-risk events, select the level from the ④**Severity** column and then view the events by clicking different types of ②**alert events**.

You can also enter keywords in the search bar on the right to search for the events you need.

Resolving alert events

This section describes how to resolve alert events. For more information about how to filter alert events, please see "Filtering alert events".

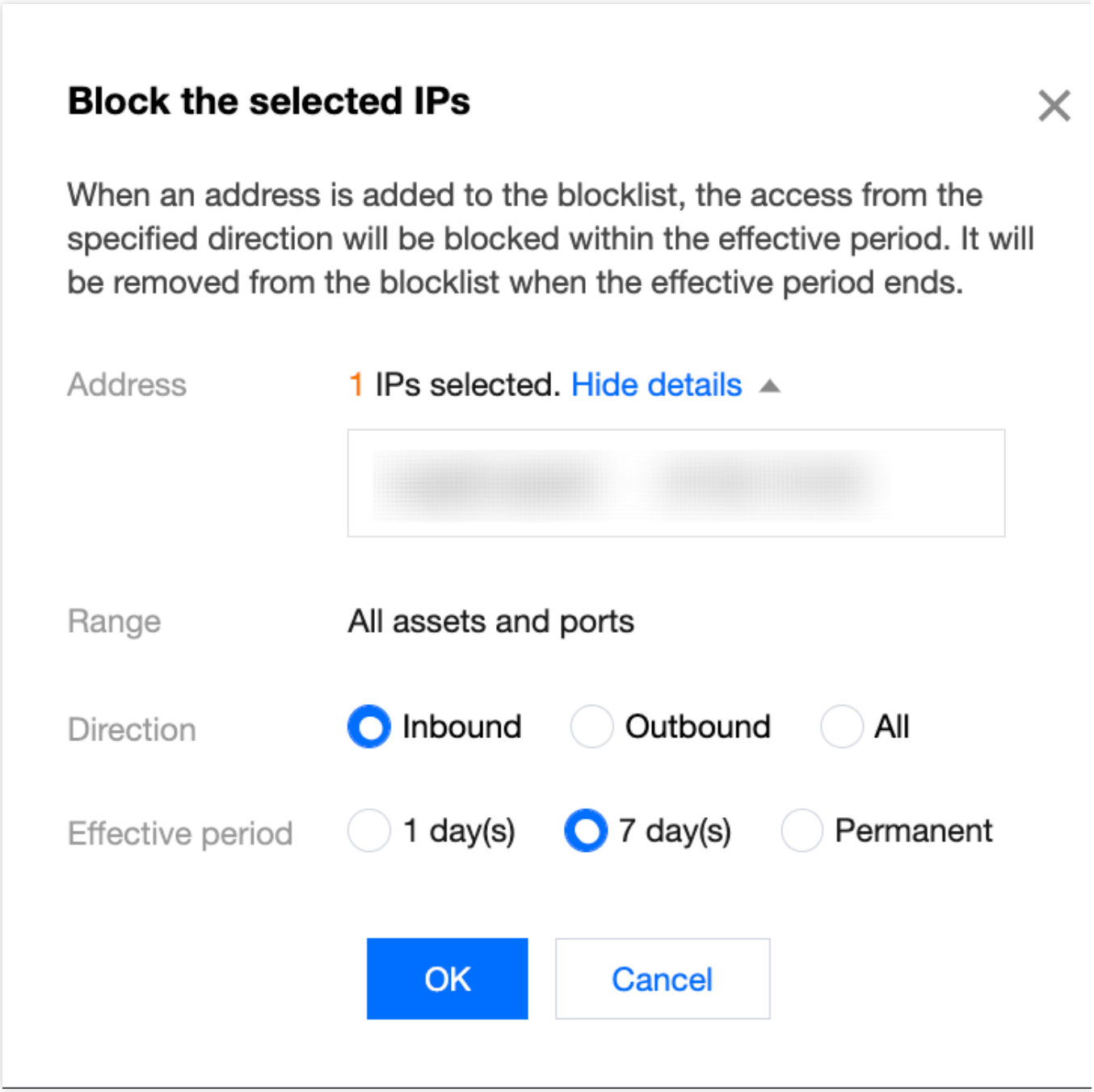


① You can click **Block**, **Allow**, or **Ignore** to resolve an alert.

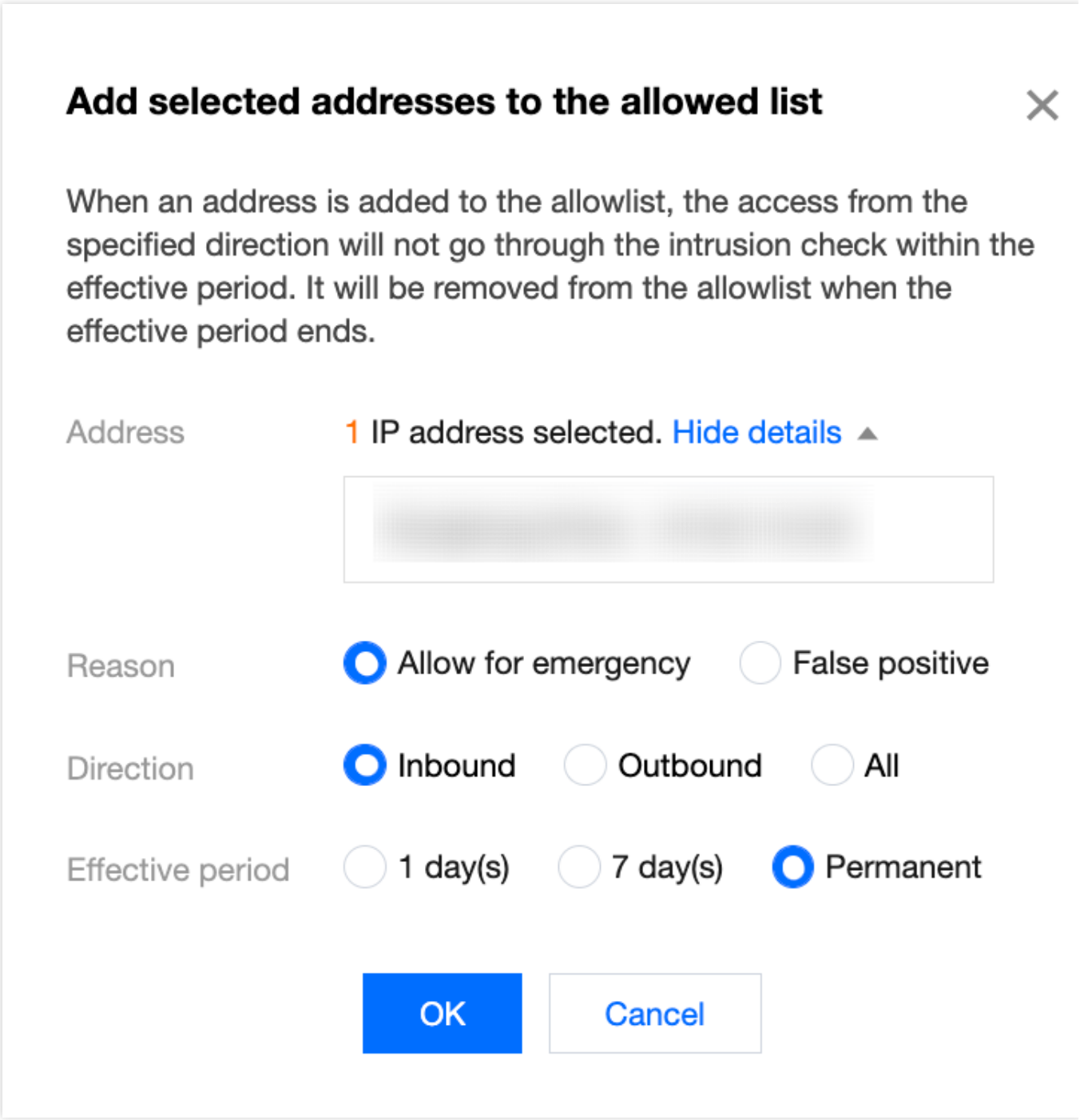
Note

To modify your operation, undo the operation in **Intrusion defense** -> **Blocklist**.

Block: For security events with a higher severity or a larger number of alerts, click **Block** to add the IP to the blocklist in Intrusion defense. CFW automatically blocks access from this IP to all your assets within the specified period.



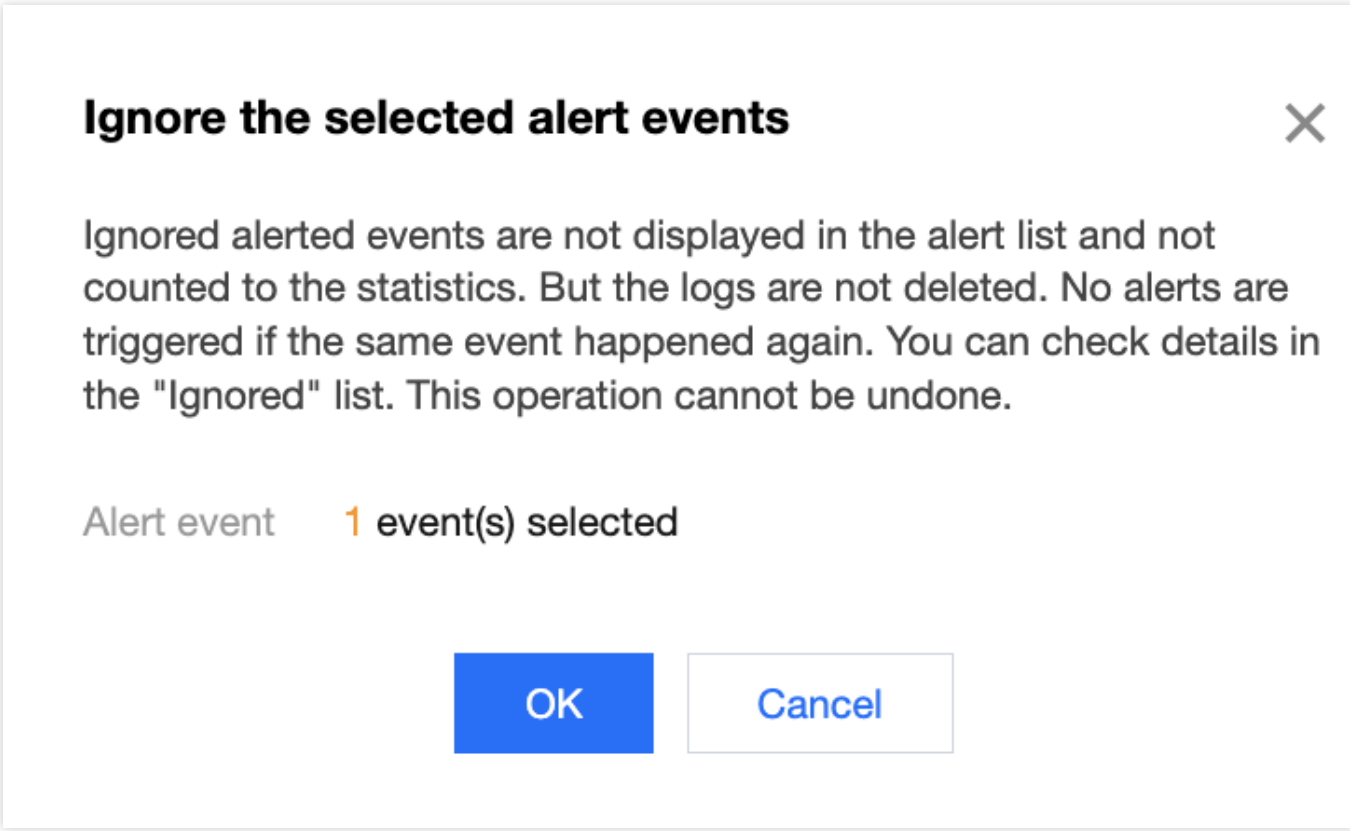
Allow: For repeated or possible false alerts, you can click **Allow** to add the IP to the allowlist in Intrusion defense. CFW allows traffic from the IP by skipping attack detection for the IP in **Intrusion defense** within the specified period.



Ignore: If you do not want to take action on an alert, click **Ignore**. The log is not deleted. You can view the log in the list of ignored alerts.

Caution

"Ignore" operation is irreversible.



② Select multiple alert events in the area marked "②" on the left.

Note

To select alert events across pages, select the target events on the current page and then go to another page to select more events.

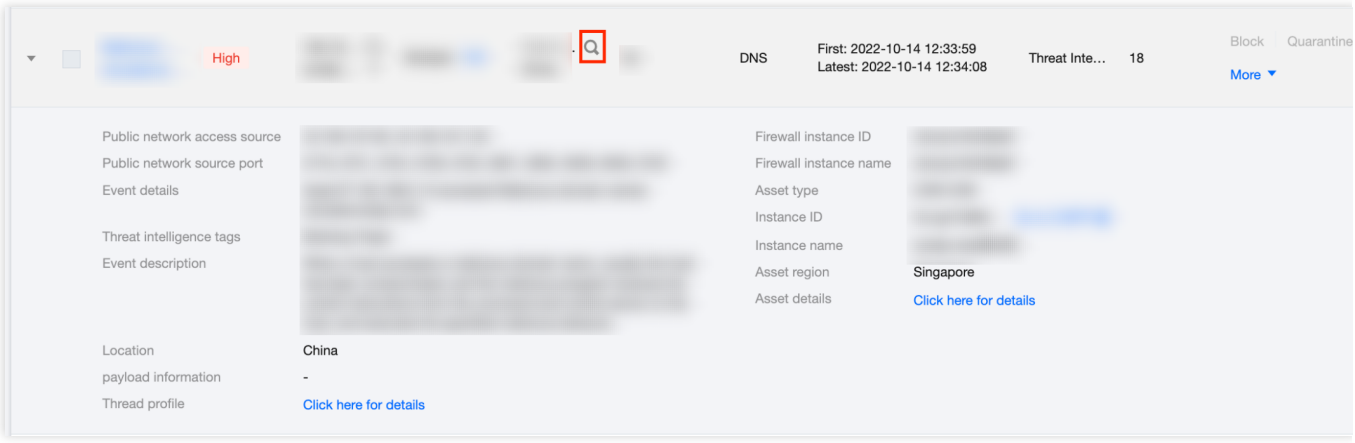
This applies to all multi-selection scenarios.

③ You can click **Block all**, **Allow**, or **Ignore** to batch resolve multiple events.

Searching for security events of an IP

This section describes how to search for all security events of an IP. Locate a security event of the IP of your interest, and click

to the right of the IP to list all security events of the IP.



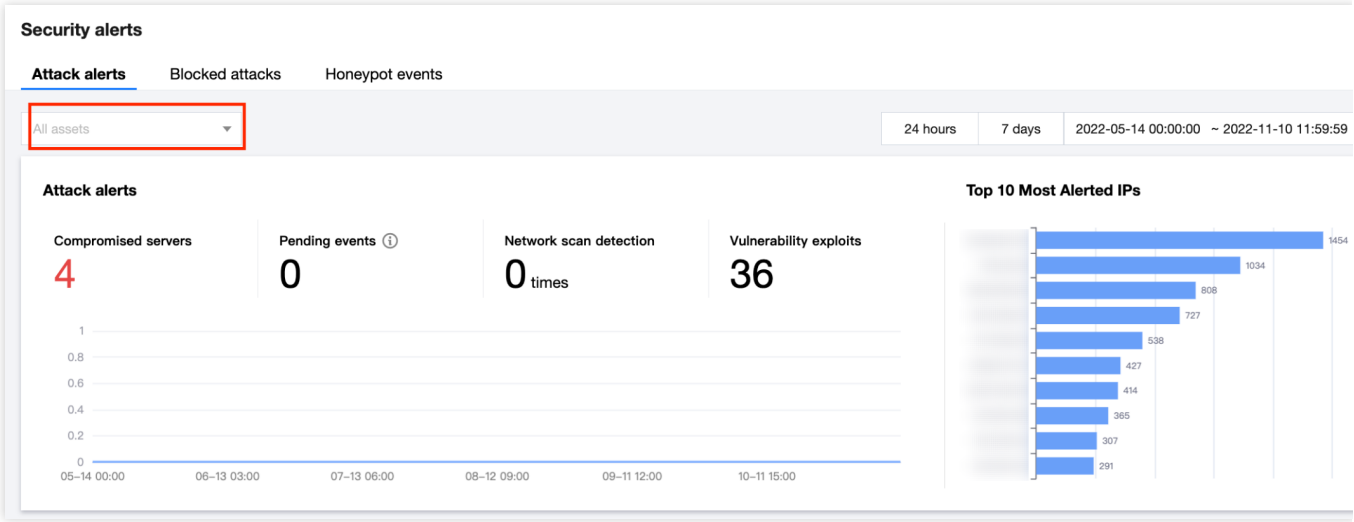
Note

This applies to all the scenarios where you need to filter security events of IPs, regardless of the IP types.

Searching for security events of an asset

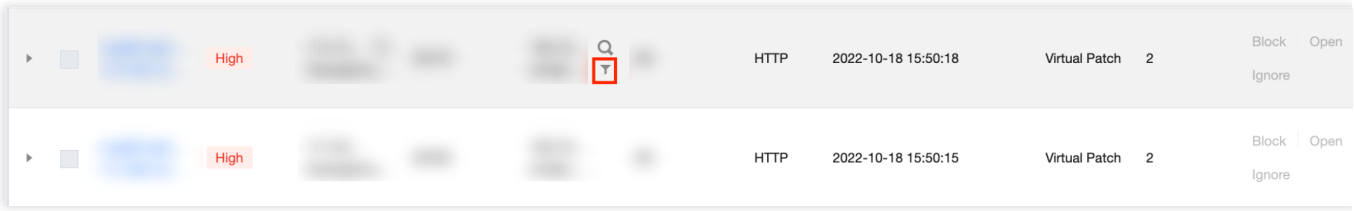
This section describes how to search for all security events of an asset.

Method 1: In the drop-down list in the upper-left corner of the view, select the target asset.



Method 2: Locate a security event of your interest, and click

to the right of the asset.

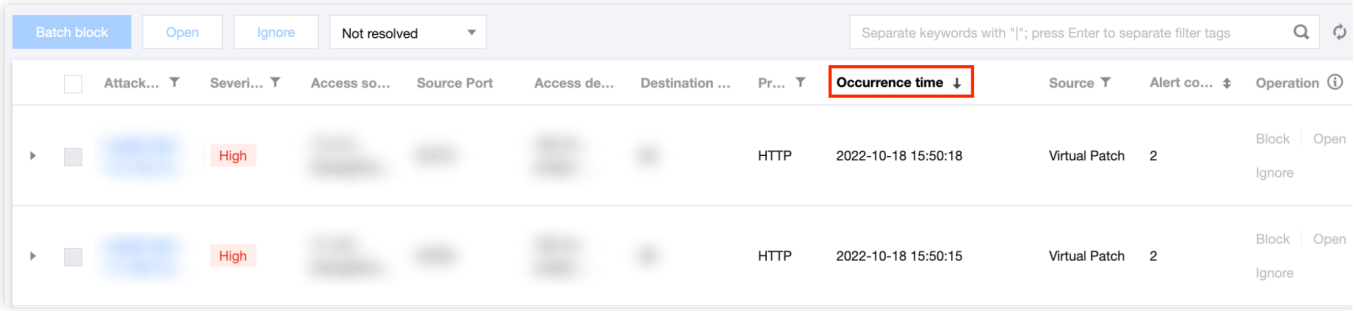


Note

This applies to all scenarios where you need to view events by asset.

Viewing recent security events

To view the recent security events, select all assets and all sources, and then click the arrow to the right of **Occurrence time** to sort the security events in reverse chronological order. You can switch between different alert types by clicking the tabs on the top. For more information, see **Filtering alert events**.



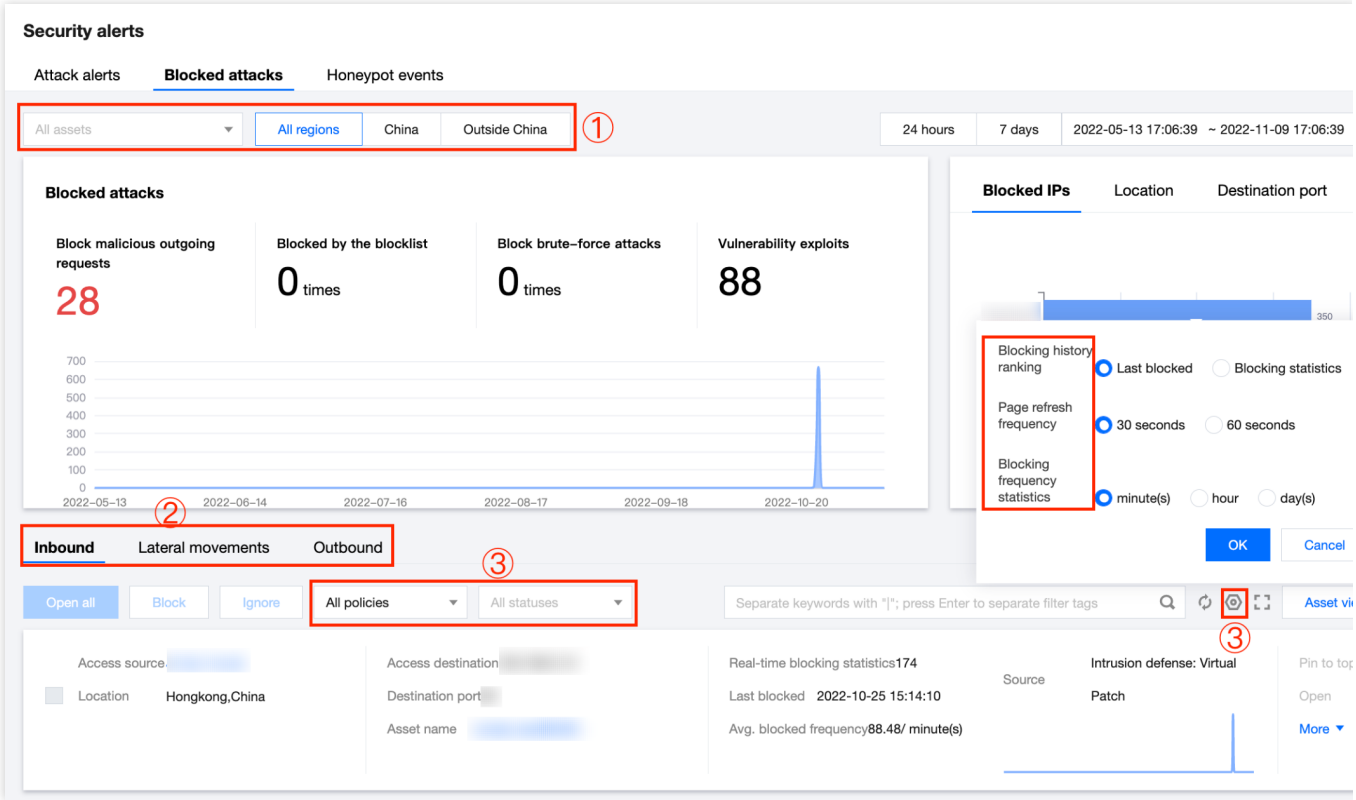
Blocked Attack Analysis and Handling

Last updated：2024-01-24 15:48:25

This topic describes the operations in **Alert Management**. Log in to the Cloud Firewall console. In the Alert Management page, click **Blocked attacks** to open the **Blocked attacks** page. This page displays a trend chart of blocked attacks, blocked IPs, regions, and destination ports to help you analyze and protect your assets.

Filtering blocked attacks

This section describes how to find the blocked attacks you want to view through filtering.
① Select the assets and regions for which you want to view the blocked attacks;
② Select **Inbound**, **Lateral movement**, or **Outbound**.
③ Select the intrusion defense policy and resolution status. You can filter the records by specifying **Blocking history ranking**, **Page refresh frequency**, and **Blocking frequency statistics**.

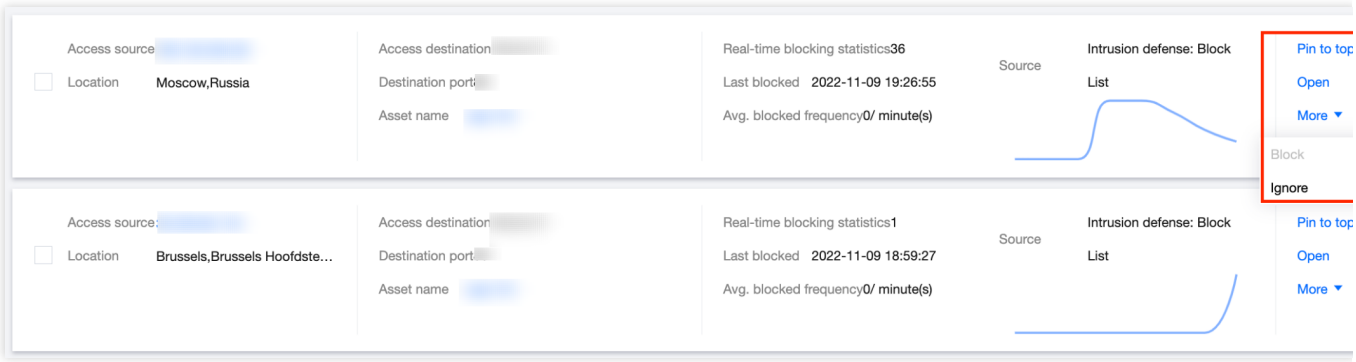


Note

The above describes the operations in the asset view. For more information about operations in the event view, please see **Filtering alert events**.

Resolving blocked attacks

1. This section describes how to resolve blocked attacks. For more information about how to filter blocked attacks, please see "Filtering blocked attacks".

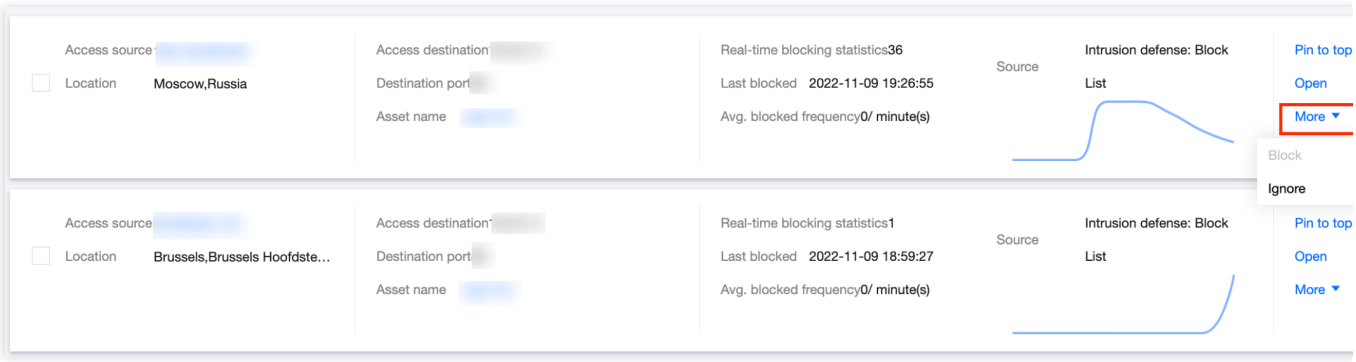


Note

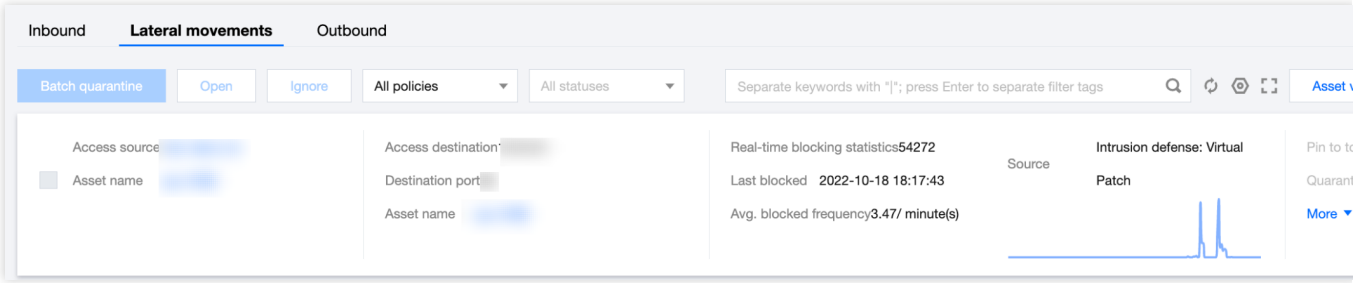
To modify your operation, undo the operation in **Intrusion defense** -> **Blocklist**, **Allowlist**, or **Quarantined list**.

2. On the **Blocked attacks** page, you can search for different assets and IPs by selecting **Inbound**, **Lateral movement**, or **Outbound**.

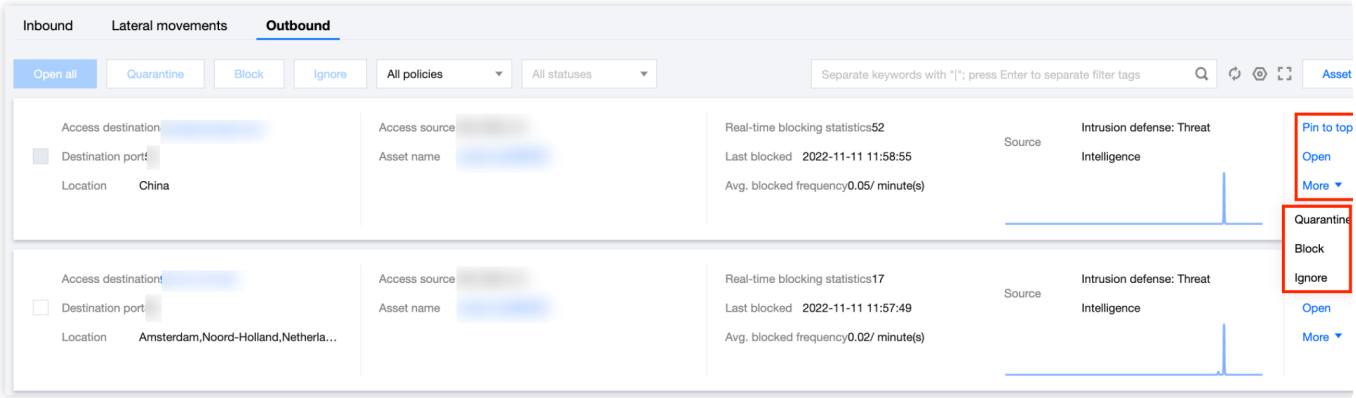
You can pin or allow the access source IPs that have been blocked in the inbound direction. For the allowed IPs, you can select **More** -> **Block** to block them if necessary.



For the assets and IPs involving lateral movement attacks, you can view the blocking history here.



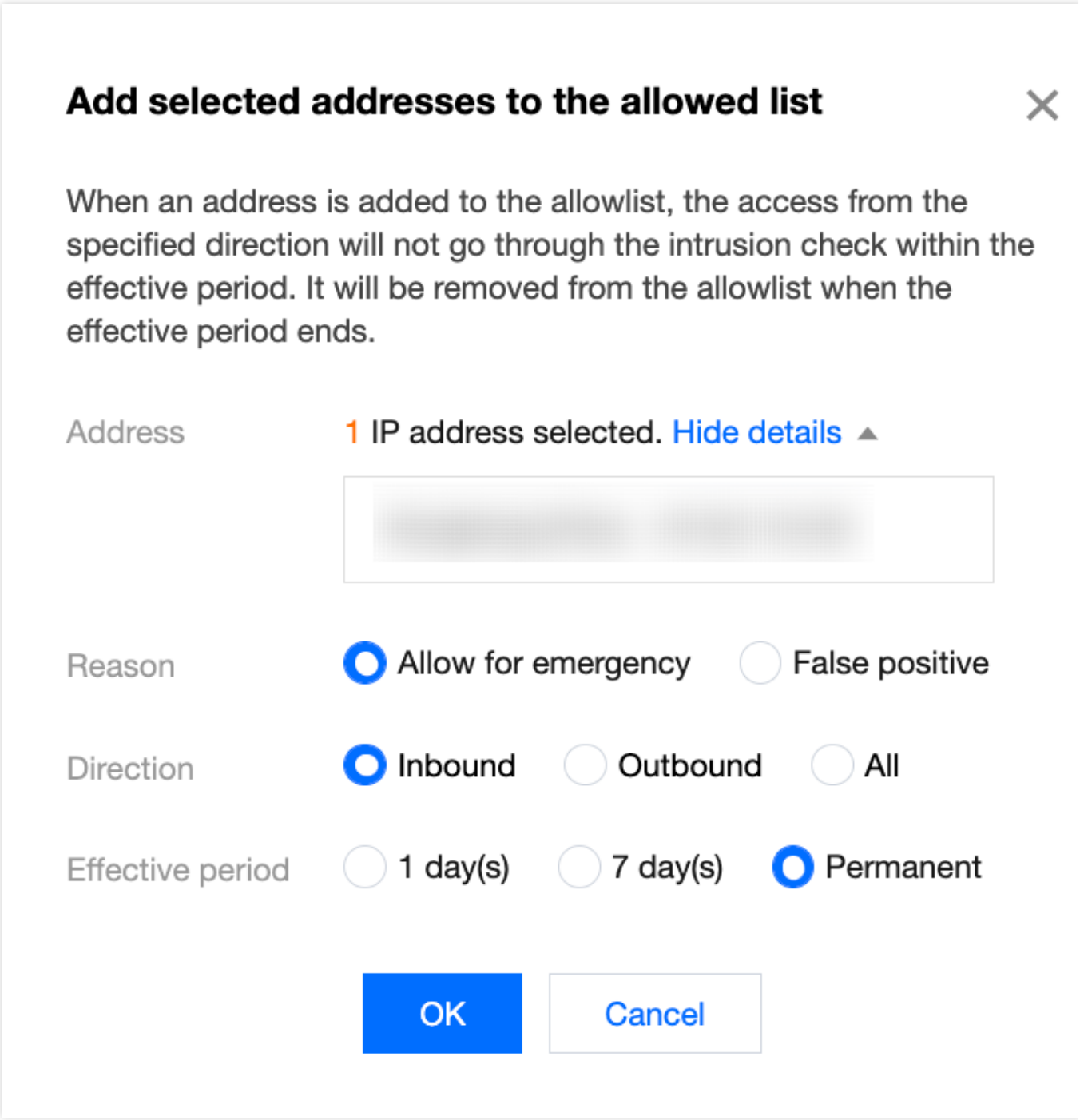
You can pin, allow, quarantine, block, or ignore the assets/IPs blocked by the **Intrusion defense** module in the outbound direction.



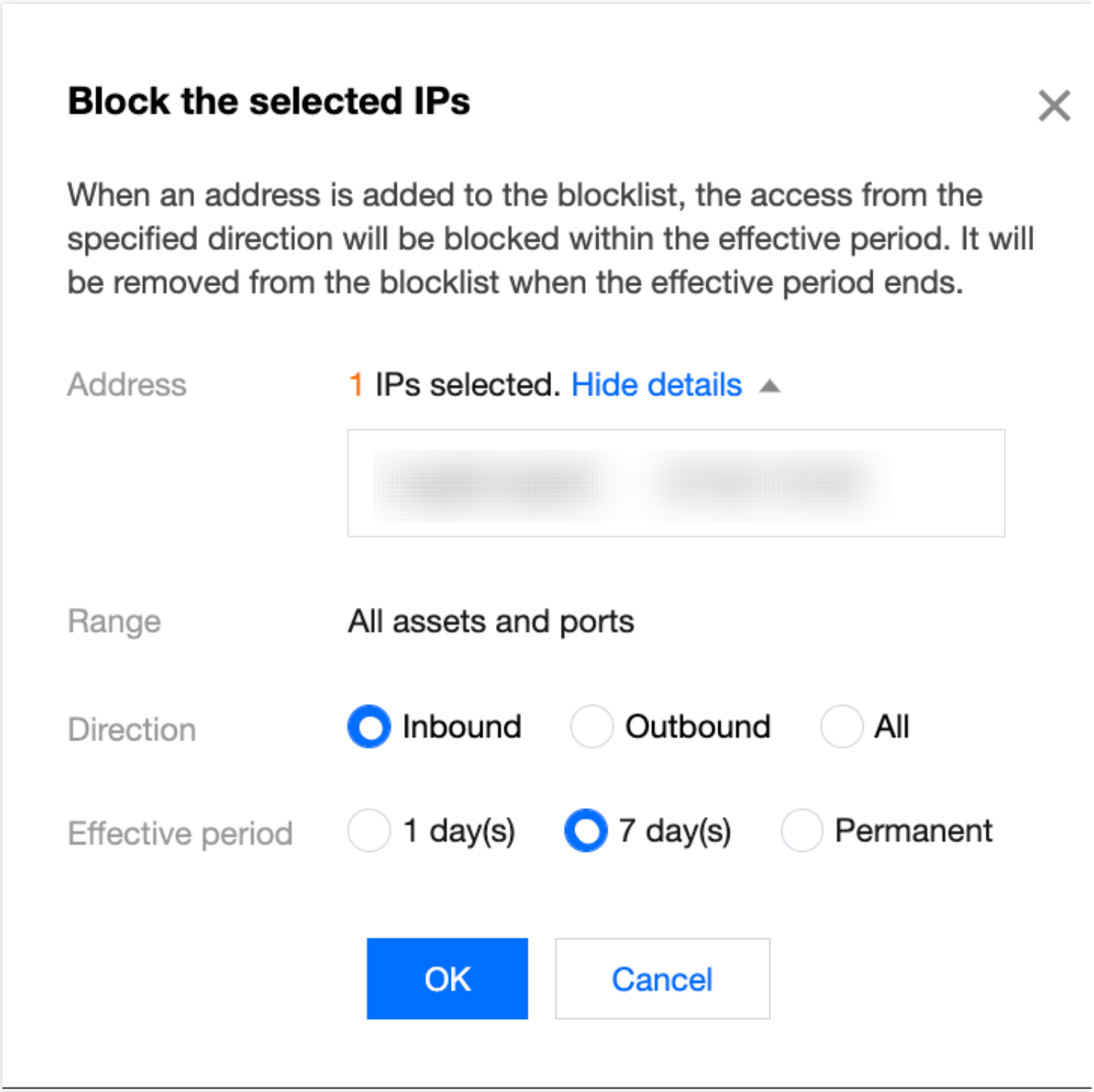
3. You can perform the following operations on different assets/IP addresses:

Pin to top/**Unpin**: You can pin or unpin assets. Note: A maximum of 5 items can be pinned for **Outbound** or **Inbound**.

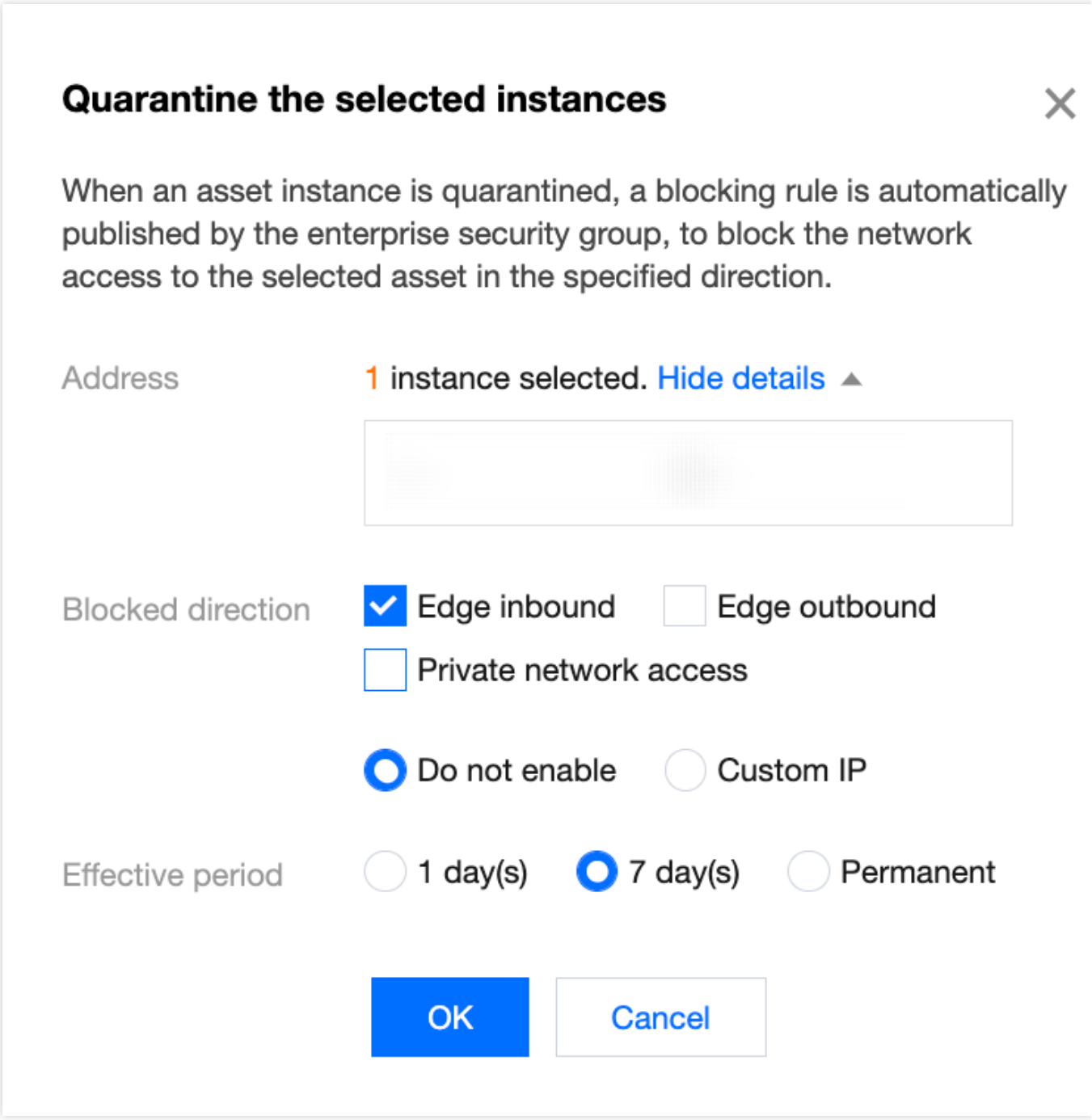
Allow: Click **Allow** for an IP that does not need to be blocked. Then, select **Reason**, **Direction**, and **Validity**. The IP will be in the allowlist in the **Intrusion defense** module within the selected period. CFW allows traffic from the IP by skipping attack detection for the IP in **Intrusion defense** within the specified period. If you are not certain about whether the reason is "false positive", you can select **Allow for emergency**, and modify it later if necessary.



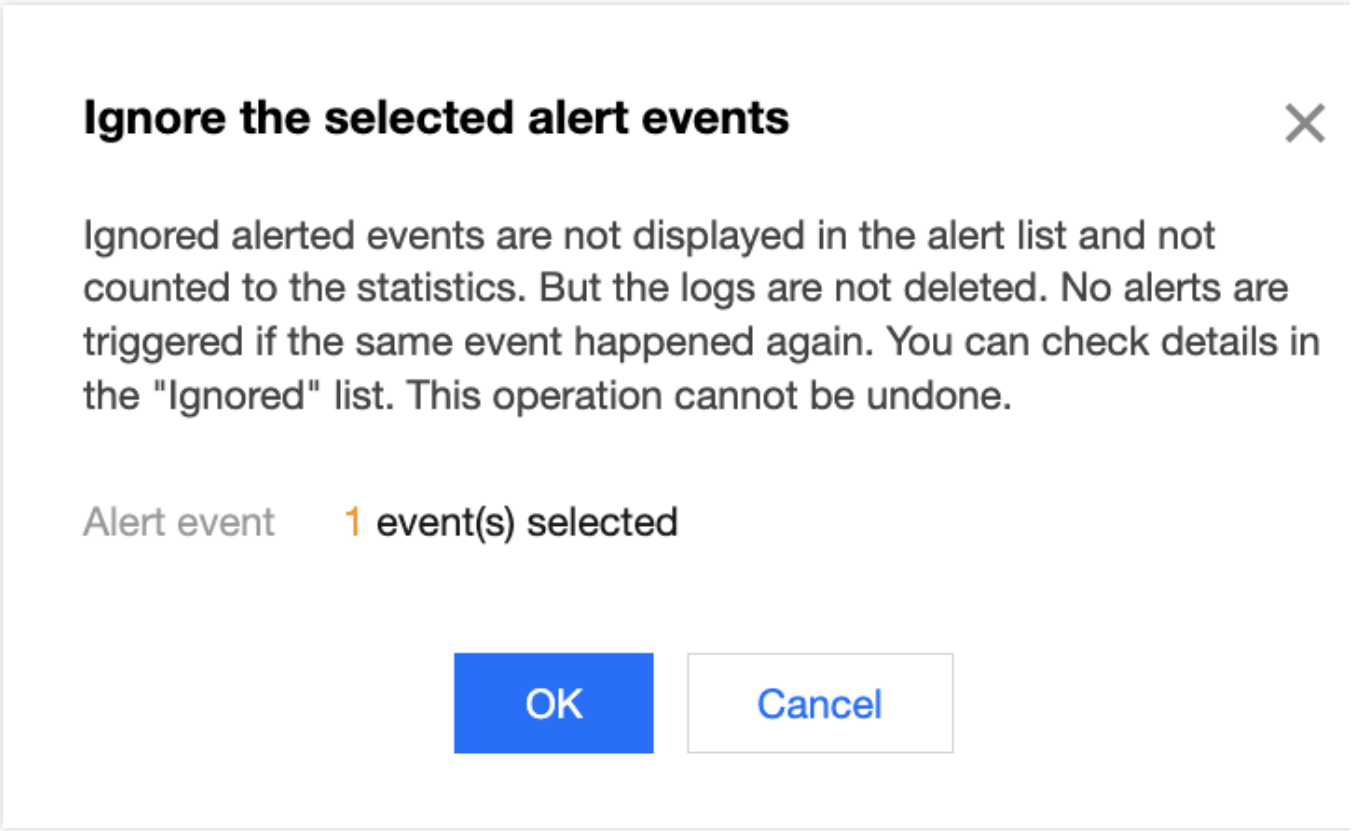
Block: For assets with a high threat level, click **Block**. Then, specify a validity period and direction to add the IP to the blocklist in **Intrusion defense**. CFW automatically blocks that IP from accessing all of your assets within the specified period.



Quarantine: Click **Quarantine**. When an asset instance is quarantined, the system automatically publishes the blocking rule for enterprise security groups to block network access to the selected asset in the specified blocking direction. This makes the subsequent troubleshooting easy and prevents the asset from being attacked.

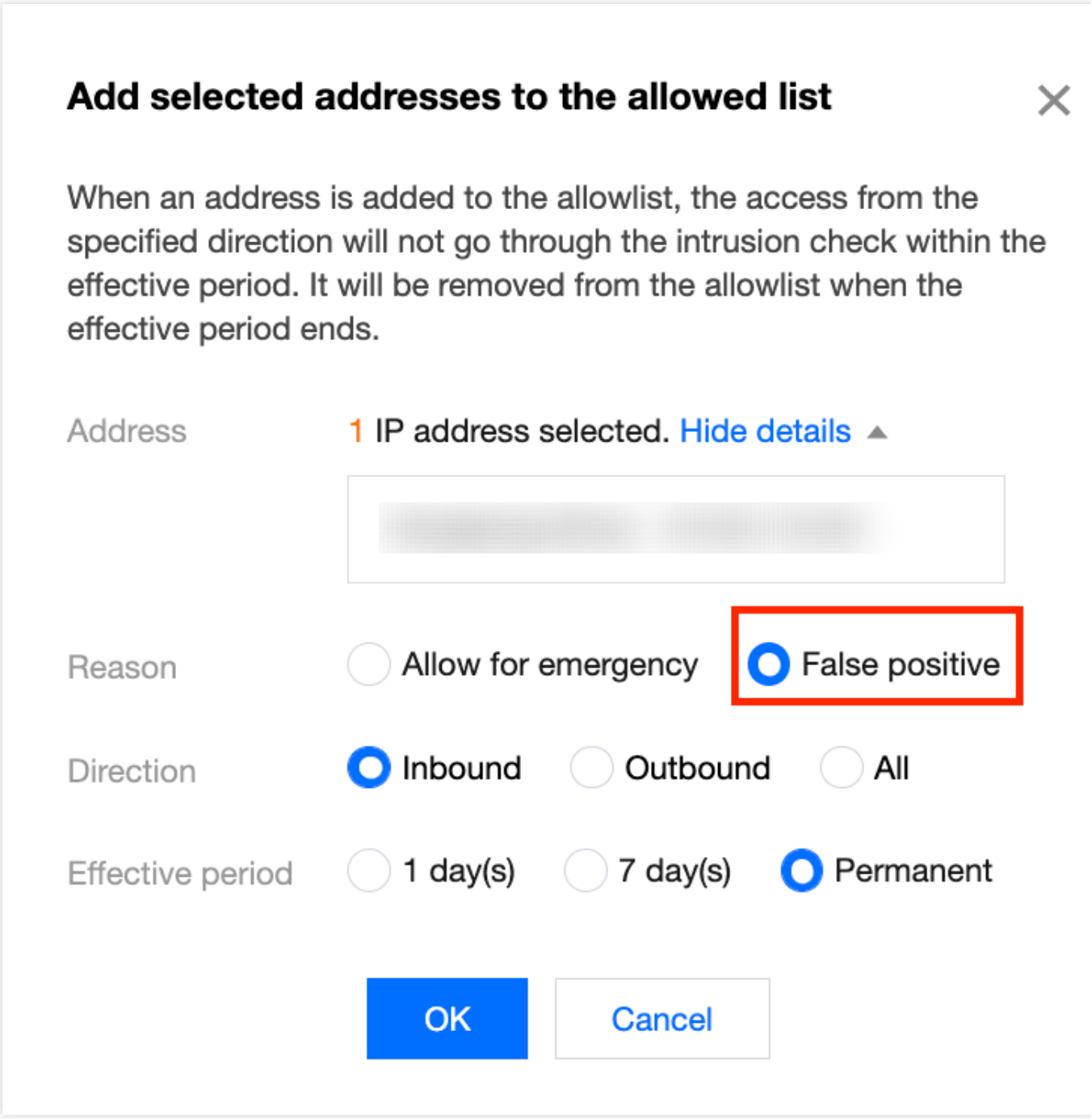


Ignore: For repeated or possible false alerts, you can click **Ignore**. The ignored alert events are not included in the alert list and statistics, but their logs are retained. You are no longer notified of the ignored alert events when they trigger alerts again. You can select **Ignored** in the list to view all the ignored events. **The "Ignore" operation is irreversible.**



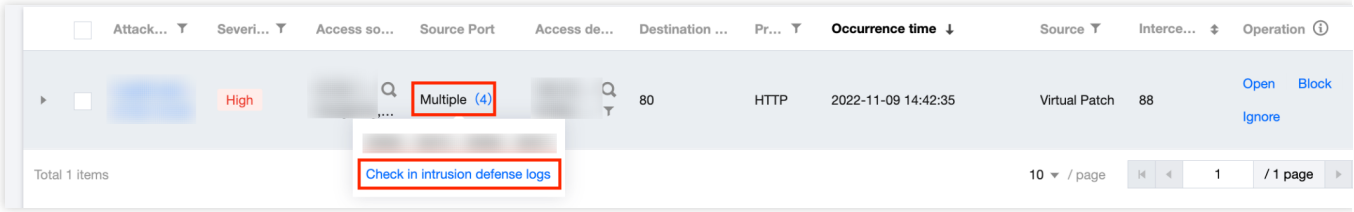
Resolving false alerts

You can add the IP to the allowlist. On the **Blocked attacks** page, select the target asset/IP, click **Allow**, select **False positive** for **Reason**, and then click **OK**.



Searching for attack events from an IP

In the **Asset view**, place the pointer over the value of **Access destination**, **Access source**, or **Asset name**, and click **Check in intrusion defense log** to view all attack events.

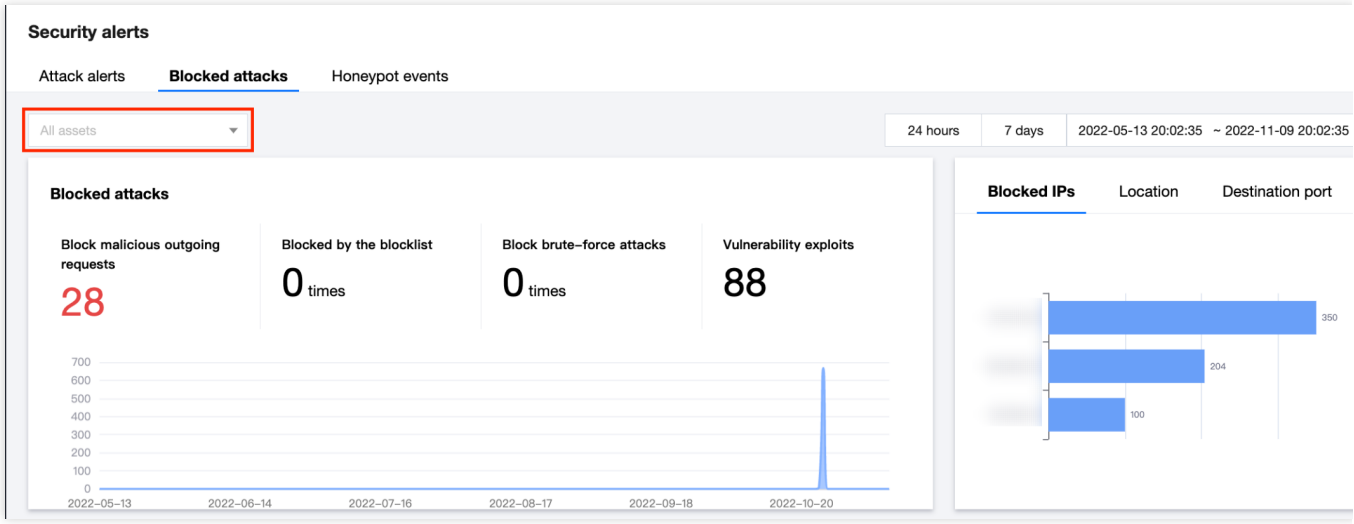


Note

The figure above shows the process.

Viewing the blocked attacks for an asset

Method 1: Select the specified asset in the upper-left corner to filter the records.

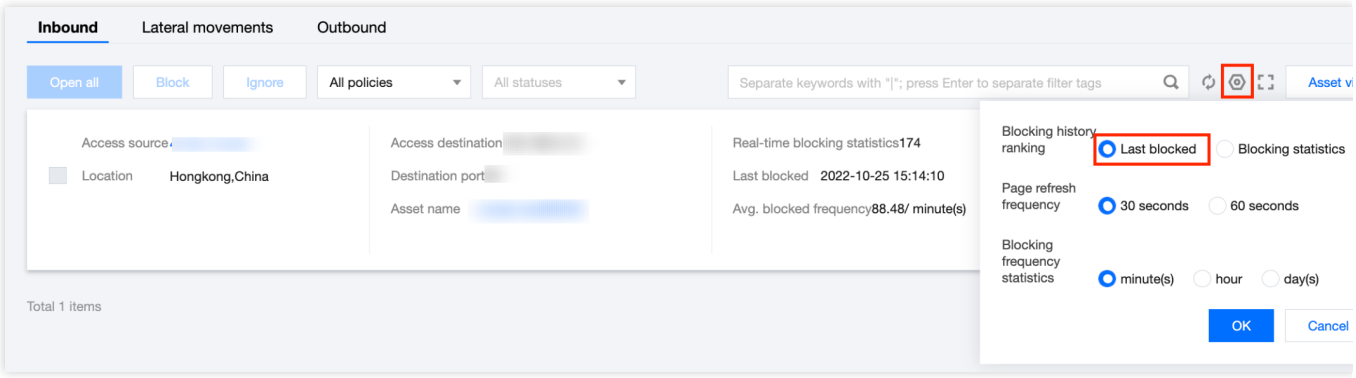


Method 2: Select the target asset by clicking **Event details** -> **Asset name** to view its records of blocked attacks.

Viewing recently blocked attacks

The **Blocked attacks** page is automatically refreshed. Click

in the upper part of the page, select *Last blocked for* ***Blocking history ranking****, and then click OK** to view the recently blocked attacks.


Inbound
Lateral movements
Outbound
Open all
Block
Ignore
All policies
All statuses
Separate keywords with "|"; press Enter to separate filter tags
Asset v
Access source
Location
Hongkong,China
Access destination
Destination port
Asset name
Real-time blocking statistics174
Last blocked 2022-10-25 15:14:10
Avg. blocked frequency88.48/ minute(s)
Total 1 items
Blocking history ranking
Last blocked
Blocking statistics
Page refresh frequency
30 seconds
60 seconds
Blocking frequency statistics
minute(s)
hour
day(s)
OK
Cancel

Traffic Monitoring

Last updated：2024-01-24 15:48:25

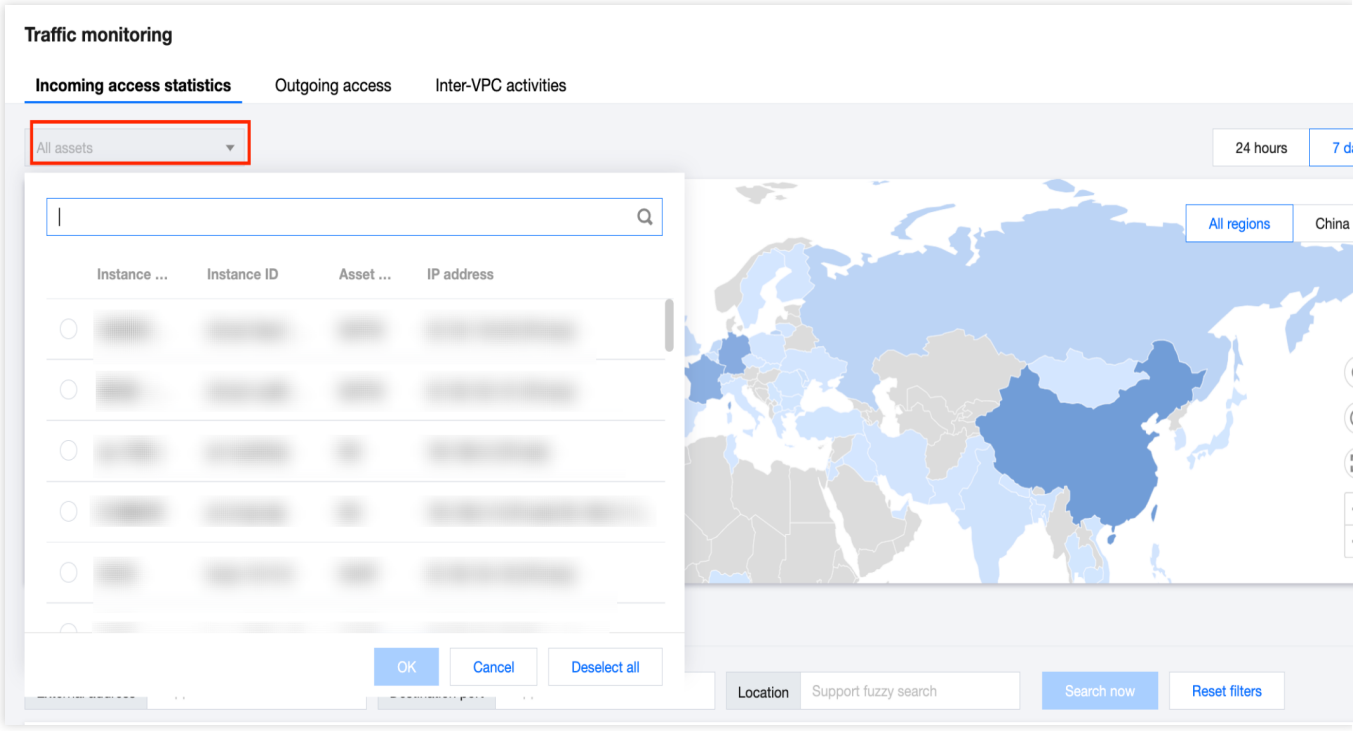
Traffic Monitoring provides incoming access statistics, outgoing access analysis, and inter-VPC activities tabs based on inbound, outbound, and inter-VPC traffic. This topic describes how to view the traffic status and understand the visual information on the three tabs in Traffic Monitoring.

Incoming access statistics

On the **Incoming access statistics** page, you can view the IP addresses, access count, and volume of the inbound traffic. You can also view details about the access to specific assets in different time periods in specified regions on the map, and view the ranking of traffic in different regions.

Directions

1. Log in to the Cloud Firewall console, click **Traffic Monitoring** in the left navigation pane, and click the **Incoming access statistics** tab.
2. In the **Incoming access statistics** tab, click **All assets** to view the access to each asset in the current region. You can also view the traffic in different time periods, such as the last 24 hours or the last 7 days.

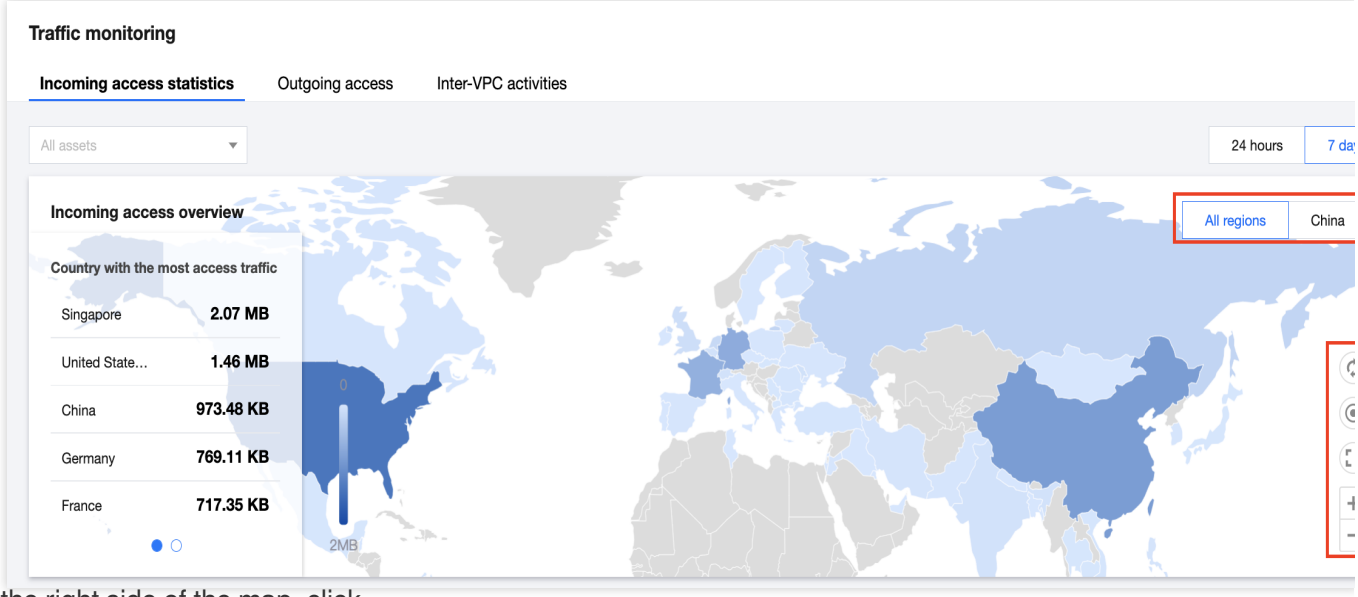


3. View the incoming access to assets in regions around the world and within China on the map.
Select **All regions** to view the distribution of traffic in each country or region around the world.

Select **China** to view the distribution of traffic in each province of China.

Caution

The carousel slider on the left side displays the top 5 countries/regions or provinces with the highest traffic volume and access count. You can hover the mouse cursor over a country/region or province to view the access by IP addresses.
The color depth on the map indicates the traffic volume in each region. A darker color indicates higher traffic. You can hover the mouse cursor over a country/region or province to view details.
The icons on the right side are used to refresh data in the carousel slider, reset the map to the initial position, expand the map, and zoom in and out the map.



4. On the right side of the map, click

to view the traffic statistics in the global mode.

5. In the global mode, view the rankings in different dimensions.

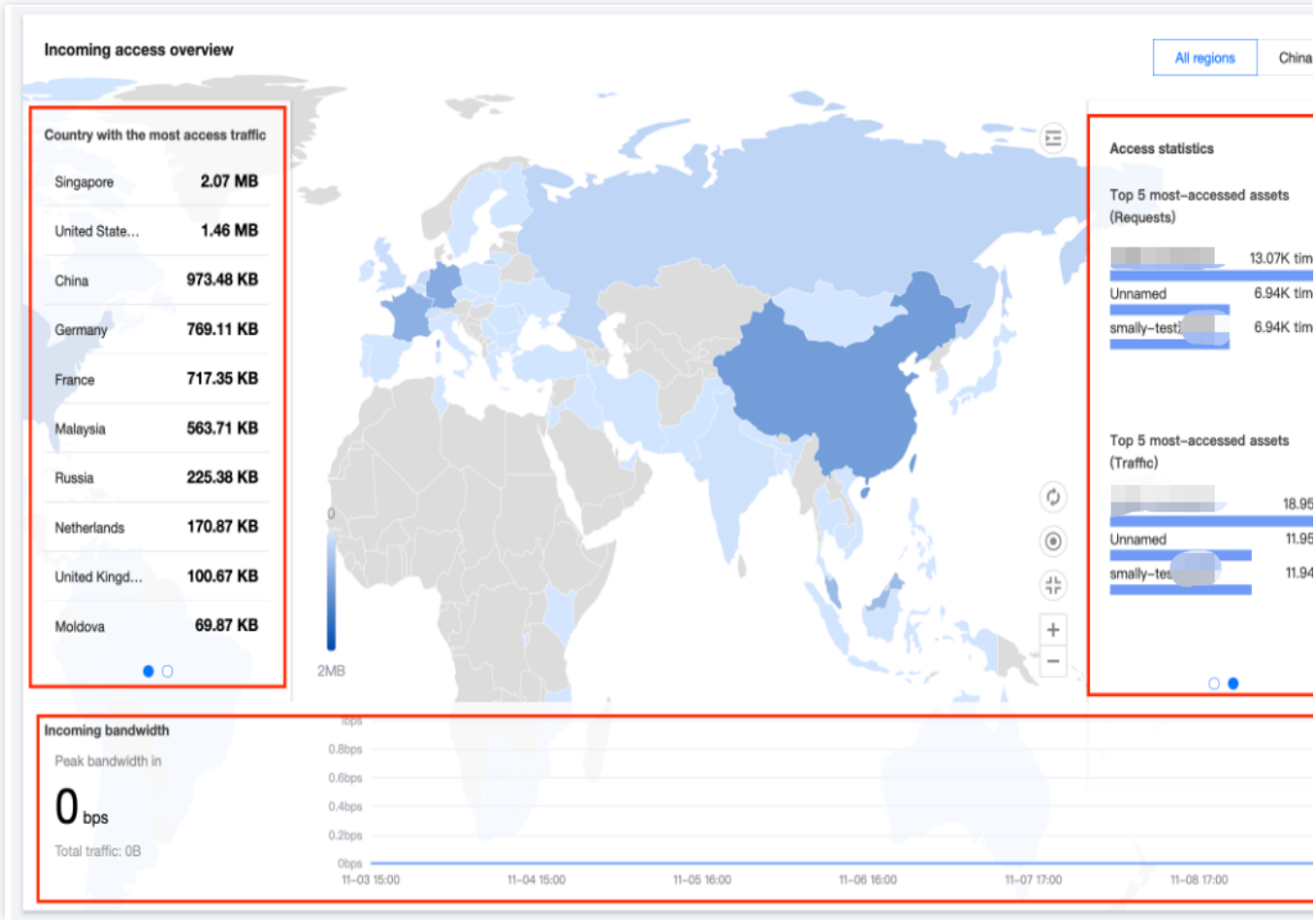
The carousel slider on the left side of the map displays top 10 countries/regions or provinces with the highest traffic volume and access count.

The carousel slider on the right side of the map displays the top 5 ports with the most visits, the protocol distribution of incoming access, the top 5 assets with the most visits, and the top 5 assets with the highest traffic volume.

Note

When a specific asset is selected, the asset ranking is not displayed in the carousel slider on the right side.

The line chart below the map shows the traffic bandwidth of incoming access within the current time range. You can also view the peak bandwidth in and the total traffic volume in the last 7 days or 24 hours.



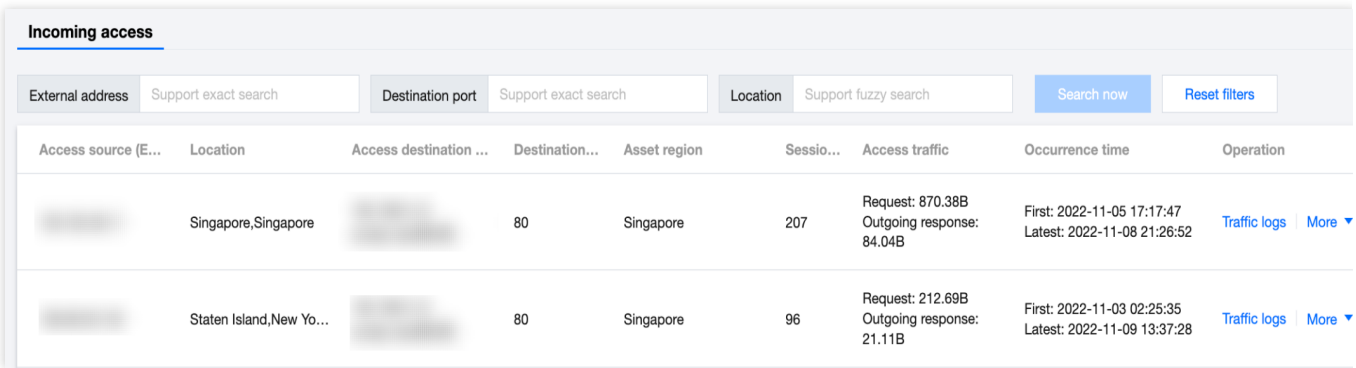
6. In the lower part of the page, view details of the incoming access IP addresses.

Note

For brevity, the list only displays the access information of top 500 IP addresses by default.

The features of the **Incoming access** list under **Internet access** are described below, and those of other lists are similar.

1. In the **Incoming access** list, enter an **exact** IP address of an access source in the **External address** search box, enter an **exact** IP address of an asset in the **Destination port** search box, or enter an **exact or fuzzy** place name in the **Location** search box, and then click **Start search** to search for access details.



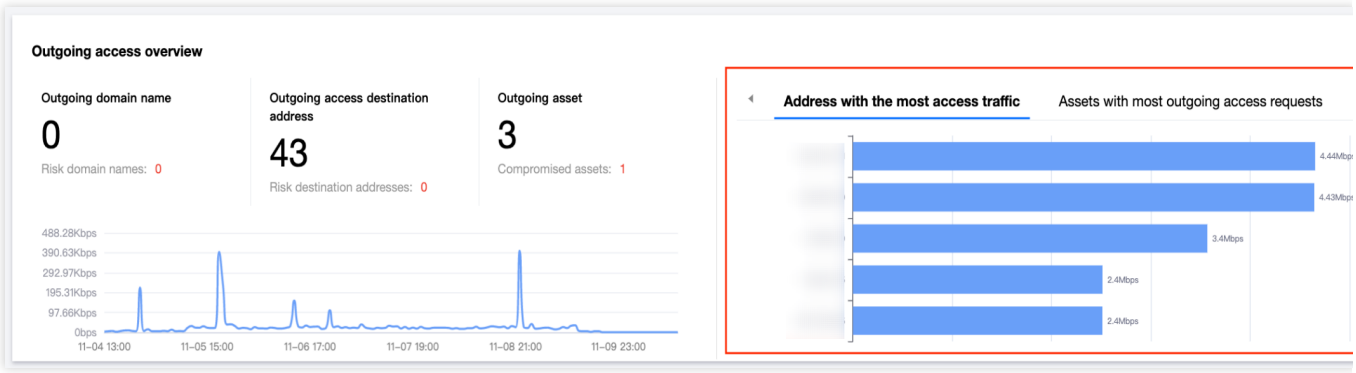
2. View data details. You can view traffic logs, threat profile, or asset details in the access list.
View traffic logs
2.1.1 Click **Traffic logs** in the action column on the right.
2.1.2 On the **Traffic logs** page, you can view details about the access between specified IP addresses. You can also filter the results by access source and access destination to obtain the details about the access from the same source to the same asset.
View the threat profile
2.1.1 Select **More** -> **Threat profile** in the action column on the right.
2.1.2 On the **Threat profile** page, view the threat profile of the external address and then perform tracing and auditing.
View asset details
2.1.1 Select **More** -> **Asset details** in the action column on the right.
2.1.2 On the **Asset details** page, view exposed assets and security events about the asset.

Outgoing access analysis

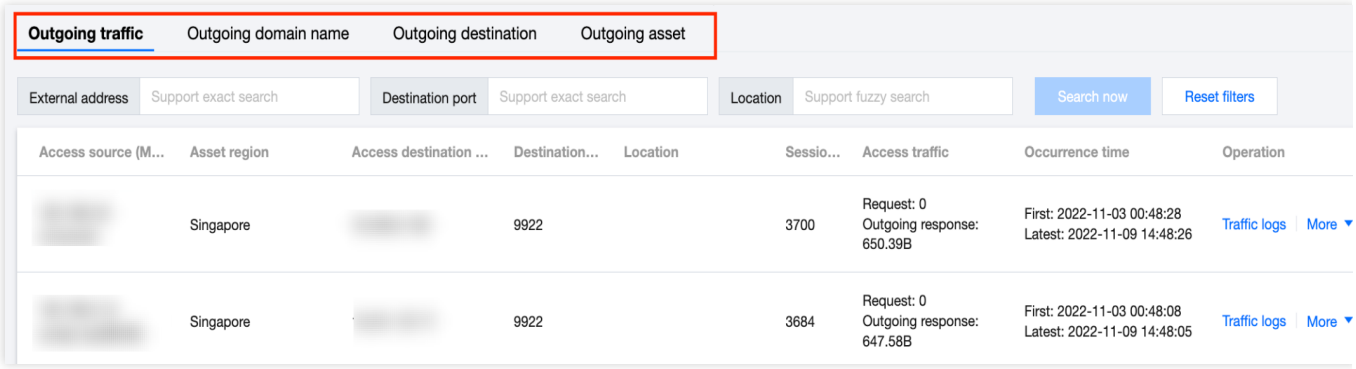
You can view details about the outgoing access from assets in the last 7 days, and learn about the outgoing traffic, outgoing domain names, and outgoing destinations on the **Outgoing access** page.

Directions

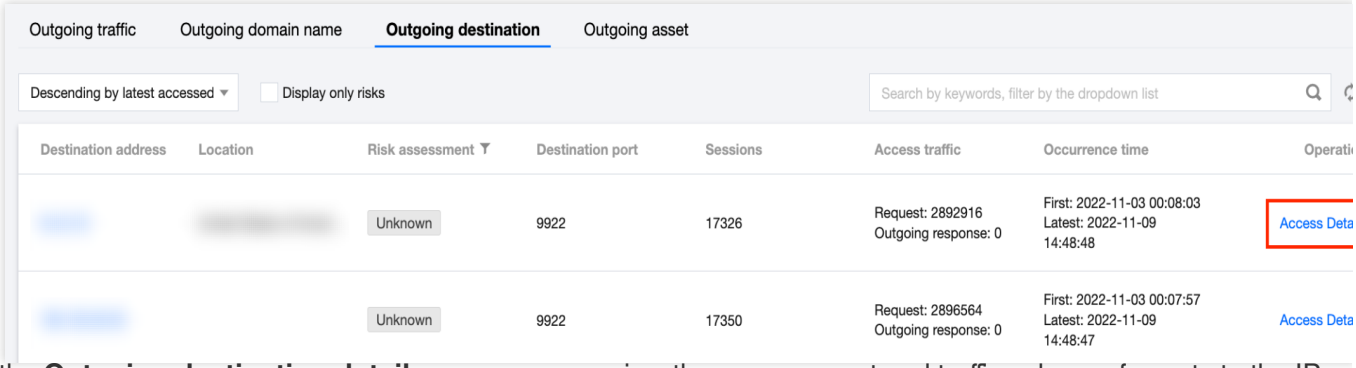
1. Log in to the Cloud Firewall console, click **Traffic Monitoring** in the left navigation pane, and click the **Outgoing access** tab.
In the **Outgoing access overview** module, you can view the access status of outbound traffic in the last 7 days or 24 hours. You can also filter the results by time and asset to obtain the outgoing access statistics of specific assets within a time range.
On the left side of the **Outgoing access overview** module, you can view the outgoing domain names and outgoing destinations of assets, the number of outgoing assets, and the number of alerts. You can select an asset from the **All assets** drop-down list to view the outgoing access of the asset.
In the line chart in the lower part, you can view the bandwidth in the last 7 days or 24 hours. Hover the mouse cursor over the line chart to view the bandwidth at a point in time.
On the right side of the **Outgoing access overview** module, you can view the top 5 most requested domain names, the top 5 most requested addresses, the address with the most access traffic, the top 5 assets with the most outgoing access requests, and the top 5 assets with the highest outgoing traffic in the last 7 days or 24 hours.



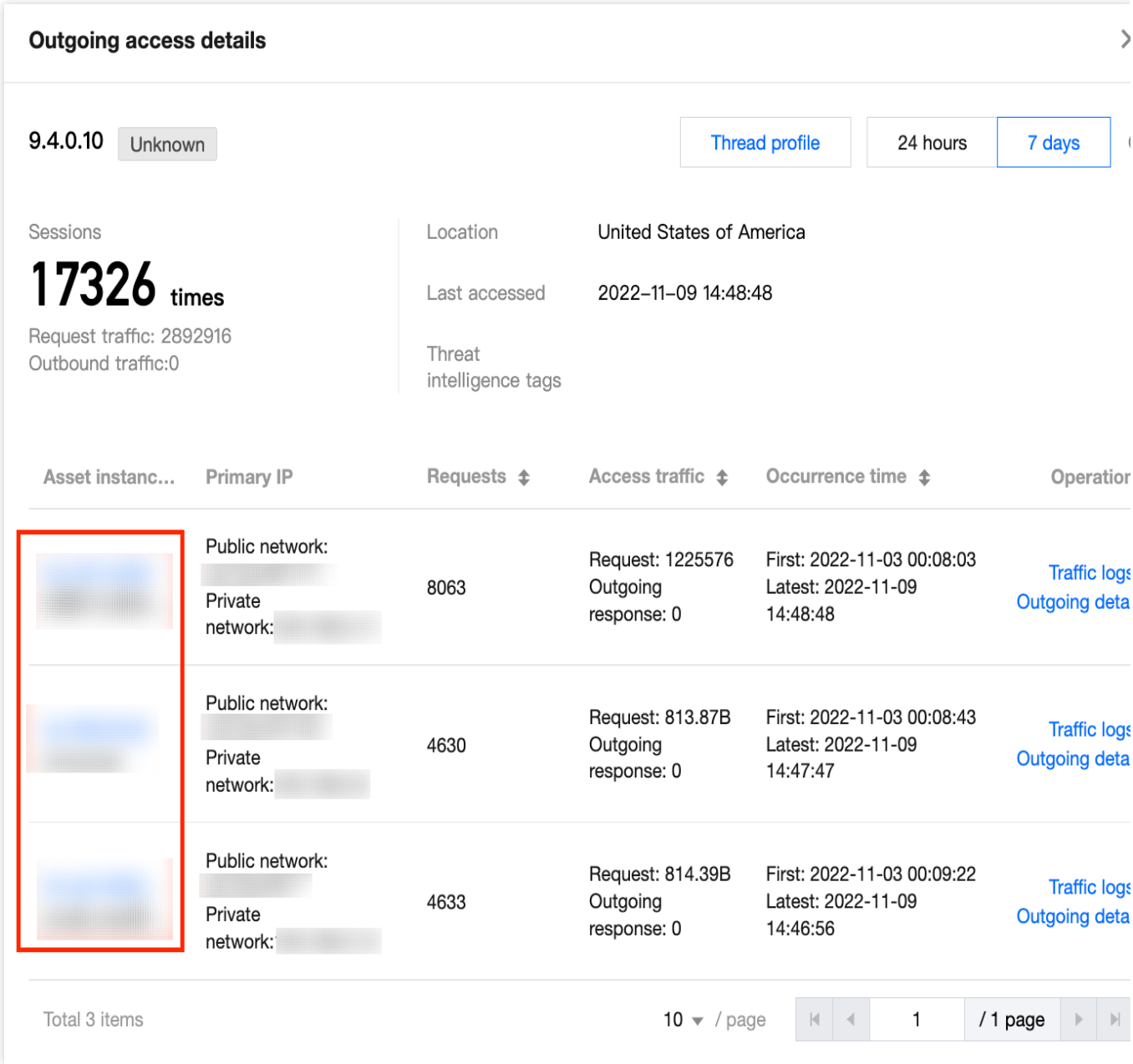
2. You can view the access statistics of outgoing traffic, outgoing domain names, outgoing destinations, and outgoing assets in the lists below. Access details are available in all the lists except the **Outgoing traffic**.



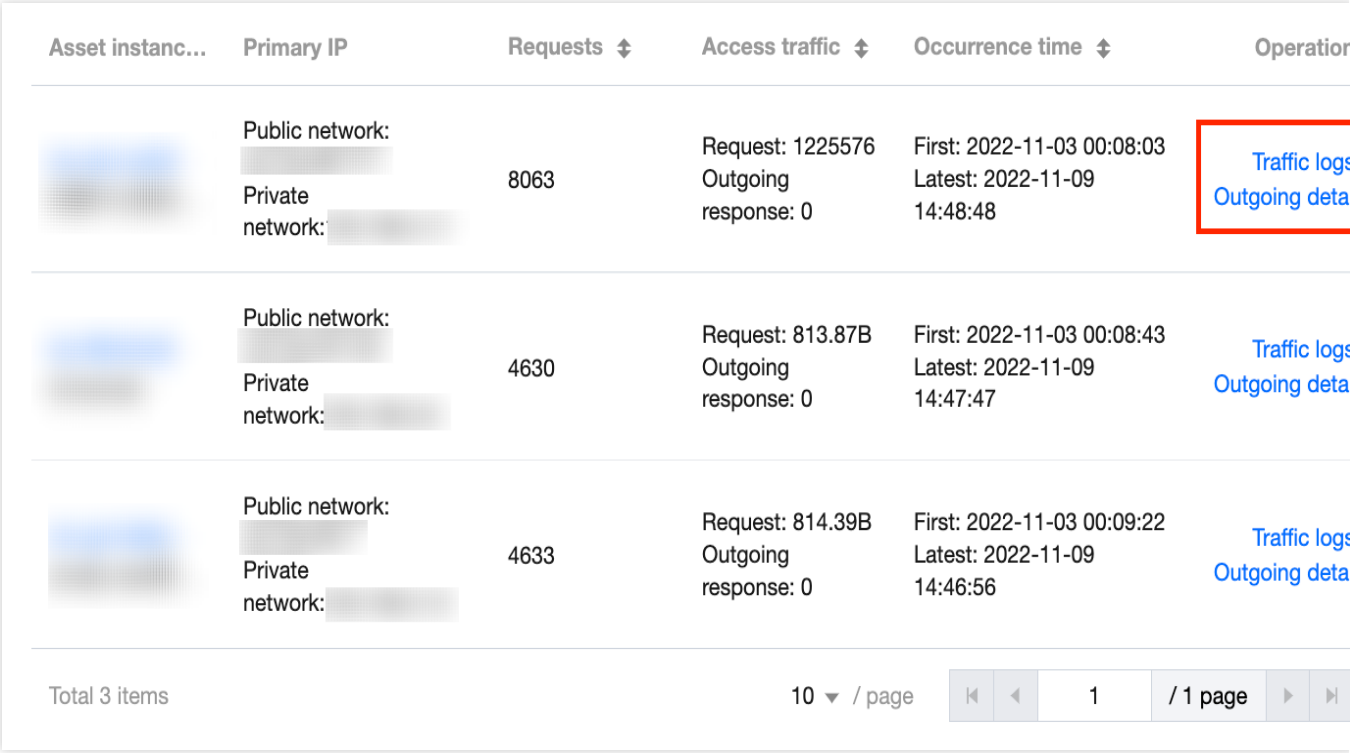
3. The **Outgoing destination** list is used as an example of how to view access details. Click **Outgoing destination**, and click **Access details** in the action column on the right side of an IP address to enter the **Outgoing destination details** page.



4. On the **Outgoing destination details** page, you can view the access count and traffic volume of assets to the IP address in the last 7 days or 24 hours, and the location of the IP address. You can also view the assets accessed from the IP address. To learn more about the traffic logs and threat profile, please see Incoming access statistics.



5. To learn more about the outgoing access of an asset in the list, click **Traffic logs** or **Outgoing details** in the action column on the right side of the instance list to view the traffic logs of the asset or the IP addresses and domain names accessed by the asset in the last 7 days or 24 hours.



Inter-VPC activities

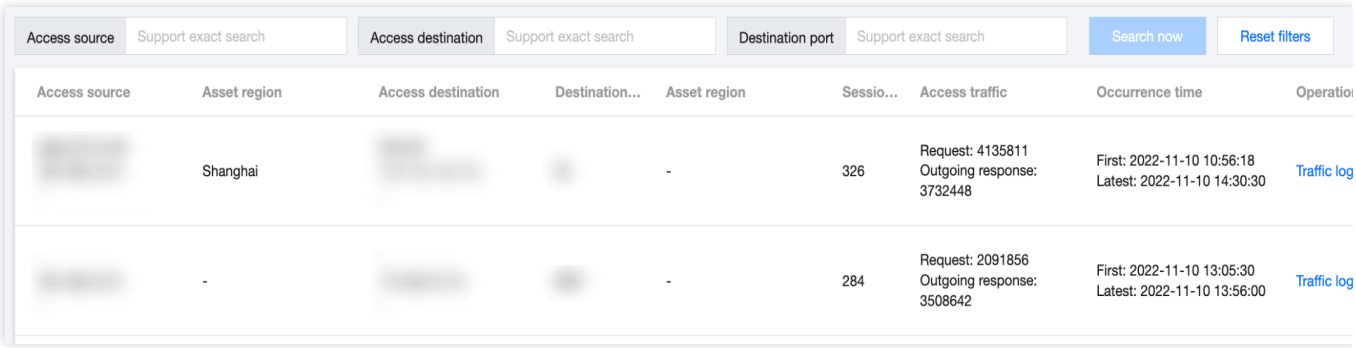
You can view traffic access between VPCs and the protocol distribution on the **Inter-VPC activities** page.

Directions

1. Log in to the Cloud Firewall console, click **Traffic Monitoring** in the left navigation pane, and click the **Inter-VPC Activities** tab.
2. In the **Inter-VPC activities** tab, select a VPC instance from the filter box in the upper part and select a time period.

3. Hover the mouse cursor over the line chart of traffic statistics to view the bandwidth at a specific time. Hover the mouse cursor over the donut chart of protocol distribution on the right to view the distribution of protocols.

4. In the lower part of the page, view the IP addresses in access between VPCs, and view the access source, access destination, and access count of IP addresses in the VPCs. Enter an access source, access destination, or destination port in the search boxes to start an exact search. For more information, please see Incoming access statistics.



More information

For questions about Traffic Monitoring, please see Bandwidth.

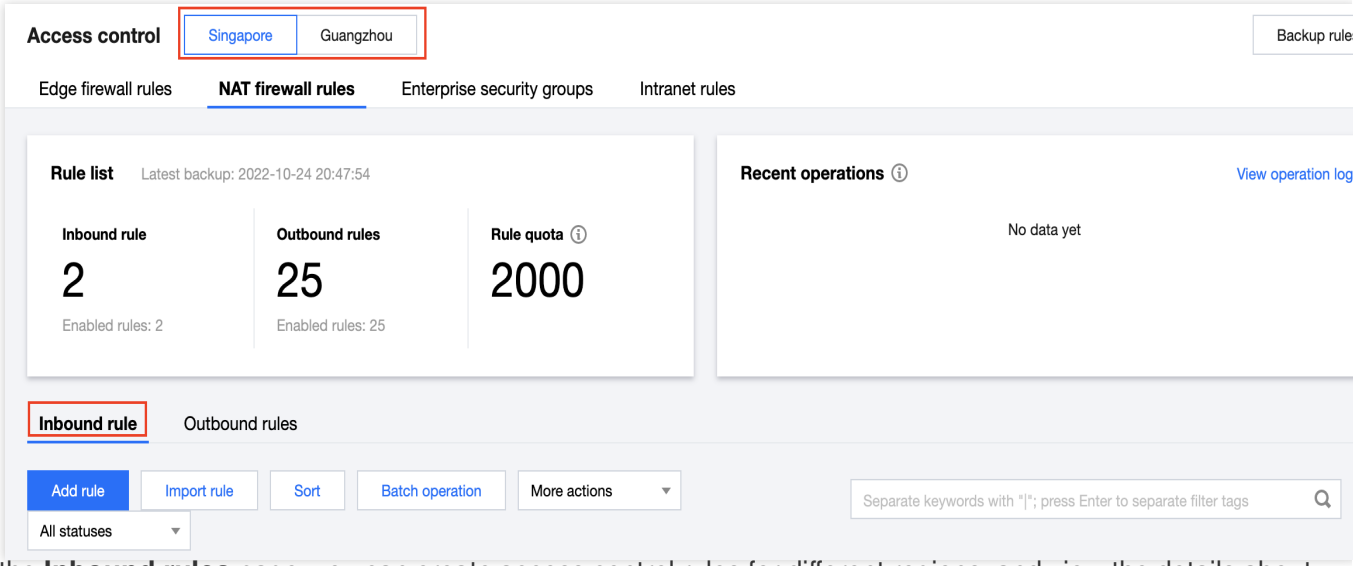
Access Control
NAT Firewall Rules

Last updated：2024-01-24 16:06:49

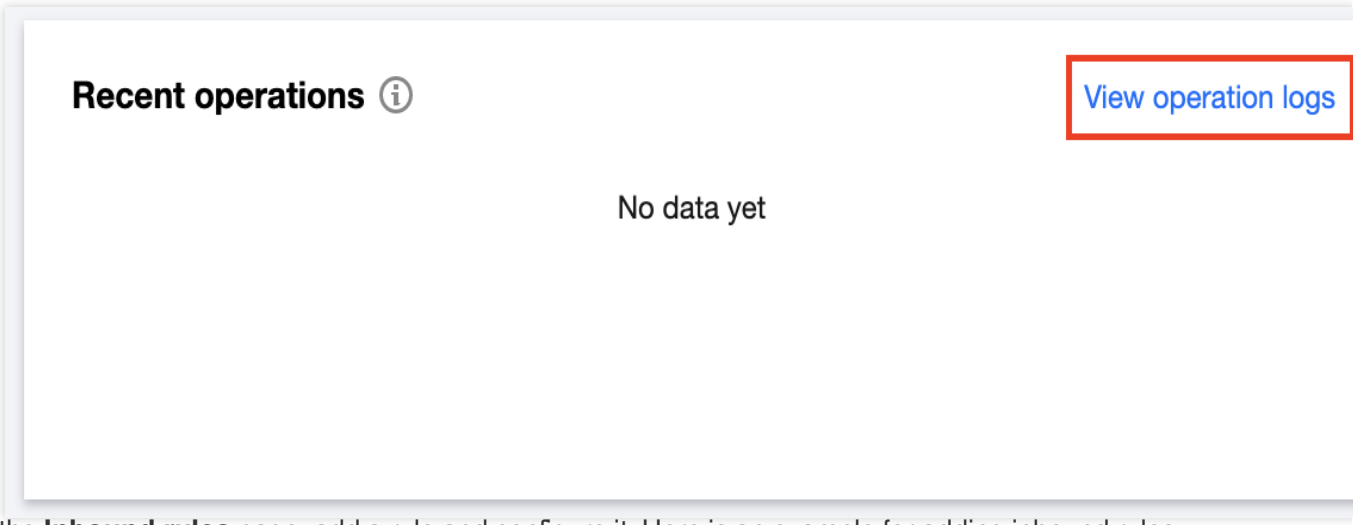
Access control rules can filter specific domain names or filter traffic by geographic location. NAT firewall has two access control rule lists, namely inbound rules and outbound rules. **Inbound rules** apply to the incoming north-south traffic over the edge firewall, while **outbound rules** apply to the outgoing north-south traffic over the edge firewall. This topic describes operations related to inbound rules, and those for outbound rules are similar.

Operation guide

1. Log in to the Cloud Firewall console, select **Access Control** in the left navigation pane, and then select **NAT firewall rules**.
2. On the "NAT firewall rules" page, select a region, and then click **Inbound rules**.

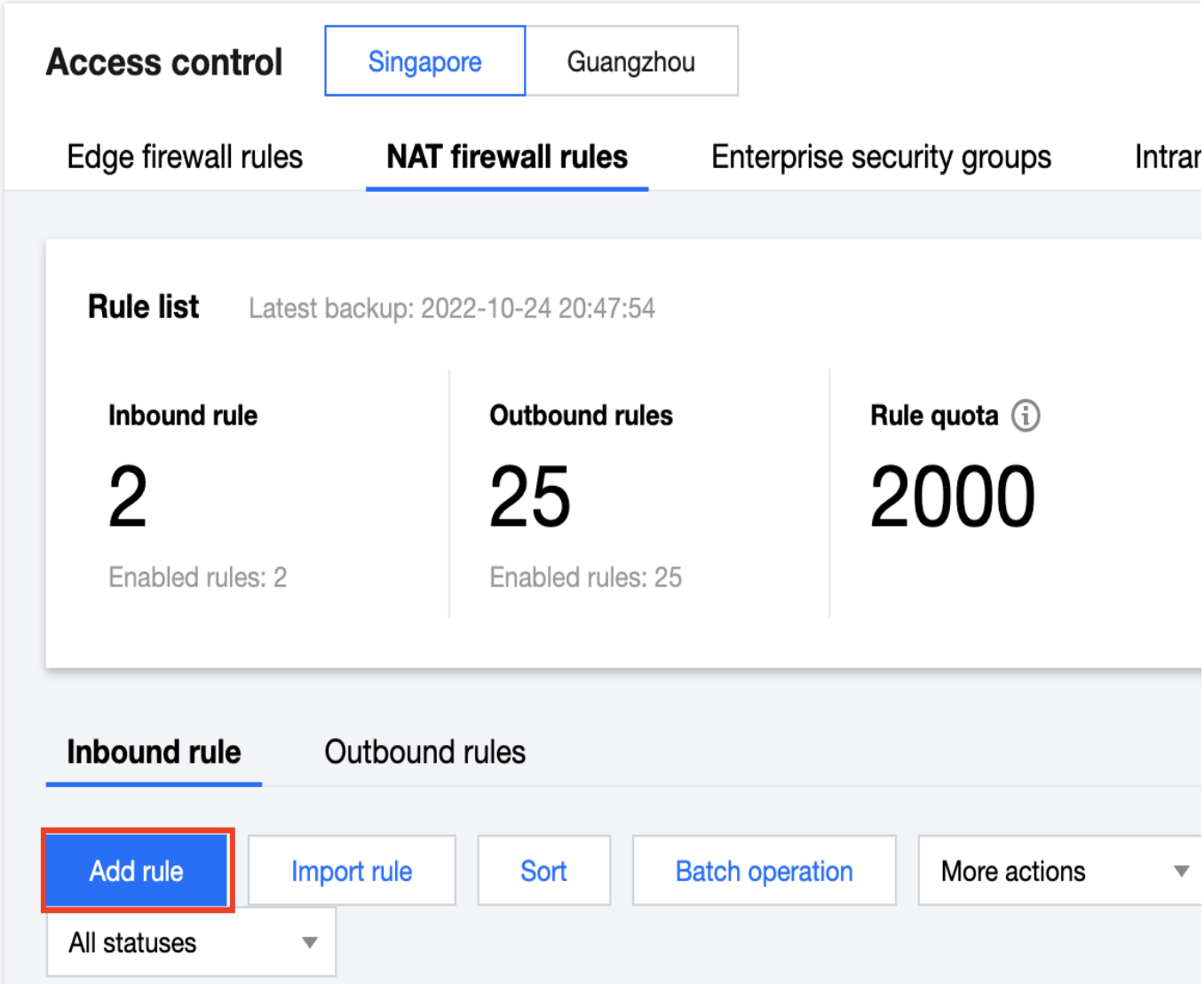


3. On the **Inbound rules** page, you can create access control rules for different regions, and view the details about rule lists (the used quota of inbound or outbound rules and the total quota of rule lists), recent operations, and access control rules. "Recent operations" show your recent operations on the rule lists:
Click **Details** to view details of a specific operation.
Click **View operation logs** to view detailed operation records.



4. On the **Inbound rules** page, add a rule and configure it. Here is an example for adding inbound rules.

i. Click **Add rule** on the **Inbound rules** page.



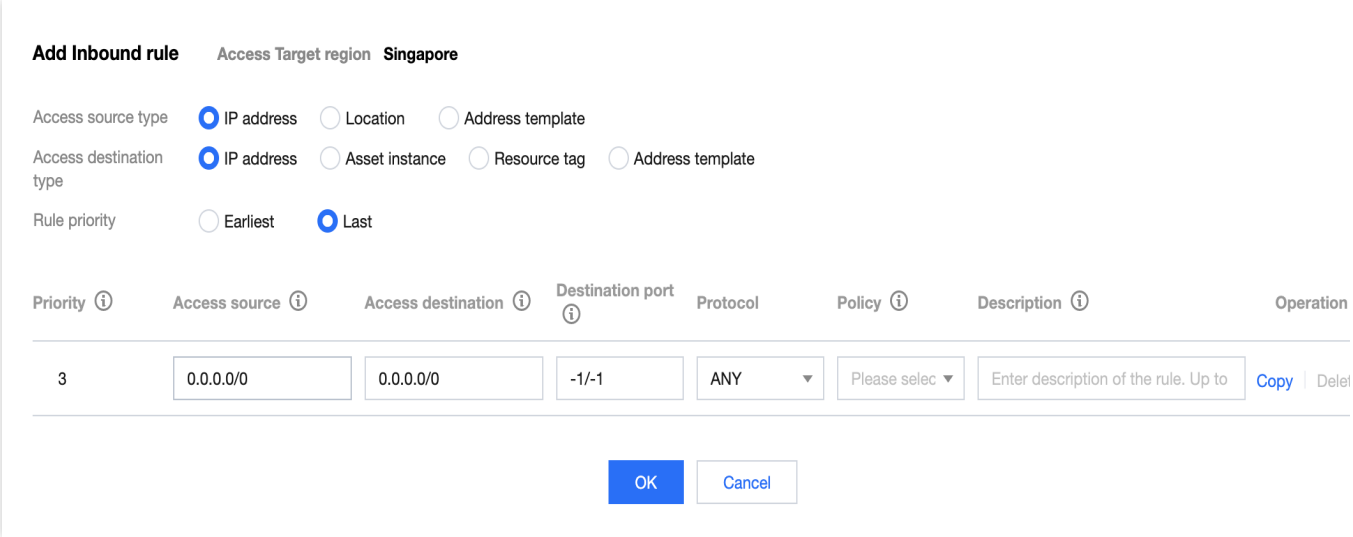
ii. Configure the inbound rule in the **Add inbound rule** window displayed. The "Access source type" can be an IP address, geographic location, cloud vendor, or address template. The "Access destination type" can be an IP

address, asset instance, resource tag, address template, or asset group. Select priority for rules based on their importance. After selecting the access source and destination, enter the destination port, select the protocol and the policy to implement, enter rule descriptions, and then click **OK** to complete the configuration.

Note

Access destination type region: The region where the cloud instance is located.

Access source type: The type of an external source when an inbound rule is added.



Field description:

Priority: The priority of the access control rule. The priorities of outbound and inbound rules are independent of each other. The rule with the highest priority is evaluated first. If a given rule is matched, rules with lower priorities will not be evaluated. When you modify the priority of a given rule, the priorities of the original rule with that priority and all the subsequent rules will increase by 1. When you delete a given rule, the priorities of all the subsequent rules will decrease by 1.

Access source: The access source of an inbound rule can be any public IP. It supports an IP, CIDR block, and location.

Access destination: The access destination of an inbound rule can be any private network asset in the current region. It supports an IP address, asset instance, resource tag, address template, and asset group. The supported access source and destination types of an outbound rule are the opposite.

Destination port: TCP/UDP rules support single port numbers (e.g., "80"), port ranges (e.g., "80/80", "-1/-1", "0/65535"), and discrete port numbers separated with commas (e.g., "80,443,3380/3389"). For ICMP rules, port configuration is not required.

Protocol: For the current CFW edition, supported inbound protocols include TCP and UDP, and supported outbound protocols include TCP, UDP, ICMP, HTTP, HTTPS, SMTP, SMTPS, DNS, and FTP.

Policy description:

Allow: Allow the matched traffic and record the hit count and traffic logs, but not access control logs.

Observe: Allow the matched traffic and record the hit count, access control logs, and traffic logs.

Block: Block the matched traffic and record the hit count and access control logs, but not traffic logs.

Description: The rule description with up to 50 characters. You can use a pair of # to insert special settings. Your current CFW edition supports #long connection#.

NAT firewall wildcard rules:

CFW provides different wildcard rules for IP address, port, and domain name.

Input field	Input example	Description
Access source/Access destination	0.0.0.0/0	Indicates all IP addresses.
Domain name	*	Indicates all domain names.
Domain name	*.aa.com	Indicates second-level domain names starting with an asterisk (*): aa.com.
Destination port	-1/-1	Indicates all ports.
Destination port	0/65535	Indicates all ports.
Destination port	80,443,3389	Indicates ports 80, 443, and 3389.
Destination port	80/443	Indicates all ports between port 80 and port 443.
Destination port	80/443,3389	Indicates all ports between port 80 and port 443, as well as port 3389.

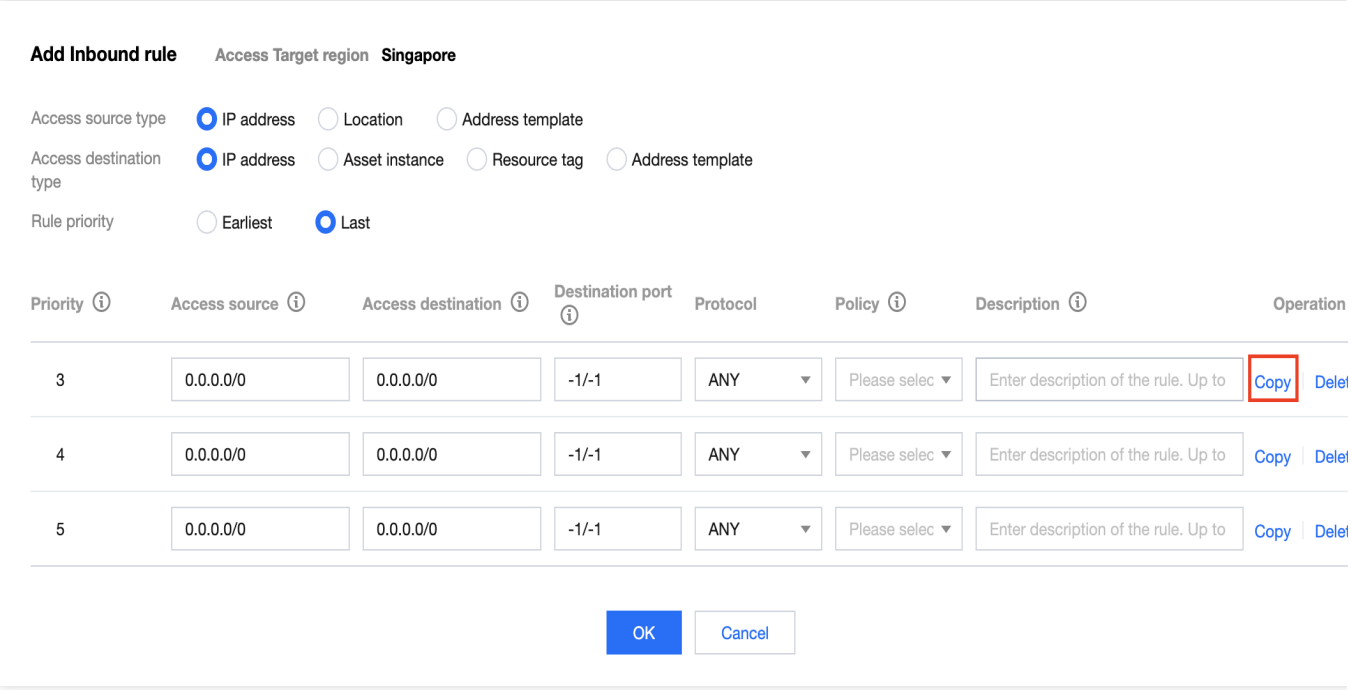
5. Click **Copy** in the action column on the right to add multiple rules.

Note

In the **Add inbound rule** window, one rule uses one line, and a new rule is added to the end of the list by default. The last rule added has the largest priority number or the lowest priority.

Scenario 1: You have configured the rule list, and need to add rules in batch.

5.1 Click **Copy** in the action column on the right to add a rule to the next line of the current rule. A maximum of 10 rules can be added at a time.



5.2 Complete all fields in the list.

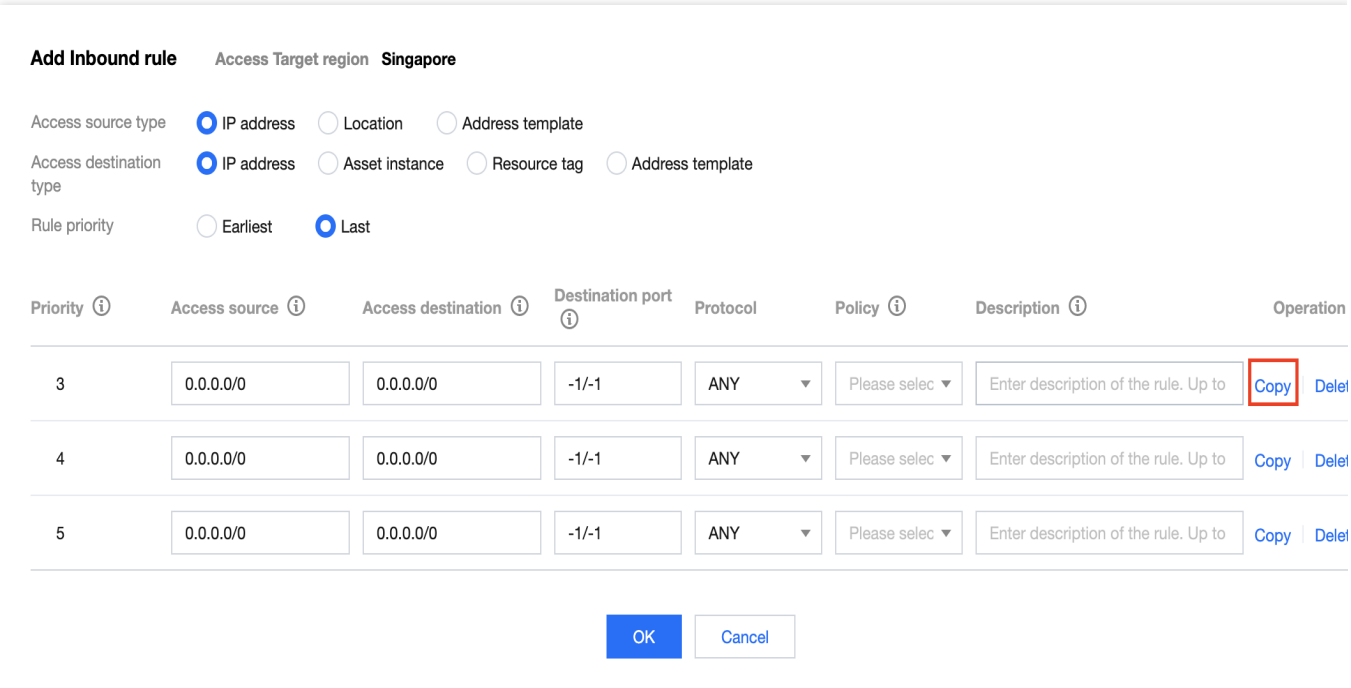
5.3 Check whether the priority of the rules added in batch meets your expectations.

5.4 Click **OK** to submit the rules configured.

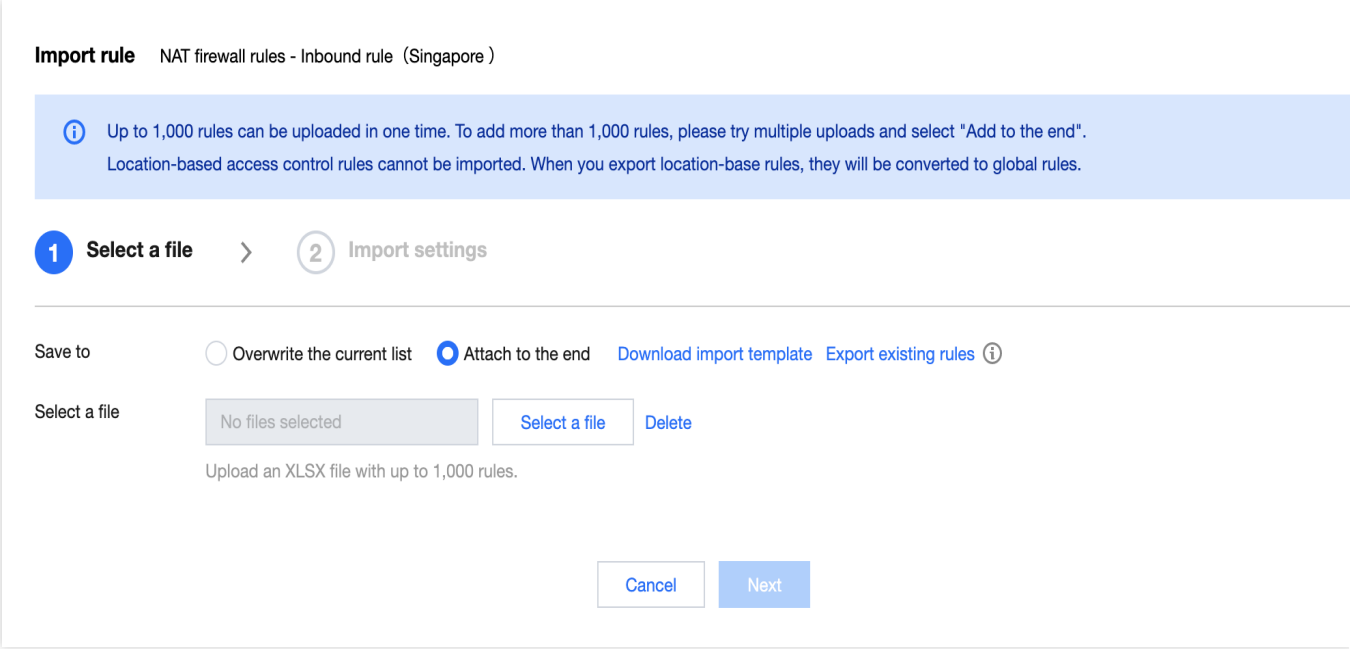
Scenario 2: You need to configure multiple rules for an IP address.

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

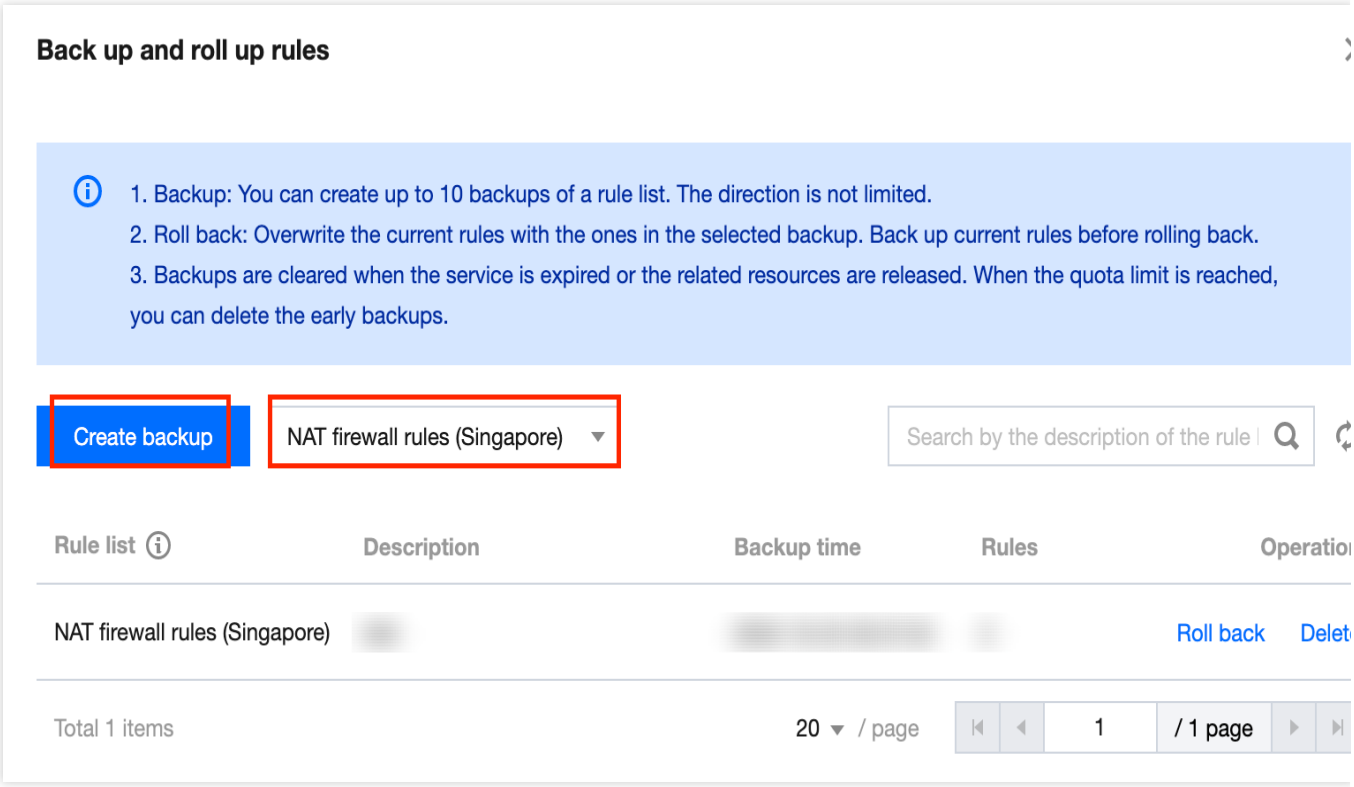
5.2 Click **Copy** in the action column on the right to add a rule to the next line of the current rule, with the fields automatically populated with the same values as from the edited rule. A maximum of 10 rules can be added at a time.



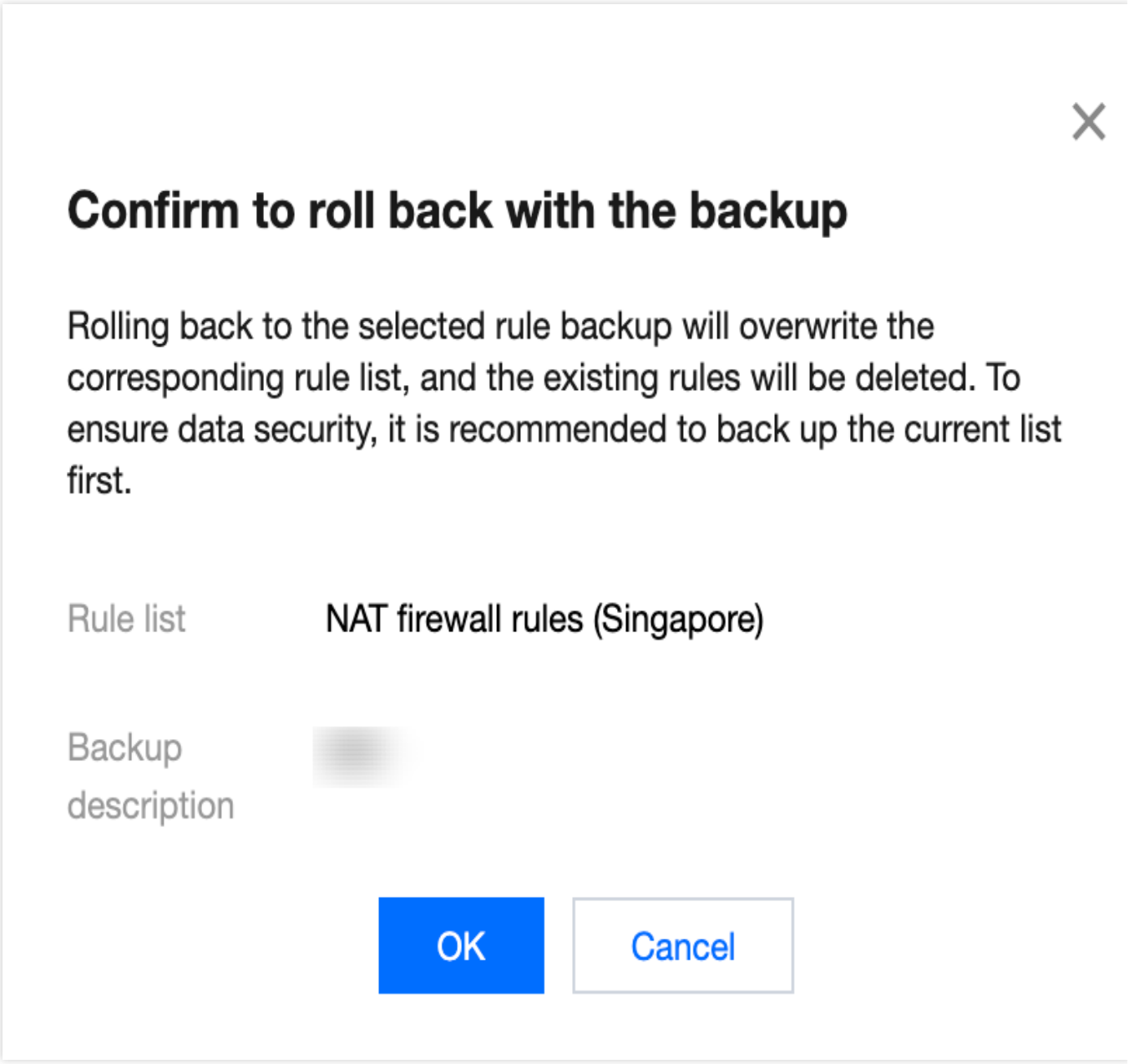
5.3 Complete other fields in the list.
5.4 Check whether the priority of the rules added in batch meets your expectations.
5.5 Click **OK** to submit the rules configured.
6. Import rules: Click **Import rule** to import rules from a local file. You can specify the import location, download the import template, or export existing rules.



7. Back up and roll back rules: Click **Backup rules** in the upper right corner to back up existing NAT firewall rules. When the rules are greatly changed, you can click **Roll back** to the right of the backup file to recover the rules.
8. Click **Backup rules** in the upper right corner to enter the **Back up and roll up rules** page. Click **Create backup**, select **NAT firewall rules** from the drop-down list and enter a description, and then click **OK** to complete the backup.



9. To roll back rules, click **Roll back** on the right side of the backup file, and you can recover the rules after confirmation.



More information

For the information about how to control the inbound and outbound traffic over the edge firewall on the Cloud Firewall console, please see Edge Firewall Rules.

For information about how to set inter-VPC firewall rules on the Cloud Firewall console, please see Inter-VPC Firewall Rules.

For the special scenarios of the Cloud Firewall access control feature, please see Special Scenarios.

For questions about NAT firewall rules, please see NAT Firewall.

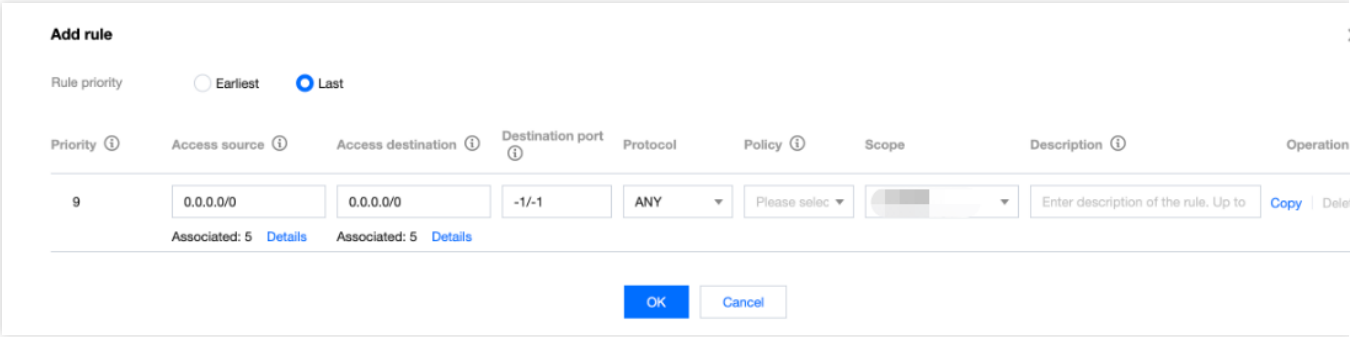
Inter-VPC Firewall Rules

Last updated：2024-01-24 16:06:49

Inter-VPC firewall rules provide multiple access control lists (ACLs), each of which is associated with a pair of connected VPCs and an inter-VPC firewall toggle. This topic describes how to set up inter-VPC firewall rules on the Cloud Firewall console.

Operation guide

1. Log in to the Cloud Firewall console, select **Access Control** in the left navigation pane, and then select **Inter-VPC firewall rules**.
2. In the upper left corner of the **Inter-VPC firewall rules** page, you can switch between different inter-VPC ACLs from the drop-down list of "Firewall toggle name".

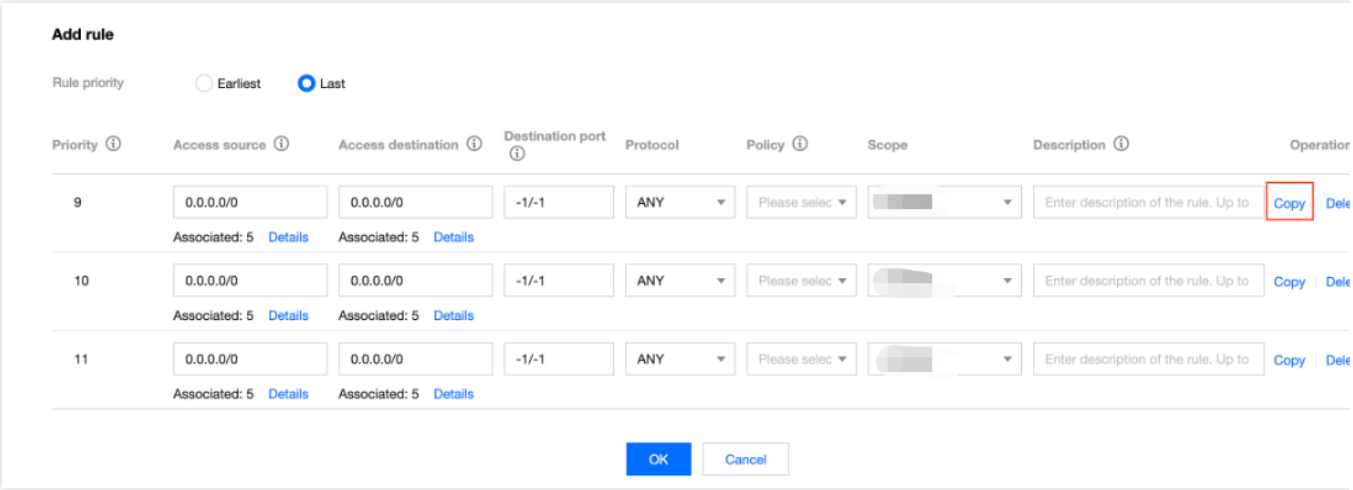


Note

Unlike the edge firewall and NAT firewall ACLs, inter-VPC ACLs have no direction limitations.

The local and peer VPCs are equivalent. When configuring rules, you can determine the VPC based on the CIDR block where the access source and destination are located to differentiate the direction.

3. On the **Inter-VPC firewall rules** page, click **Add rule**.
4. On the **Add rule** page, the information of local and peer VPCs and firewall toggle of the inter-VPC ACLs is already available. You only need to enter the access source IP, access destination IP, destination port, and other information to complete the configuration.



Field description:

Priority: The priority of the access control rule, which is independent of that of the rule list for the firewall toggles. The outbound and inbound rules are executed independently. The rule with the highest priority is evaluated first. If a given rule is matched, rules with lower priorities will not be evaluated. When you modify the priority of a given rule, the priorities of the original rule with that priority and all the subsequent rules will increase by 1. When you delete a given rule, the priorities of all the subsequent rules will decrease by 1.

Access source: It can be an IP in the CIDR block of the local/peer VPC or a subnet range of it. Note that it cannot be in the same VPC network range as the access destination. You can also enter 0.0.0.0/0 as a wildcard access source.

Access destination: It can be an IP in the CIDR block of the local/peer VPC or a subnet range of it. Note that it cannot be in the same VPC network range as the access source. You can also enter 0.0.0.0/0 as a wildcard access destination.

Destination port: Supports single port numbers (e.g., "80"), port ranges (e.g., "80/80", "-1/-1", "0/65535"), and discrete port numbers separated with commas (e.g., "80,443,3380/3389").

Protocol: The current CFW edition supports UDP, TCP, and ICMP.

Policy description:

Allow: Allow the matched traffic and record the hit count and traffic logs, but not access control logs.

Observe: Allow the matched traffic and record the hit count, access control logs, and traffic logs.

Block: Block the matched traffic and record the hit count and access control logs, but not traffic logs.

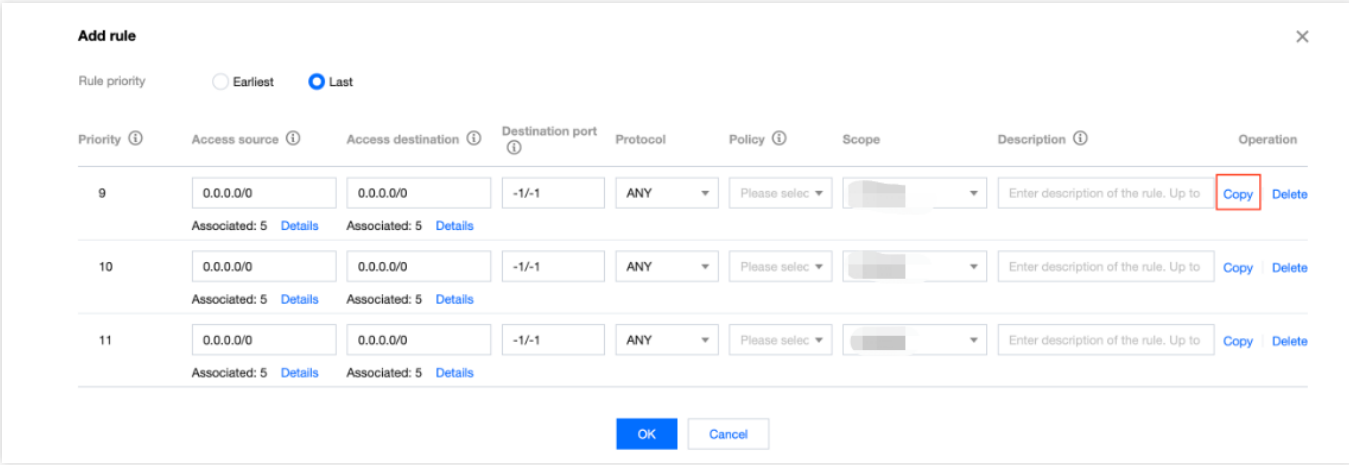
Description: The rule description with up to 50 characters. You can use a pair of # to insert special settings. Your current CFW edition supports #long connection#.

Inter-VPC wildcard rules: For more information about the IP address ranges that support wildcard, please see the wildcard rules in Edge Firewall Rules.

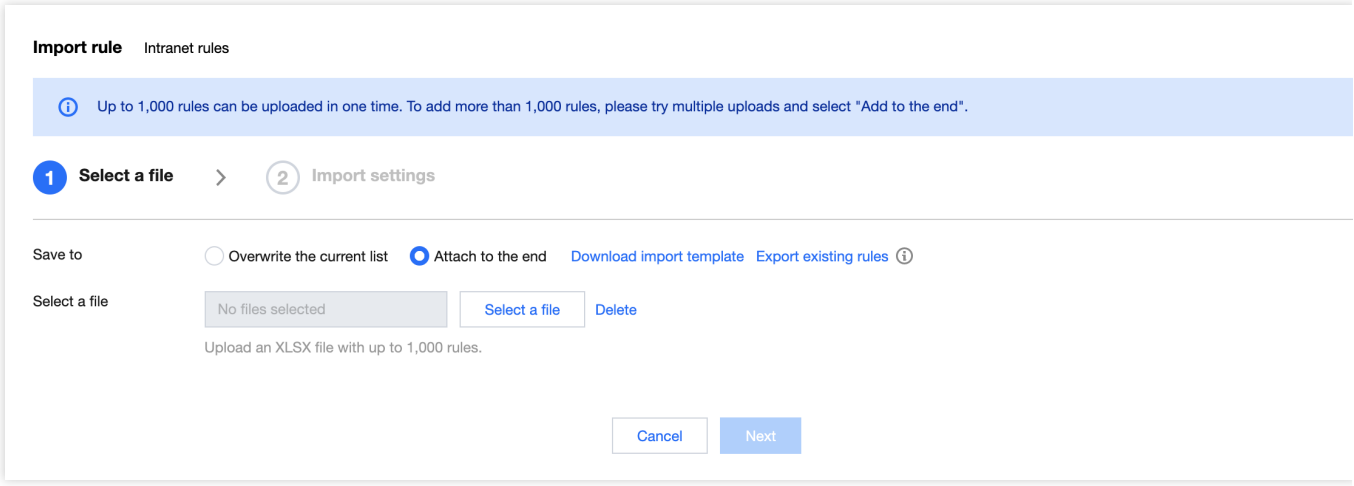
Caution

The CIDR blocks of the local and peer VPCs cannot be the same or overlap. Otherwise, the firewall cannot be enabled.

In the inter-VPC access control rules, the access source and access destination can only be an IP in the CIDR block of the local/peer VPC or a sub-network range of it. As the CIDR blocks of the local and peer VPCs cannot be the same, the direction of the traffic controlled by a rule can be distinguished by the "Access source" or "Access destination".
The rule will not take effect if you enter an address other than those in the CIDR block of the local or peer VPC.
If you enter 0.0.0.0/0 for "Access source" and "Access destination", it indicates all the addresses of the VPC.
5. Click **Copy** in the action column on the right to add multiple rules.
Note
In the **Add inbound rule** window, one rule uses one line, and a new rule is added to the end of the list by default. The last rule added has the largest priority number or the lowest priority.
Scenario 1: You have configured the rule list, and need to add rules in batch.
5.1 Click **Copy** in the action column on the right to add a rule to the next line of the current rule. A maximum of 10 rules can be added at a time.
5.2 Complete all fields in the list.
5.3 Check whether the priority of the rules added in batch meets your expectations.
5.4 Click **OK** to submit the rules configured.
Scenario 2: You need to configure multiple rules for an IP address.
5.1 Edit a rule to fill in the fields that need to be input repeatedly.
5.2 Click **Copy** in the action column on the right to add a rule to the next line of the current rule, with the fields automatically populated with the same values as from the edited rule. A maximum of 10 rules can be added at a time.

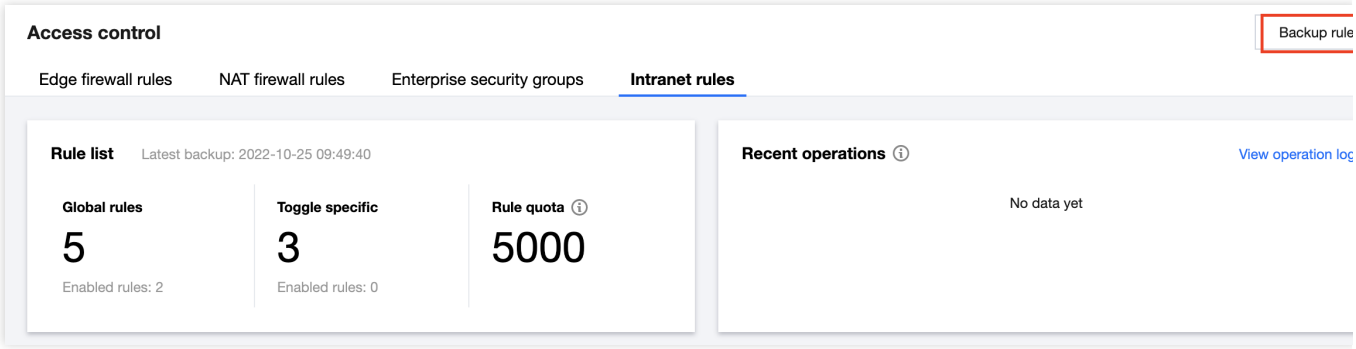


5.3 Complete other fields in the list.
5.4 Check whether the priority of the rules added in batch meets your expectations.
5.5 Click **OK** to submit the rules configured.
6. After the rules are added, you can view them in the rule list.
7. Import rules: Click **Import rule** to import rules from a local file. You can specify the import location, download the import template, or export existing rules.

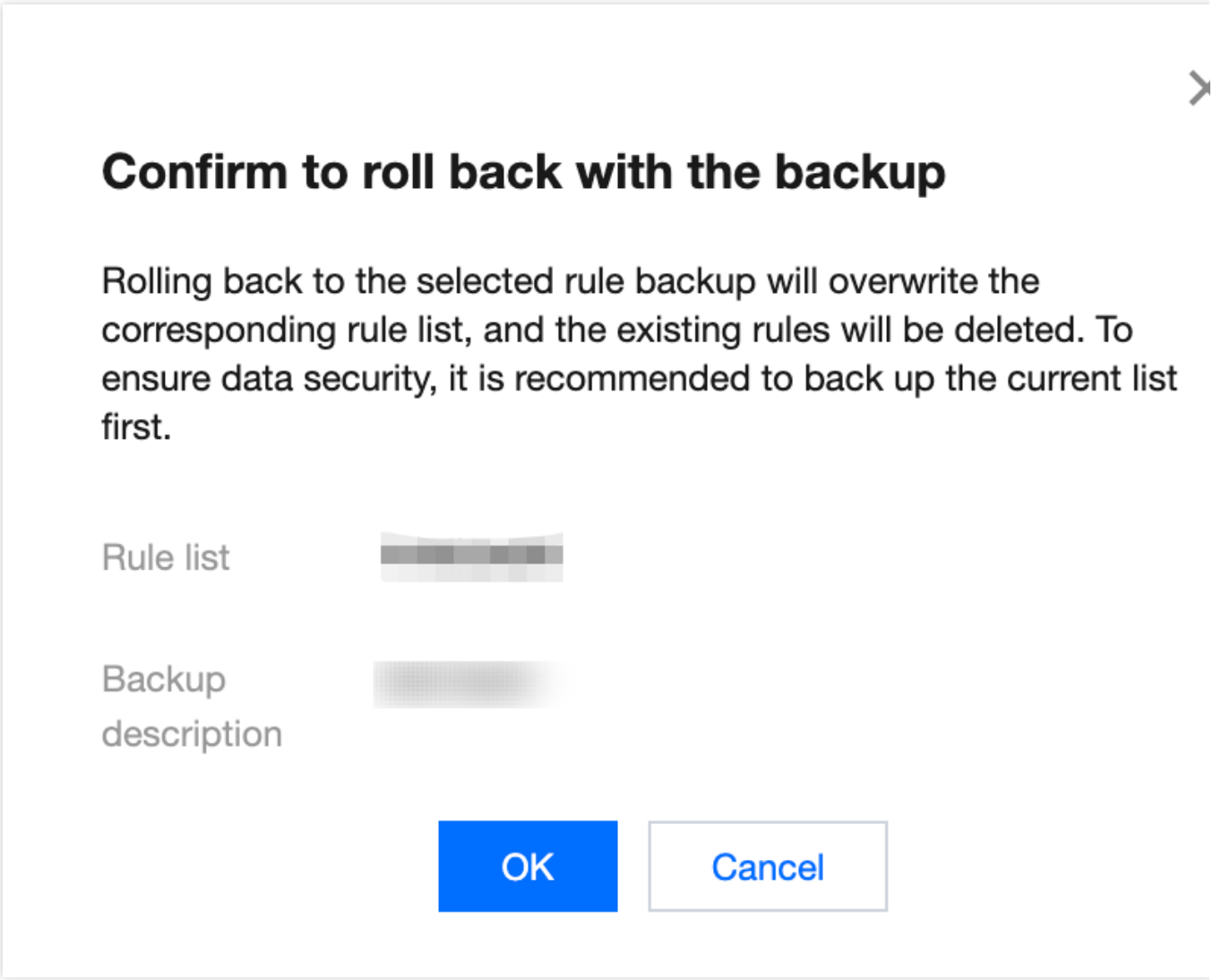


8. Back up and roll back rules: Click **Backup rules** in the upper right corner to back up existing NAT firewall rules. When the rules are greatly changed, you can click **Roll back** to the right of the backup file to recover the rules.

1. Click **Backup rules** in the upper right corner to enter the **Back up and roll up rules** page. Click **Create backup**, select **Inter-VPC firewall rule group** from the drop-down list and enter a description, and then click **OK** to complete the backup.



2. To roll back rules, click **Roll back** on the right side of the backup file, and you can recover the rules after confirmation.



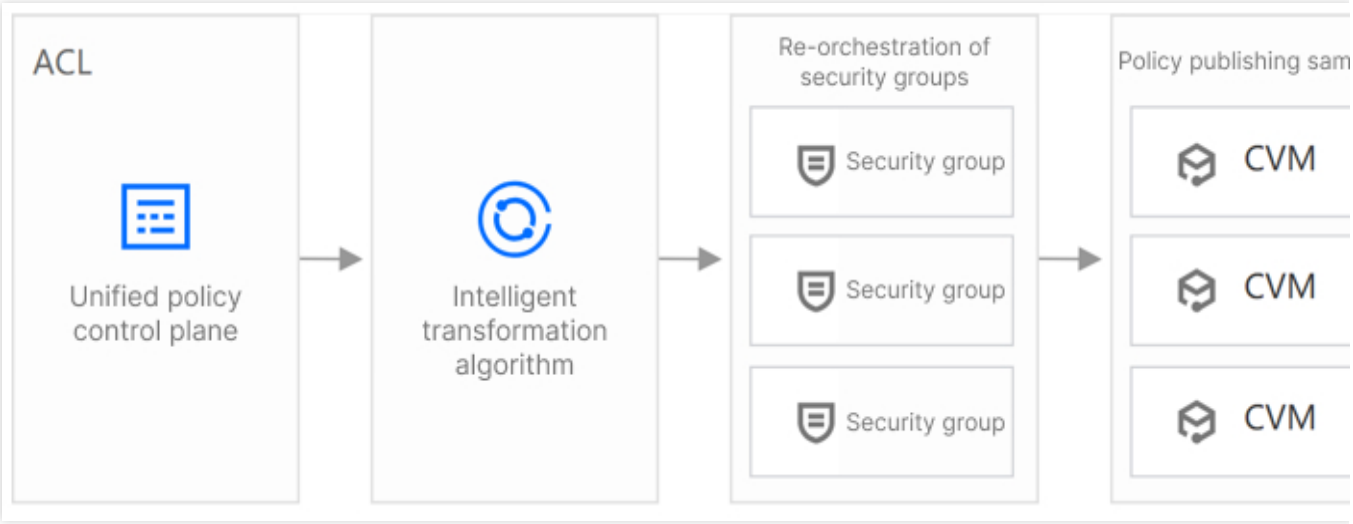
More information

For the information about how to control the inbound and outbound traffic over the edge firewall on the Cloud Firewall console, please see Edge Firewall Rules.
For the information about how to control the inbound and outbound traffic over the NAT firewall on the Cloud Firewall console, please see NAT Firewall Rules.
For the special scenarios of the Cloud Firewall access control feature, please see Special Scenarios.
For questions about inter-VPC firewall rules, please see Inter-VPC Firewall.

Enterprise Security Group Feature Overview

Last updated：2024-01-24 16:06:49

Enterprise security group is a new security group control plane that replaces the security group administration interface in the CVM console. The configuration logic of security groups has been redesigned and a centralized access control administration page has been maintained, which improves the user experience of security groups. CFW provides five-tuple-based rule configuration and automatically publishes security group rules through intelligent transformation algorithms, which simplifies the configuration of security groups.



Features

It simplifies the configuration of security groups based on the 5-tuple rules.
It supports inter-VPC, inter-subnet, and direct connect access control.
It provides access control logs of security groups for easy backtracking of blocking and routine troubleshooting.
It requires no change in the network architecture, and has no impact on network stability and network performance.

Restrictions

Enterprise security group is developed based on the underlying architecture of the CVM security group, and thus is restricted by the underlying functional implementation and resource quotas of the security group.

Rules

Rule composition

Access source and access destination: Depending on the inbound or outbound direction, they can be IPs, CIDR blocks, instances, subnets, or private networks.
Destination port: The destination port number. Not required when the protocol type is ICMP or ANY.
Protocol type: TCP, UDP, and ICMP are supported. ANY indicates all supported protocols.
Policy: the operation performed after the rule is hit.
Allow: Allow the matched traffic but do not record access control logs.
Block: Block the matched traffic and record access control logs.

Rule priorities

The security group rules are prioritized in a way that the rule at the top of the list has the highest priority while the rule at the bottom has the lowest priority.
The rule with the highest priority is evaluated first. If a given rule is matched, rules with lower priorities will not be evaluated.
The inbound and outbound rules are in different lists and independent of each other.

Auto two-way publishing

Enterprise security group provides the "Auto two-way publishing" feature to improve the configuration efficiency of security groups. This eliminates the need to configure two identical rules in both directions to block or allow traffic between private networks, thus reducing the workload of rule configuration.
When the access source address is an instance, subnet, or private network address, an identical outbound rule (with the highest priority) can be automatically configured using "Auto two-way publishing".
Note：
It only applies to communication between private networks.
For example, there are two instances, instance 1 and instance 2, and their IP address is IP1 and IP2, respectively.
If you have configured a "deny all" policy for the security group for instances 1 and 2, respectively, and want to allow the access from instance 1 to instance 2, you need to manually configure two security group rules:
Instance 1: Allow IP2 in the outbound direction.
Instance 2: Allow IP1 in the inbound direction.

Logs

Security group blocking logs

The security group blocking logs record the implementation of all blocking policies for enterprise security groups. This is only available to specified models.

Enterprise security group operation logs

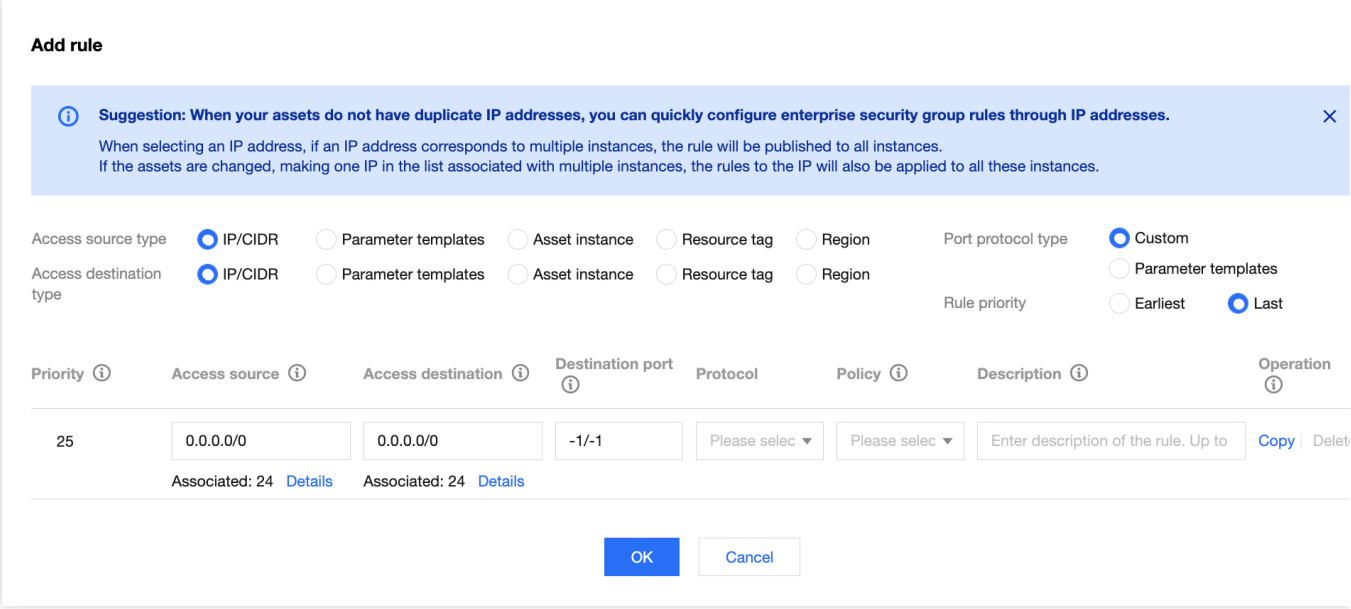
The enterprise security group operation logs record the operations performed by an account on the "Enterprise security groups" page.

Configurations

Last updated：2024-01-24 16:06:49

Adding rules

1. Log in to the Cloud Firewall console, select **Access Control** in the left navigation pane, and then select **Enterprise security groups**.
2. On the **Enterprise security groups** page, click **Add rule**.
3. In the **Add rule** window displayed, configure the parameters and click **OK**.



Parameters

Priority: The execution order of access control rules. The rule with the highest priority is evaluated first. If a given rule is matched, rules with lower priorities will not be evaluated. When you modify the priority of a given rule, the priorities of the original rule with that priority and all the subsequent rules will increase by 1. When you delete a given rule, the priorities of all the subsequent rules will decrease by 1.

Access source: It can be an IP/CIDR, parameter template, asset instance, asset group, resource tag, region, and other types.

Access destination: It can be an IP/CIDR, parameter template, asset instance, asset group, resource tag, region, and other types.

Note

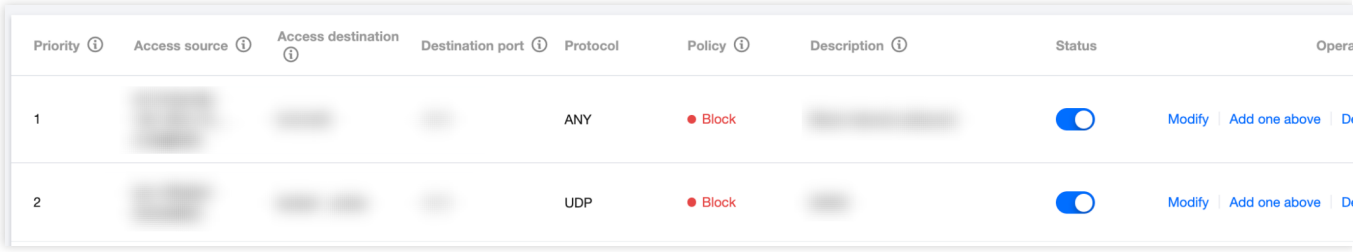
You can select any type for the access source and access destination as listed above. But you cannot select region for the access source and access destination at the same time.

Destination port: Supports single port numbers (e.g., "80"), port ranges (e.g., "80/80", "-1/-1", "1/65535"), and discrete port numbers separated with commas (15 at most).
Protocol: The current CFW edition supports UDP, TCP, and ICMP.
Policy:
Allow: Allow the matched traffic but do not record the hit logs of enterprise security groups.
Block: Block the matched traffic and record the hit logs of enterprise security groups.
Description**: The rule description with up to 50 characters. You can use a pair of # to insert special settings. Your current CFW edition supports #Only publish to source# and #Only publish to destination#.

Note

When the access destination address is an instance, subnet, or private network address, an identical inbound rule can be automatically assigned using "Auto two-way publishing". To cancel auto two-way publishing, you can add keywords to the description: #Only publish to source# (the security group rules are only published to the source); #Only publish to destination# (the security group rules are only published to the destination).

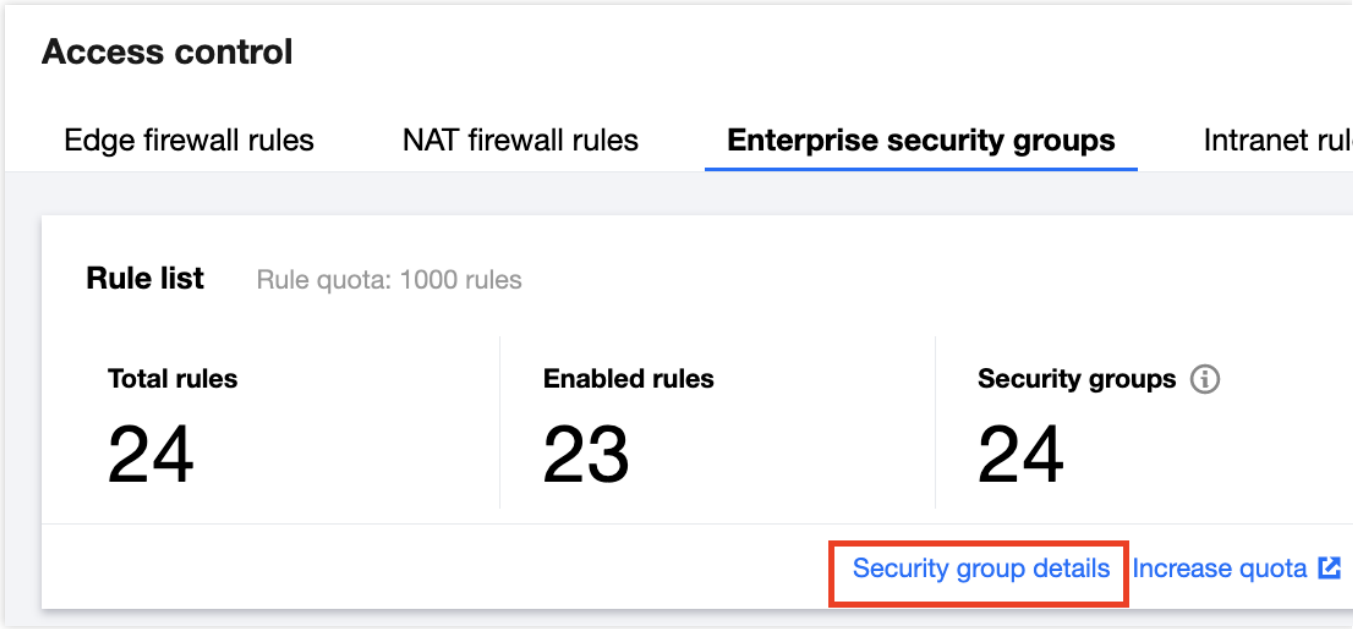
4. Once added, the rules will be displayed in the rule list.



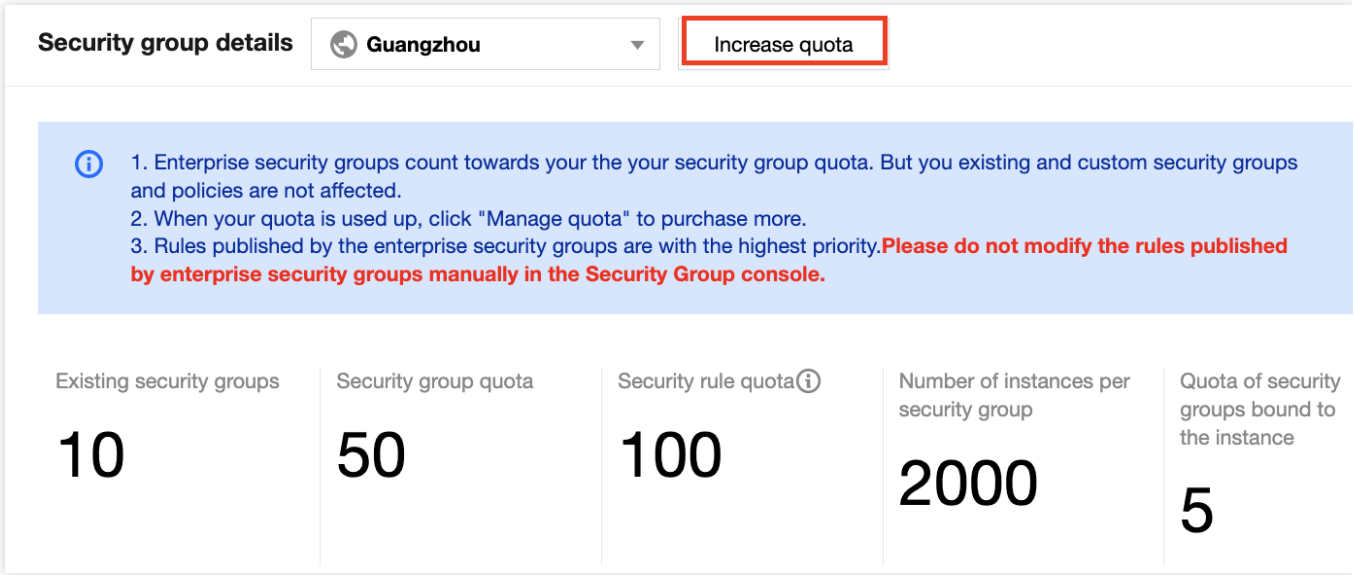
5. Once the rules are added and published successfully, you can view security groups on the **CFW security group details** page or the Security group page on the VPC console, which are associated with instances automatically.

Viewing security group details

1. Log in to the Cloud Firewall console, select **Access Control** in the left navigation pane, and then select **Enterprise security groups**.
2. On the **Enterprise security group** page, click **Security group details**.

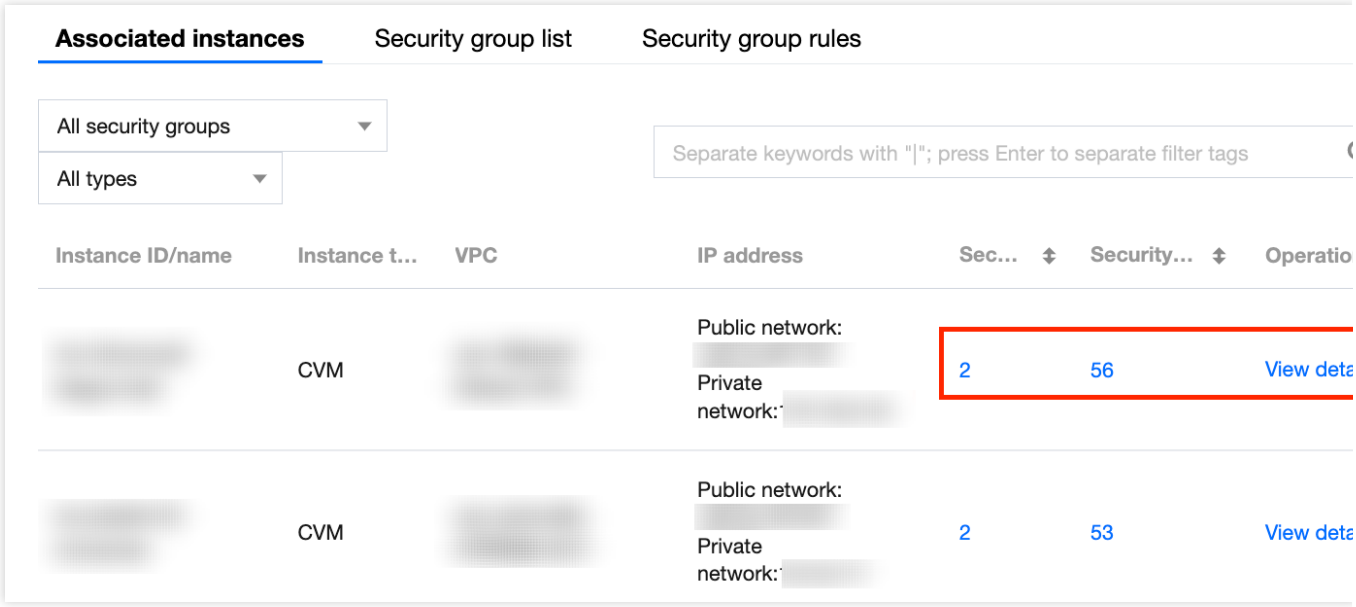


3. On the **Security group details** page, you can view the regions of instances and quota information. The quota can be increased as needed.

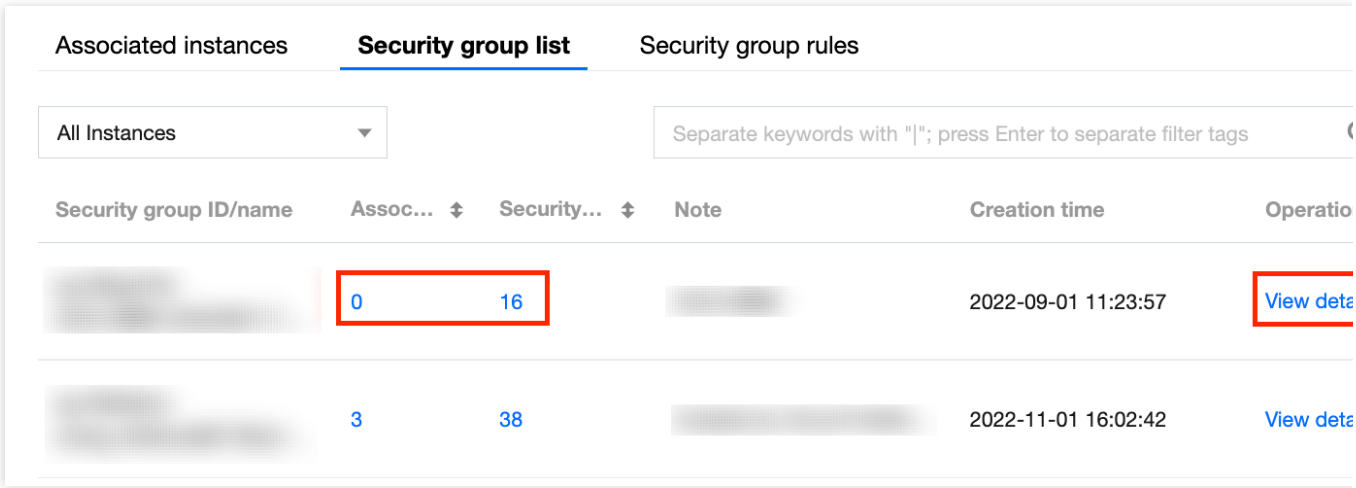


4. At the bottom of the **Security group details** page, you can view associated instances, security group lists, and security group rules.

Associated instances: Display information of all instances in a region, such as instance name, instance type, network, and IP address. Click the number in the "Security group" or "Security group rule" column to go to the security group list or rule details page of an instance. Click **View details** to go to the instance details page.

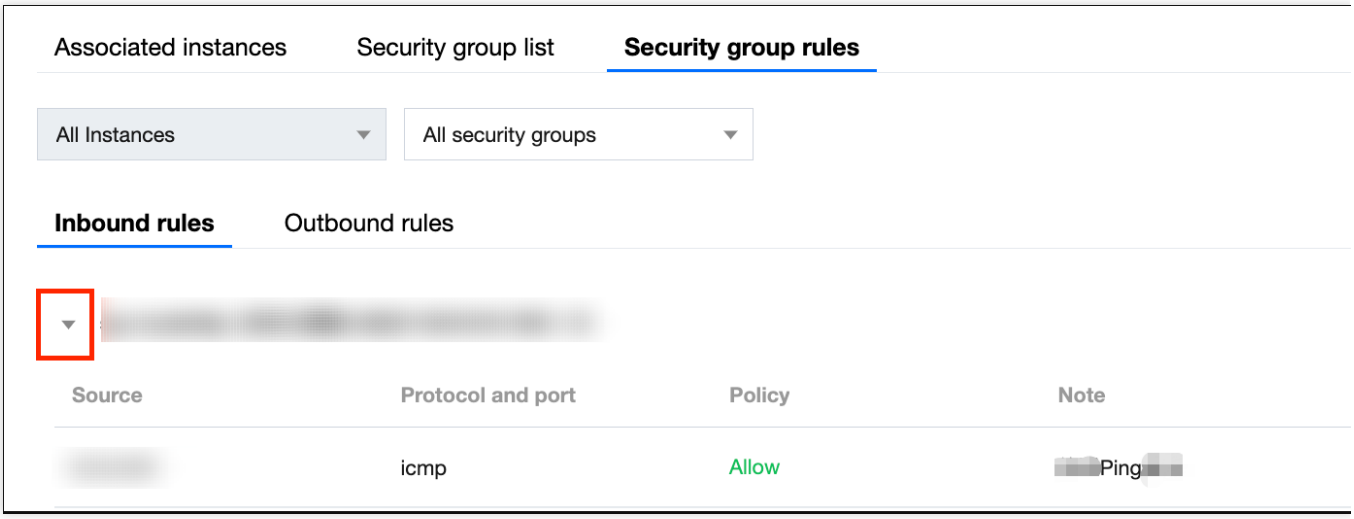


Security group list: It displays all the security group lists for the current region, the instances associated with each security group, the number of security group rules, the creation time, and other information. Click the number in the "Associated instance" or "Security group rule" column to go to the security group list or rule details page of an instance. Click **View details** to go to the security group details page in the VPC console.

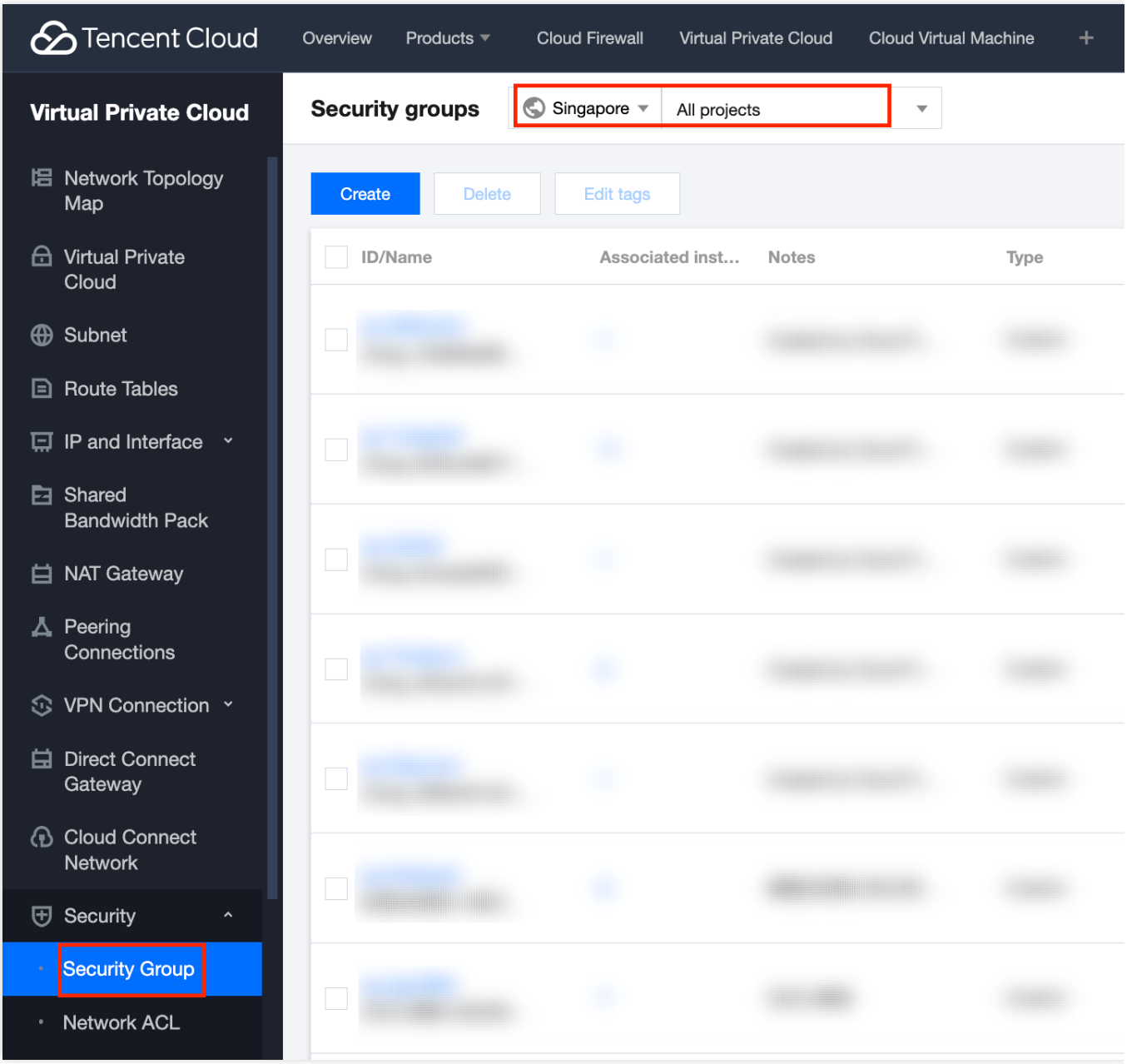


Security group rules: Display the inbound and outbound rules of all security groups in the current region. Click

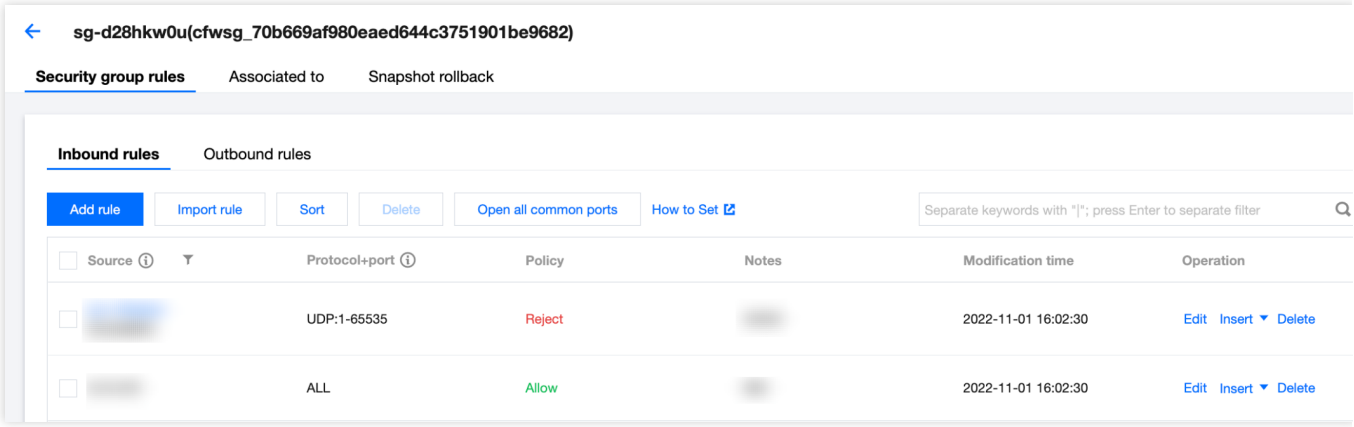
to view the rule details, or check whether the enterprise security group rules are published successfully.



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



6. Click the ID/name of a security group to view its inbound rules, outbound rules, and associated instances.

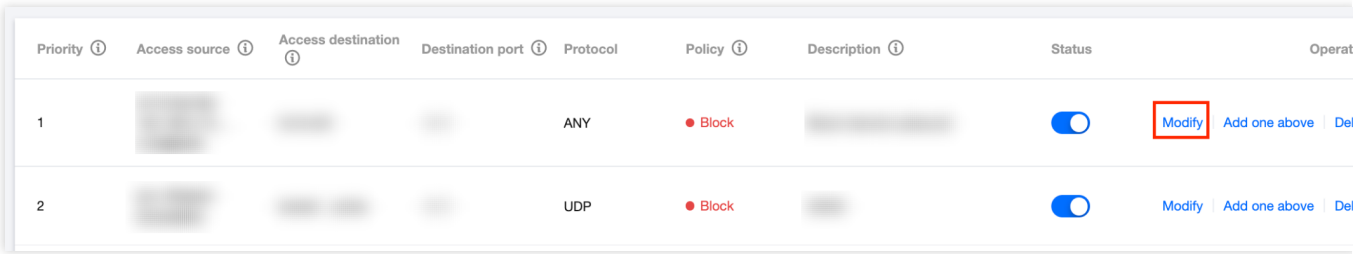


Managing rules

After setting enterprise security group rules, you can modify, insert, delete, or sort the rules on the **Enterprise security group** page.

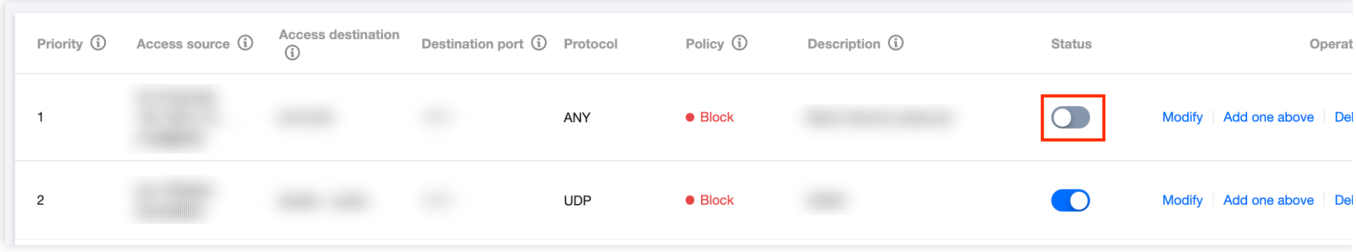
Editing rules

On the Enterprise security groups page, select a rule, click **Modify** to modify the parameters, and then click **OK**.



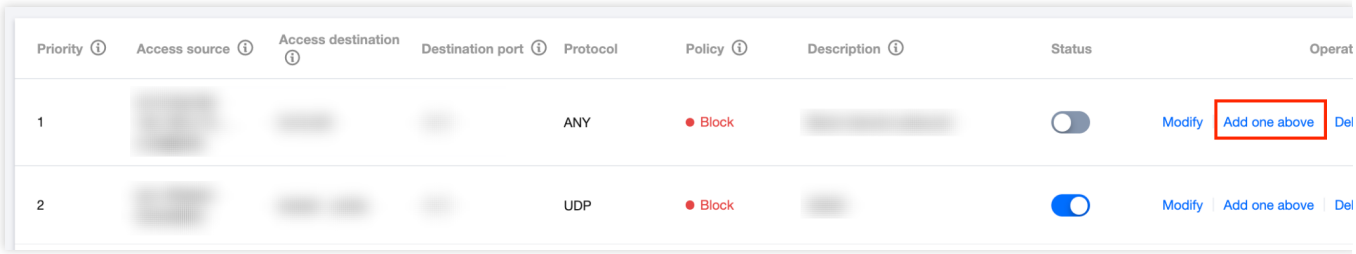
Disabling rules

On the Enterprise security groups page, you can disable or enable rules. Once you disable a rule, it will no longer be matched.



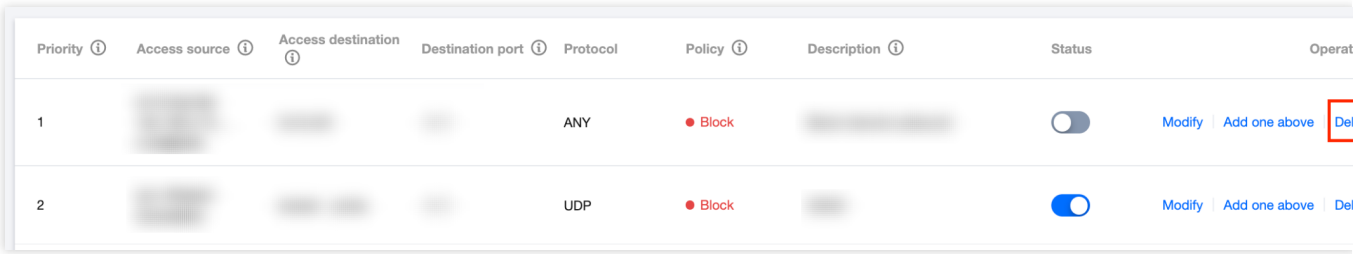
Inserting rules

On the Enterprise security groups page, select a rule, click **Insert**, enter parameters, and click **OK** to add a rule above the current rule. The new rule has higher priority than the current rule.



Deleting rules

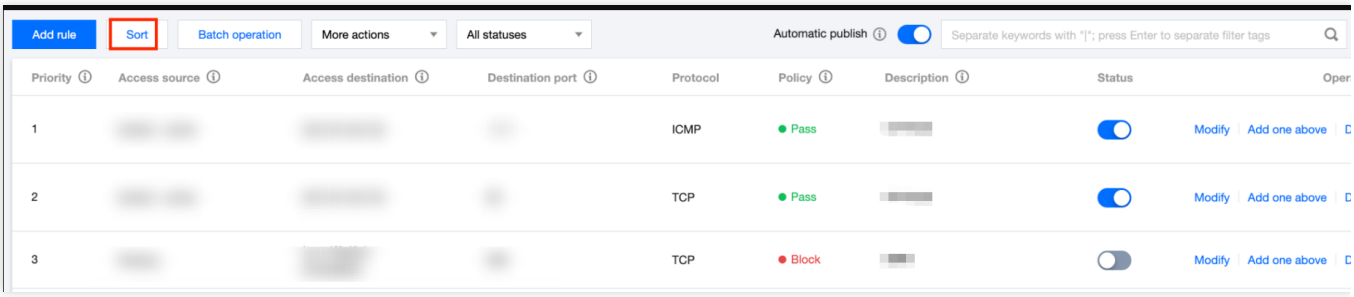
On the Enterprise security groups page, select a rule and click **Delete** to delete it upon second confirmation.



Sort

The priority of a rule depends on its order in the list.

1. On the Enterprise security groups page, click **Sort**, select a rule, and click and hold the rule to drag it to the desired position.

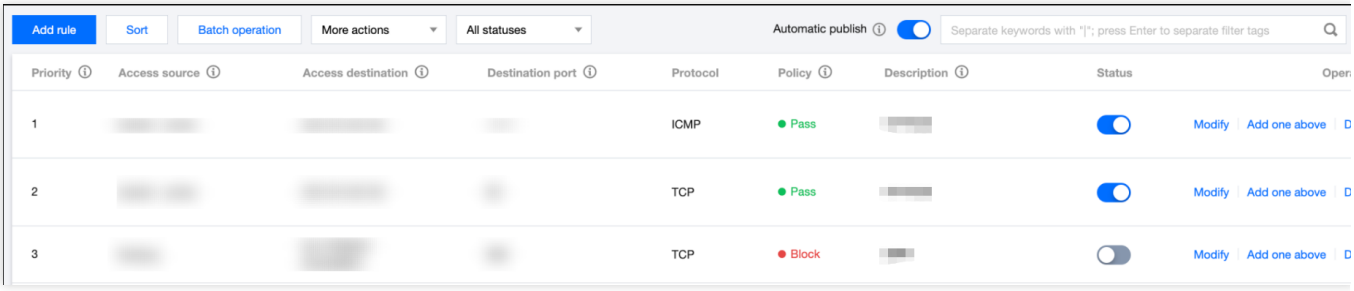


2. Click **Save**, and the new priority of rules will take effect and be automatically published to the instance.

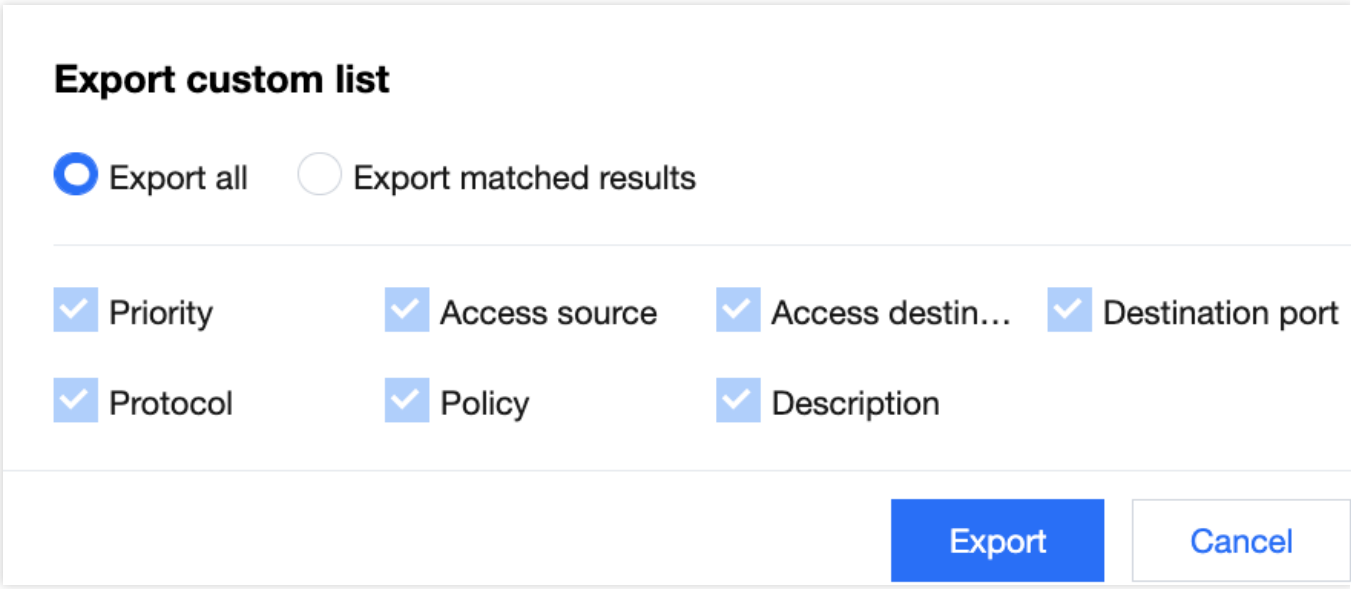
Exporting rules

1. On the Enterprise security groups page, click

in the upper right corner of the rule list, and the **Export custom list** window will pop up.



2. In the pop-up window, select "Export all" or "Export matched results", and then click **Export**.



Special Scenarios

Last updated：2024-01-24 16:06:49

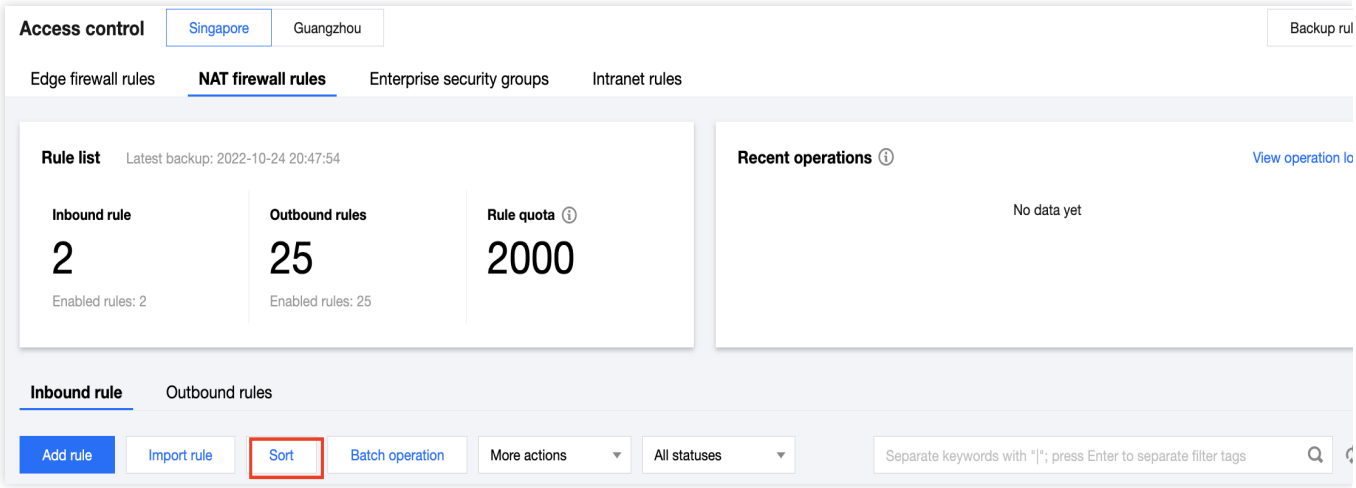
This topic describes special scenarios of the Cloud Firewall access control feature.

Managing the execution priority of the rule lists

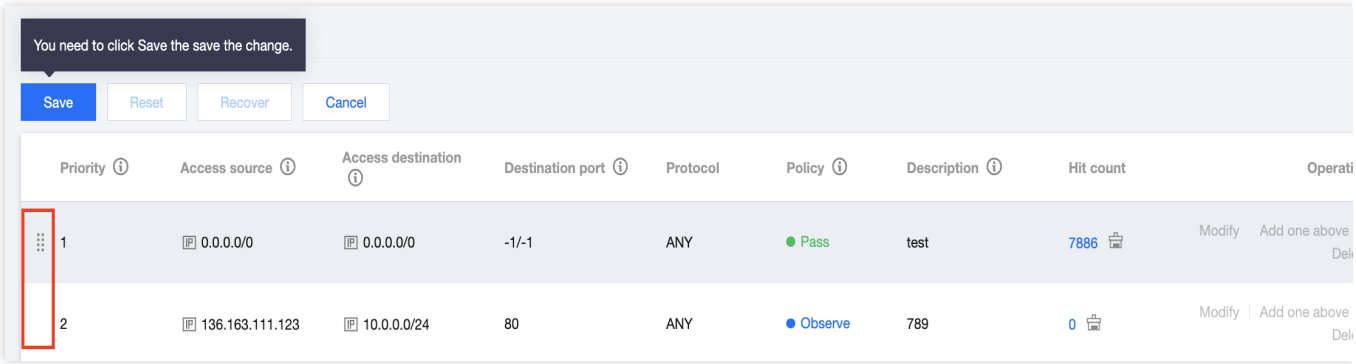
You can manage the execution priority of edge firewall rules, NAT firewall rules, and inter-VPC rules. The following takes **Edge firewall rules** as an example.

Scenario 1: Sorting rules in the list

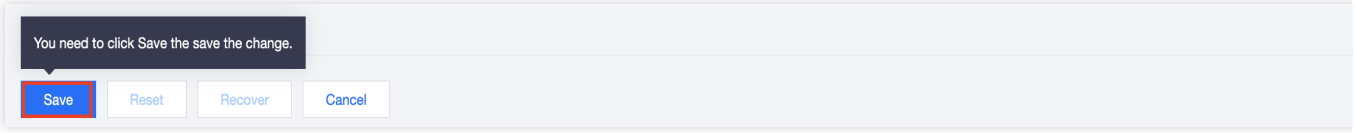
1. Log in to the Cloud Firewall console and select **Access Control** -> **Edge firewall rules** in the left navigation pane.
2. On the **Edge firewall rules** page, click **Sort** on the top of the list to enter the modification mode.



3. You can move the positions and priority of rules in batch within the current page, and sort the rules by dragging the icons on their left.



4. When you are done, click **Save**.



Sort operations:

If you change the **position** of any rule when you release the mouse cursor, one sort operation has taken place.

If you do not change the **position** of any rule when you release the mouse cursor, no sort operation has taken place.

After a sort operation takes place, the **Cancel** button becomes active.

Click **Recover** once to return the list to the state before the last sort operation.

If you click **Save**, you will see a **Sorted successfully** toast at the top of the page.

If you click **Cancel**, the list will return to the initial state and all sort operations will not take effect.

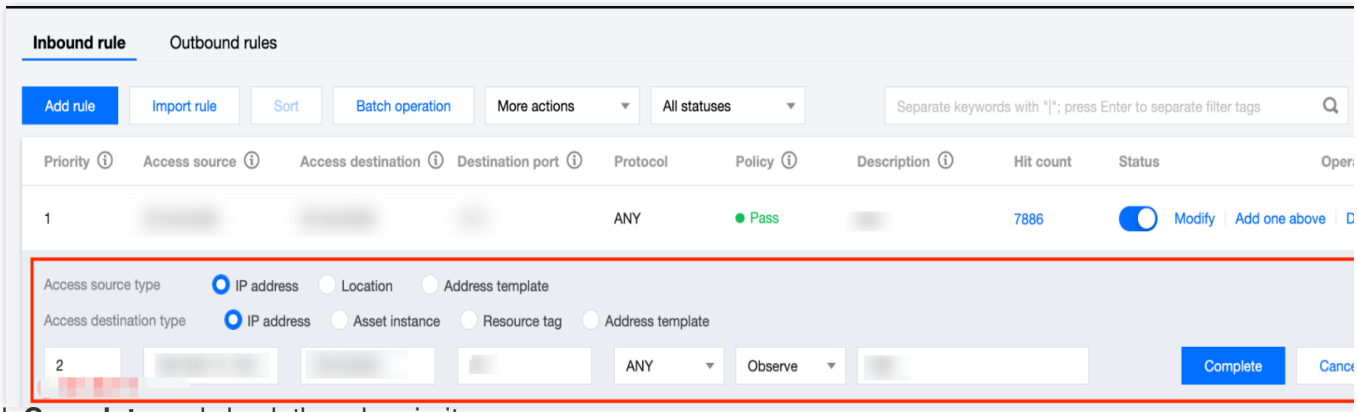
Scenario 2: Modifying a rule to move it to a specified position

When you need to move a rule within a large range, sorting is inefficient. Instead, you can use the modification feature. You can modify the execution priority of only one rule at a time.

1. Log in to the Cloud Firewall console and select **Access Control** -> **Edge firewall rules** in the left navigation pane.
2. On the **Edge firewall rules** page, find the rule you want to move in the list, and determine the new position.
3. Click **Modify** on the right to enter the rule modification mode.
4. Modify the execution priority to the desired value.

Note：

Execution priority values cannot be repeated and are continuous. As such, the minimum value is 1 and the maximum value is the total number of rules in the current list.



5. Click **Complete** and check the rule priority.

Note：

When you modify the execution priority of a rule in the list, the positions of all other rules will be automatically adjusted.

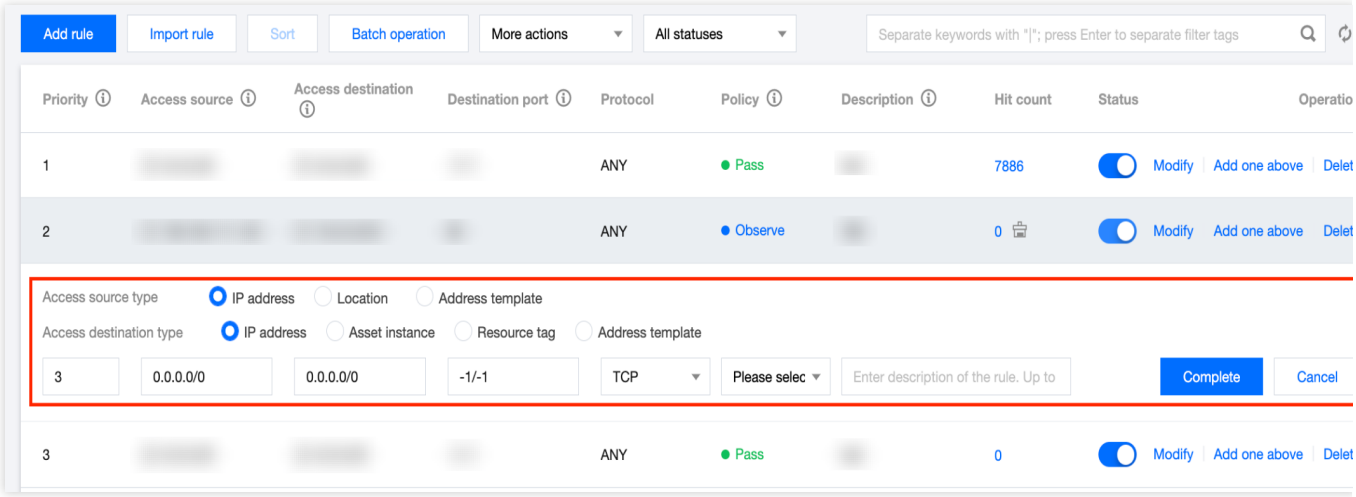
Scenario 3: Inserting a rule to a specified position in an existing list

Cloud Firewall allows you to insert a rule between any two rules, and the inserted rule will be executed in the priority. The rule will be inserted above the selected position. In the following example, we want to insert a rule between the rules in positions **2** and **3**:

1. Log in to the Cloud Firewall console and select **Access Control** -> **Edge firewall rules** in the left navigation pane.
2. On the **Edge firewall rules** page, find the rule in position **3** in the list, and click **Add one above** on the right.
3. The rule modification box will be displayed above the rule in position **3**.
4. In the box, enter the fields of the new rule and click *Complete** to insert the rule.

Note：

The inserted rule will take the position of the rule below it, and the execution priority of all the rules below the new rule will be **moved down by one position**.

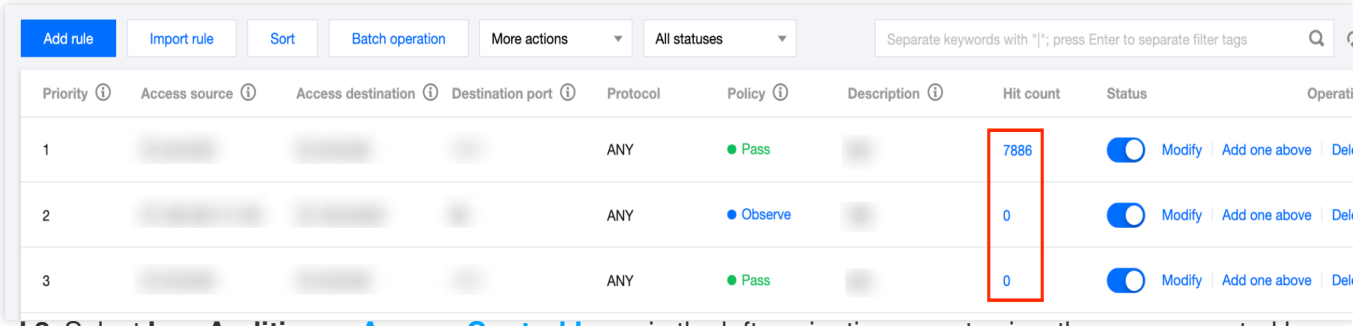


Checking if rules are effective

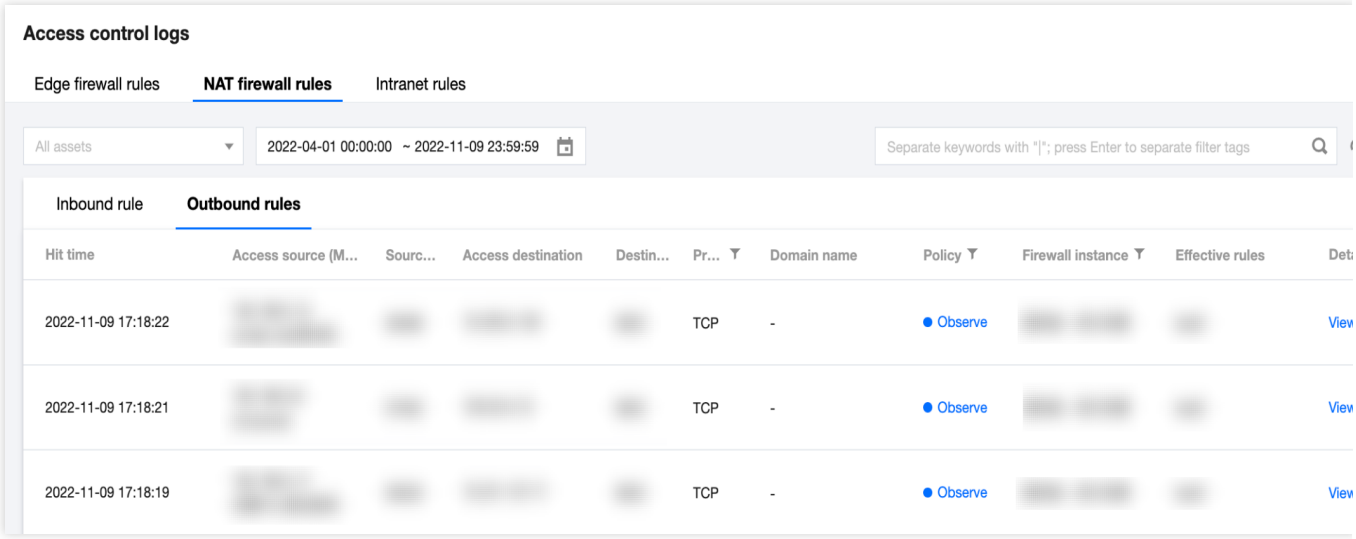
Method 1: Check the hit counts in the access control list. If there are hits, the rules have taken effect.

Note：

If a rule has zero hits, it does not necessarily mean that the rule is incorrectly configured. The rule may simply have no hits for the time being.



Method 2: Select **Log Auditing** -> **Access Control Logs** in the left navigation pane to view the access control logs (rule hit logs). If a rule is included in the log, the rule has taken effect.

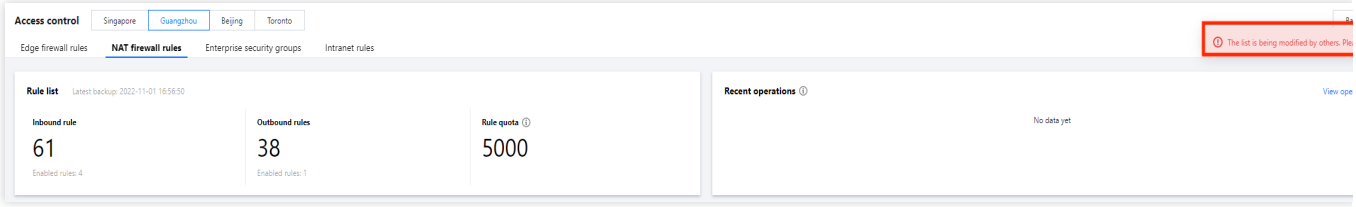


Operation locking

At any one time, only one user is allowed to execute any one of the following operations on a single access control list with the same AppID (the firewall ID is used for VPCs): **Add rule**, **Import rule**, **Sort**, **Modify**, and **Add one above**. When performing operations on a list, you may see the toast **The list is being modified by others. Please wait.** This means that another user is performing operations on the list.

Note

Operations are locked for 5 minutes, and will be automatically unlocked after that time period.



More information

For more information, please see Access Control.

Intrusion Defense
Enabling Threat Intelligence

Last updated：2024-01-24 16:09:41

After threat intelligence is enabled, CFW feeds network perimeter traffic to the threat intelligence detection and analysis engine to identify unknown risks beyond access control rules. Prioritized protection packages are also available to enhance risk resistance capabilities in prioritized protection scenarios.

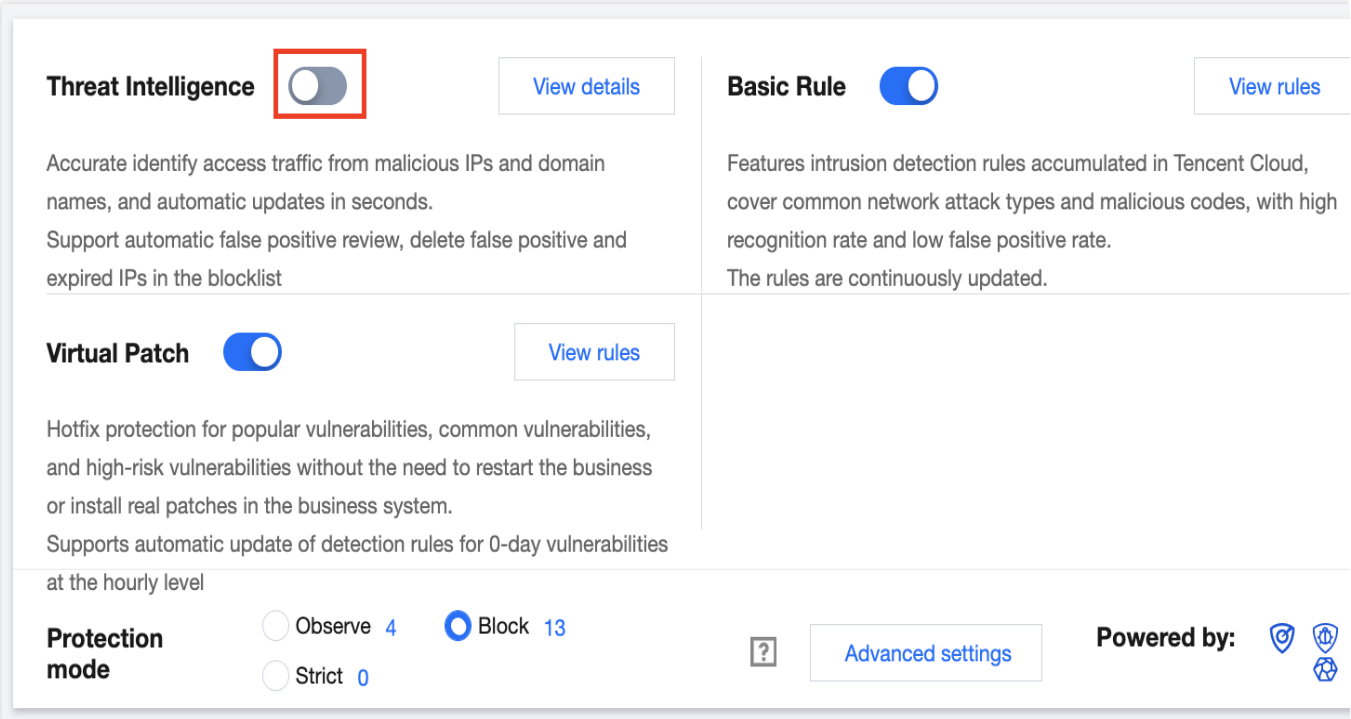
Directions

1. Log in to the Cloud Firewall console and click **Intrusion Protection System** in the left navigation pane.
2. On the **Intrusion protection system** page, click

next to **Threat intelligence** to enable this feature.

Note：

Only when threat intelligence and edge firewall are both enabled for a public IP address, CFW monitors and analyzes the north-south traffic on this IP address based on the threat intelligence.



3. After threat intelligence is enabled, CFW feeds network perimeter traffic to the threat intelligence detection and analysis engine to identify unknown risks beyond access control rules:

Malicious incoming access: CFW detects malicious scanning, brute-force attacks, and remote control from malicious IP addresses to cloud assets, as well as mining Trojans, ransomware, and other threat samples.
Outgoing access: CFW detects outgoing access from cloud assets to external malicious IP addresses or domain names, and identifies potential server compromise risks through the comparative analysis of big data provided by threat intelligence.

More Information

For questions about intrusion defense, please see Intrusion Protection System.

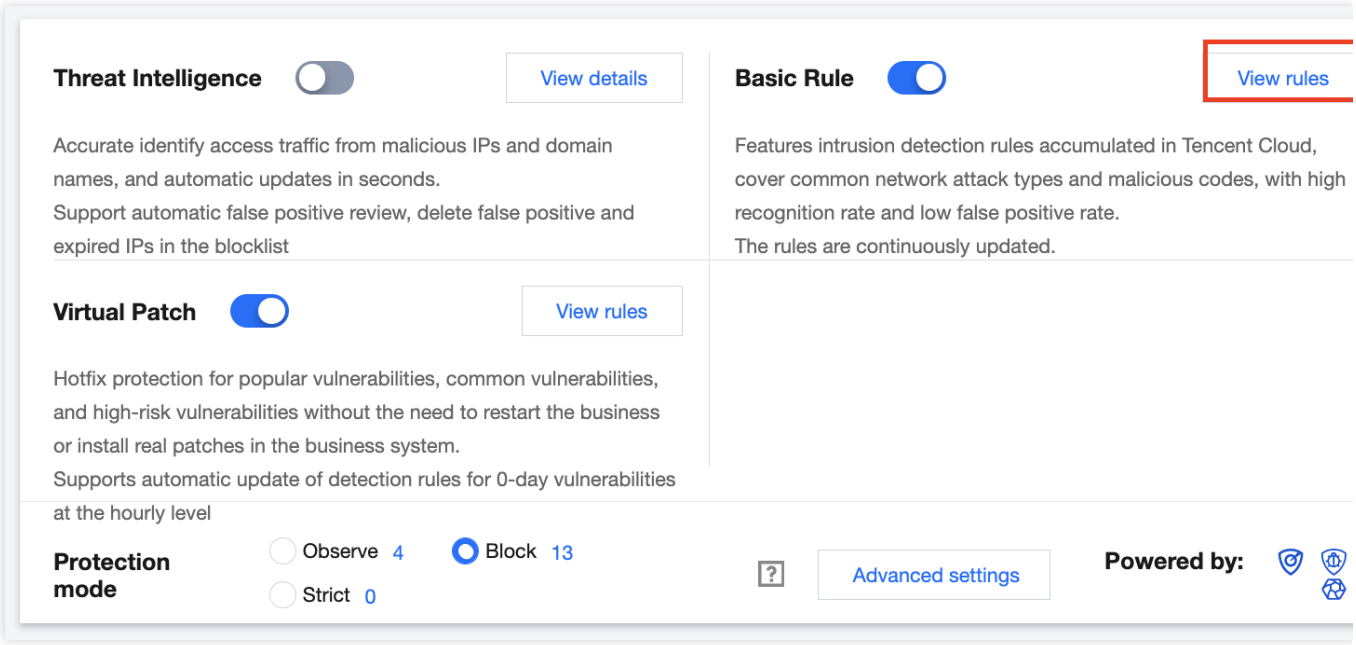
Enabling Basic Protection

Last updated：2024-01-24 16:09:41

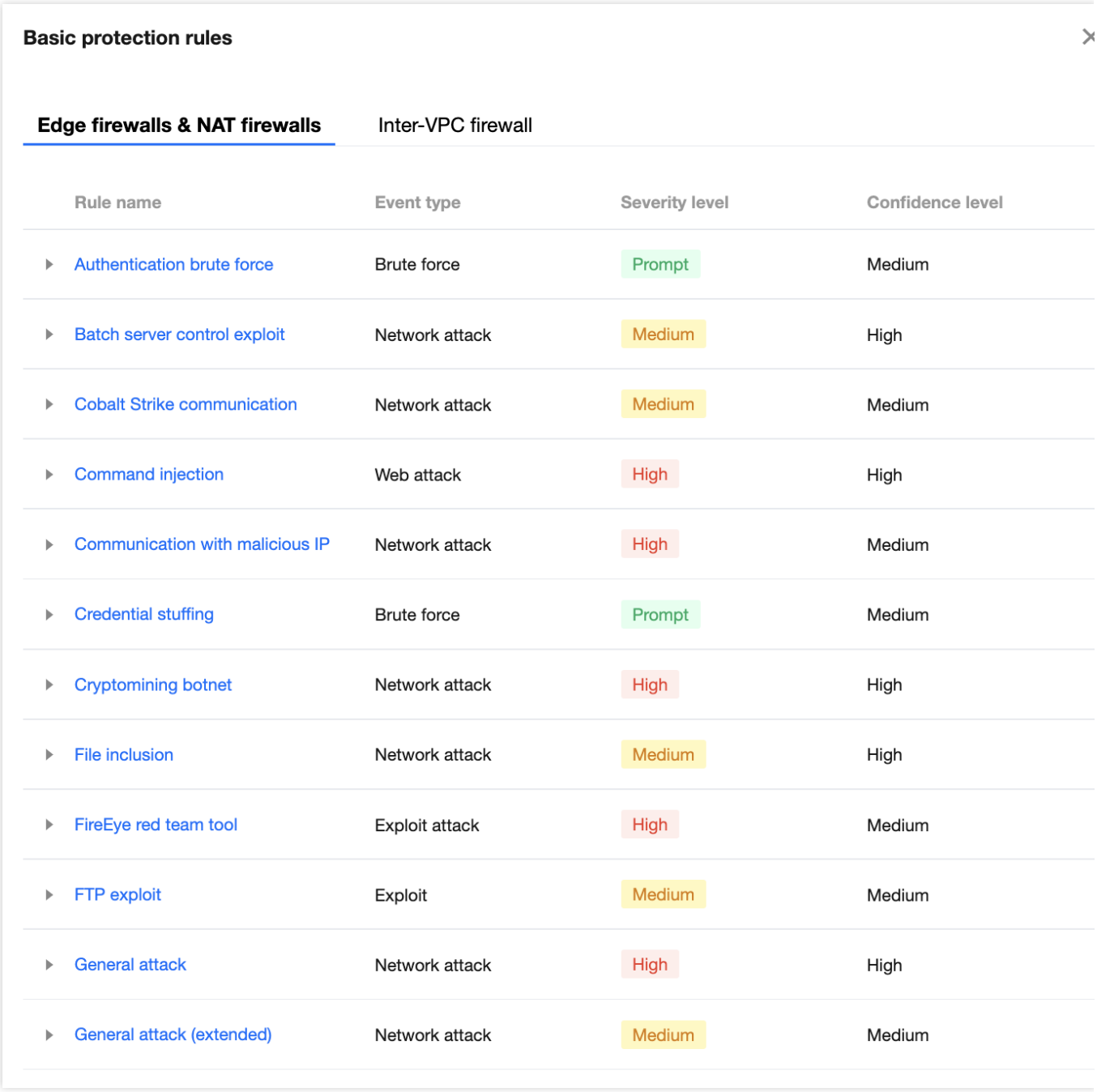
After basic protection is enabled, the north-south traffic on public IP addresses can be monitored based on intrusion defense rules.

Directions

1. Log in to the Cloud Firewall console and click **Intrusion Protection System** in the left navigation pane.
2. On the **Intrusion protection system** page, click **View rules** in the **Basic protection** module.



3. In the **Basic protection rules** window displayed, you can view the description of any rule.



4. After viewing the rules, click

in the **Basic protection** module to enable this feature.

Note

When basic protection is disabled, the basic protection rules no longer take effect.

Only when basic protection and edge firewall are both enabled for a public IP address, CFW monitors the north-south traffic on this IP address based on intrusion defense rules.
In the Block mode, malicious behaviors that hit high-confidence rules are automatically blocked, and security event alerts are generated when other rules are hit.

More information

For questions about intrusion defense, please see Intrusion Protection System.

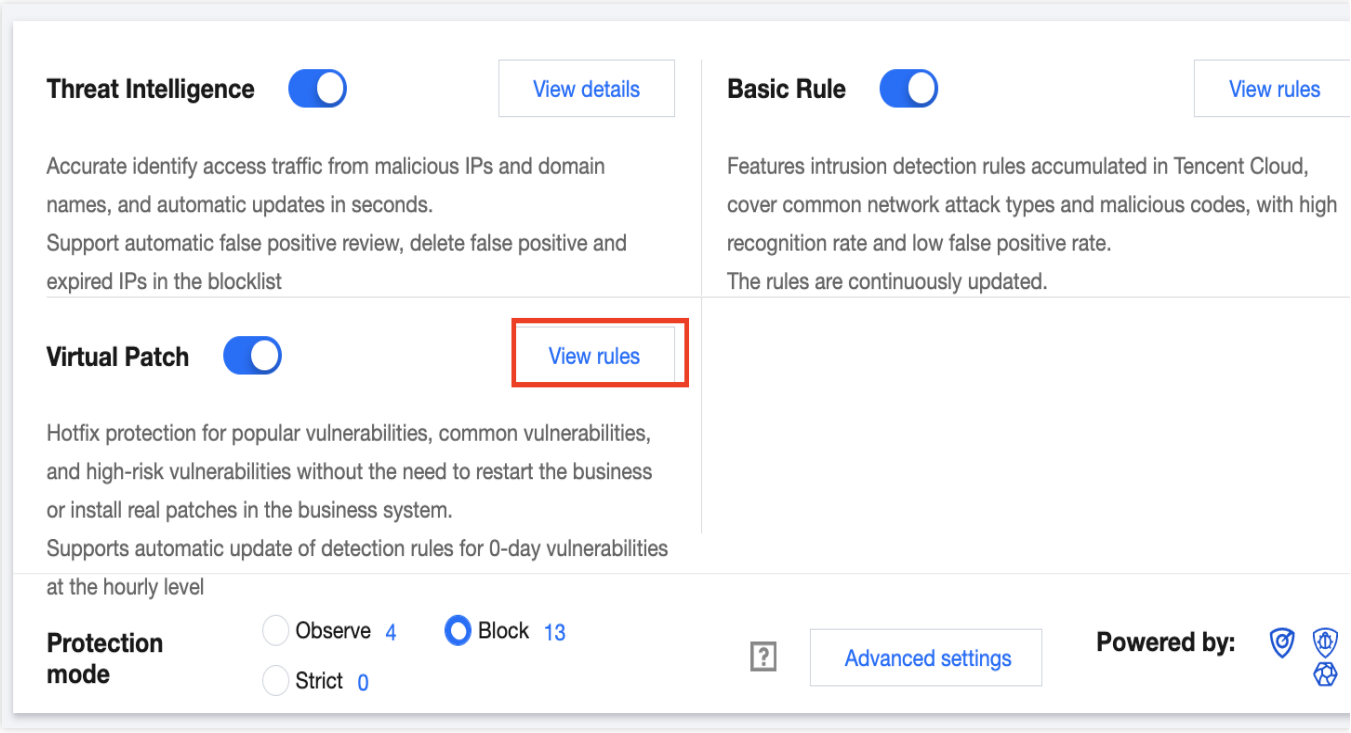
Enabling Virtual Patching

Last updated：2024-01-24 16:09:41

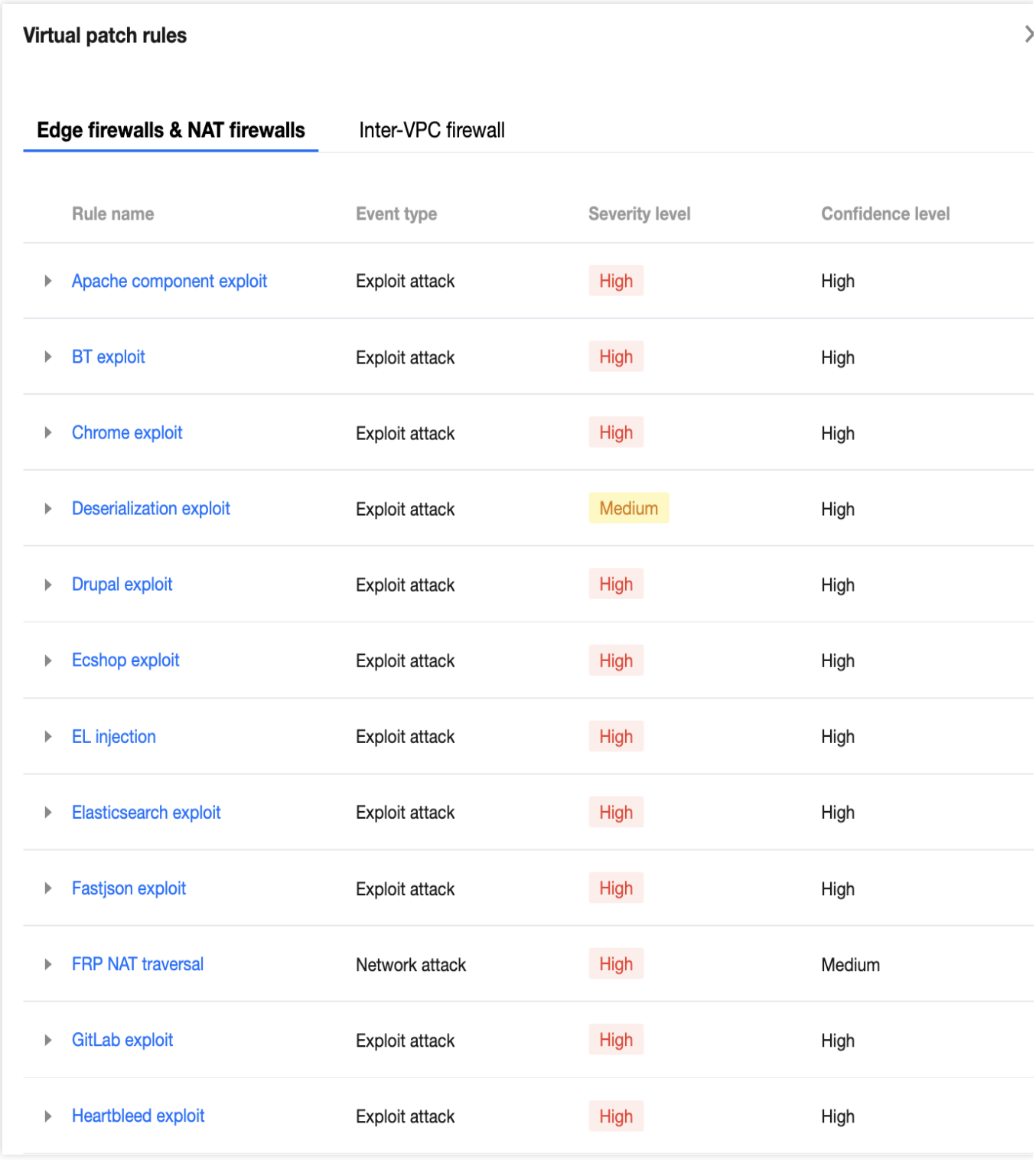
After virtual patching is enabled, CFW automatically identifies and blocks north-south traffic that may exploit vulnerabilities to launch attacks, preventing CVM vulnerabilities from being exposed to the Internet.

Directions

1. Log in to the Cloud Firewall console and click **Intrusion Protection System** in the left navigation pane.
2. On the **Intrusion protection system** page, click **View rules** in the **Virtual patching** module.



3. In the **Virtual patch rules** window displayed, you can view all the patches applied and the description of corresponding vulnerabilities.



4. After viewing patch rules, click

next to **Virtual patching** in the **Virtual patching** module to enable this feature.

Caution

When virtual patching is enabled, the virtual patch rules take effect for public IP addresses with this feature enabled.

When virtual patching is disabled, the virtual patch rules do not take effect.

In the Block mode, all intrusions are automatically blocked.

More information

For questions about intrusion defense, please see Intrusion Protection System.

Managing Defense Operations

Last updated：2024-01-24 16:11:14

This topic describes how to use the Intrusion Protection System (IPS) to identify unknown risks beyond access control rules, monitor the north-south traffic of public IP addresses based on intrusion defense rules, and prevent CVM vulnerabilities from being exposed to the Internet.

Selecting a protection mode

1. Log in to the Cloud Firewall console and click **Intrusion Protection System** in the left navigation pane.
2. On the **Intrusion protection system** page, configure the protection mode in the **Protection mode** module.
Three protection modes are available: **Observe**, **Block**, and **Strict**.

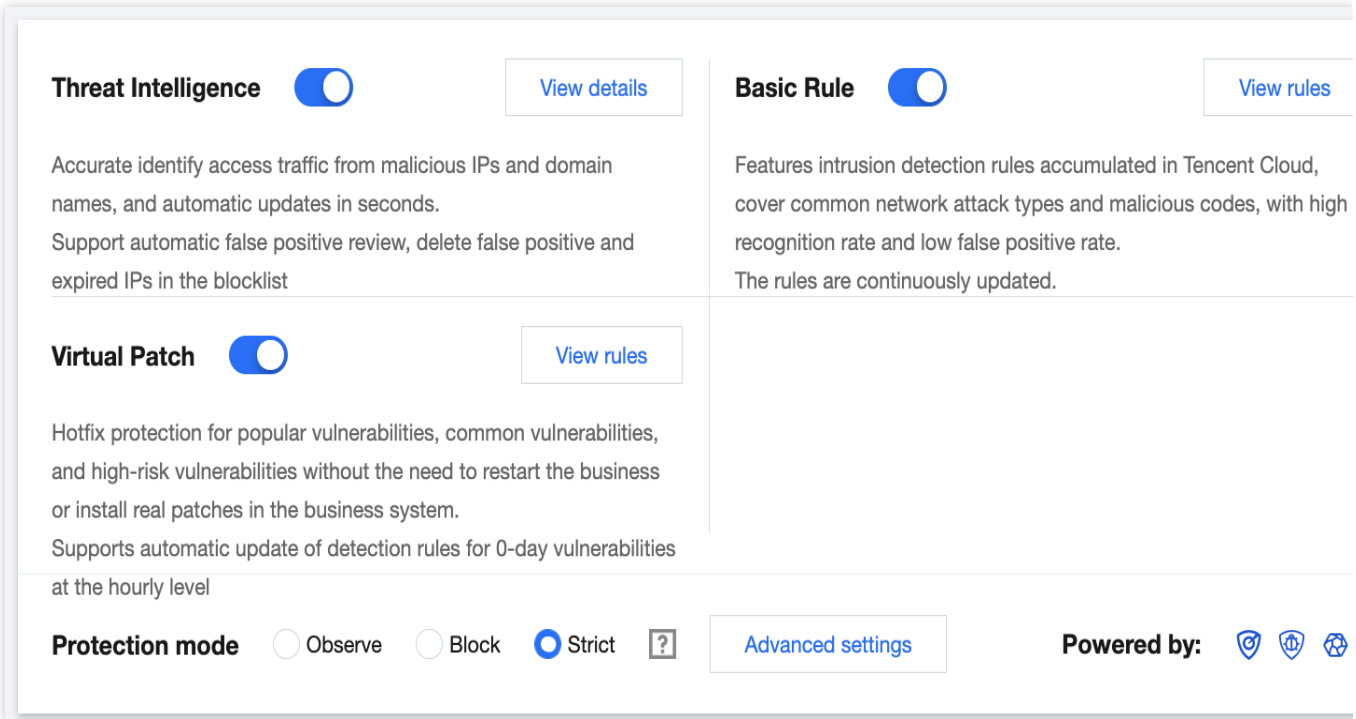
Note：

The default protection mode is Observe.

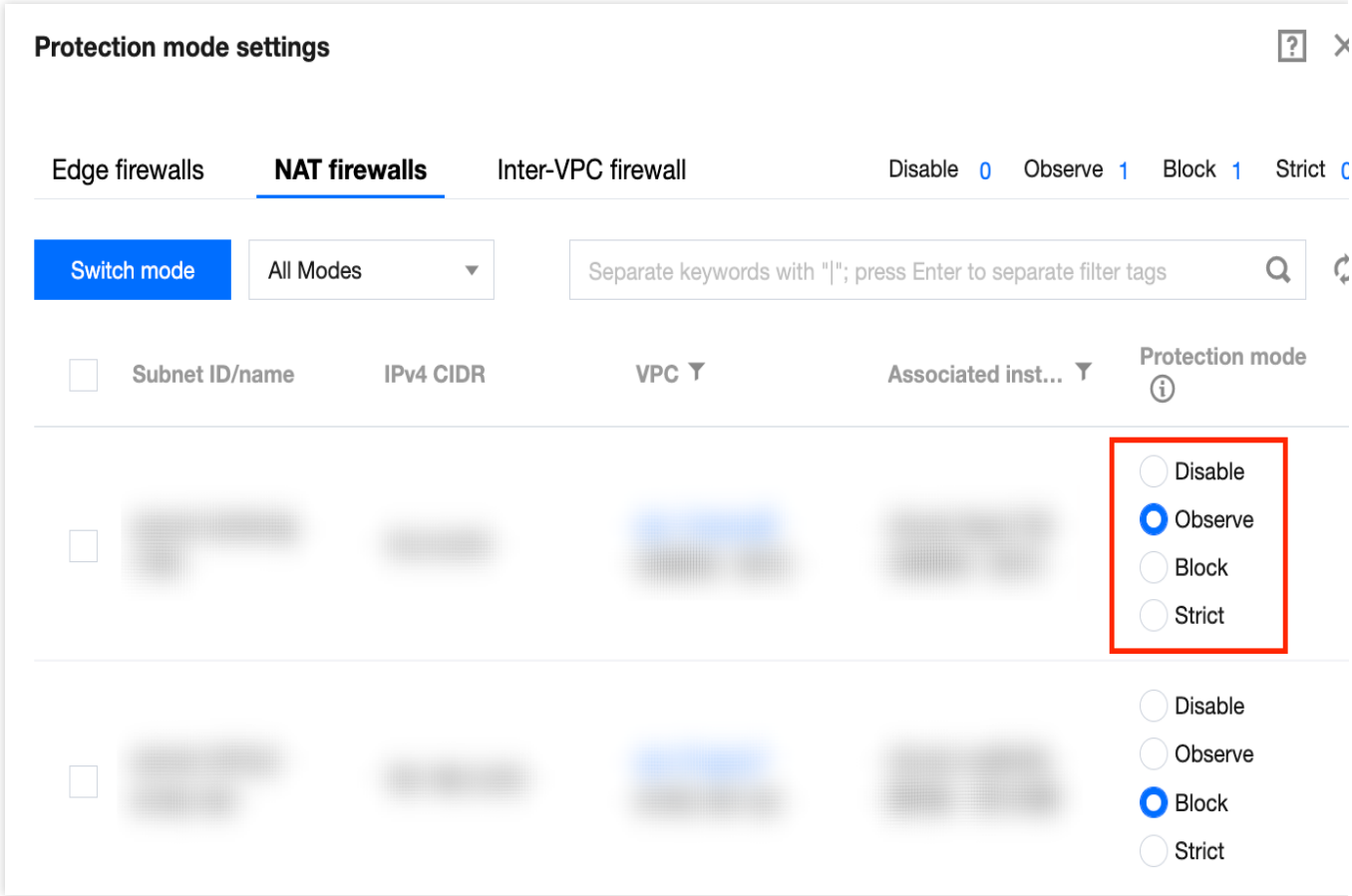
In the Observe mode, threat intelligence, basic protection, and virtual patching only detect and send alerts against malicious access or network attacks without interrupting the connections.

In the Block mode, threat intelligence automatically blocks outbound malicious access, basic protection blocks network attacks that trigger high-confidence rule alerts, and virtual patching blocks all the traffic detected as vulnerability exploits.

In the Strict mode, threat intelligence (except for detection of outbound domain names), basic protection, and virtual patching block any detected malicious behaviors that trigger alerts while interrupting the connections. Note that this can cause false positives and is only suggested when the asset is under attack.



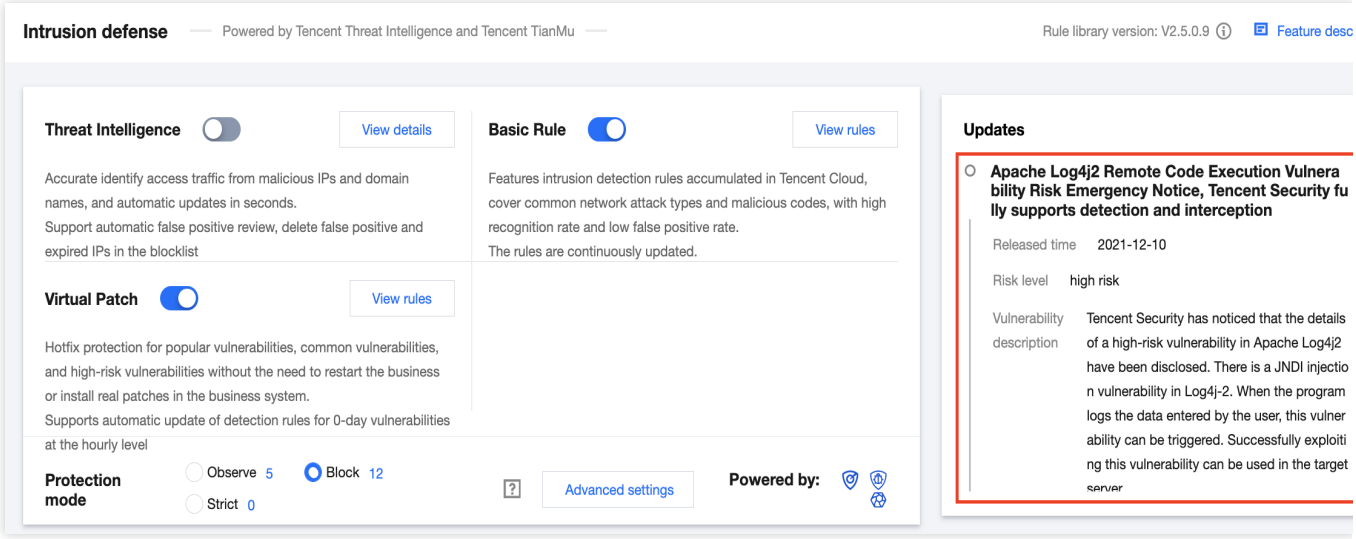
3. Click **Advanced settings** on the right side of the **Protection mode** module.
4. In the **Advanced settings** window displayed, configure the protection mode for each asset under **Edge firewall**, **NAT firewall**, and **Inter-VPC firewall** respectively.



IPS overview

1. Log in to the Cloud Firewall console and click **Intrusion Protection System** in the left navigation pane.
2. On the right side of the **Intrusion protection system** page, feature updates and feature descriptions are displayed.

Feature updates: You can view the features of IPS modules.



Intelligence center:

2.1.1 Click **Intelligence center** at the upper right corner of feature updates to view security threat intelligence information.

2.1.2 In the **Intelligence center** window displayed, click an intelligence title to view details about vulnerability description and threat level. You can also scan your assets for the threats reported in the vulnerability intelligence.

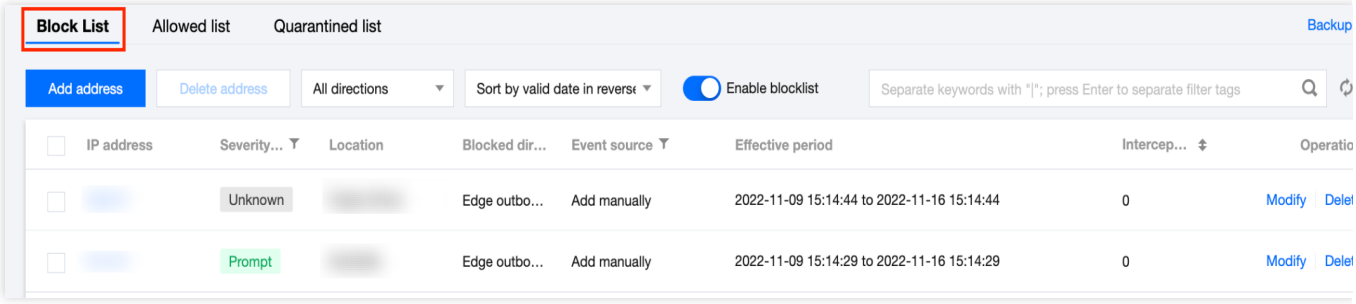
Managing lists

1. Log in to the Cloud Firewall console and click **Intrusion Protection System** in the left navigation pane.
2. At the bottom of the **Intrusion protection system** page, you can view the **Blocklist**, **Allowlist**, and **Quarantined list**.

Blocklist

Viewing the blocklist

1. Click **Blocklist** to enter the blocklist.

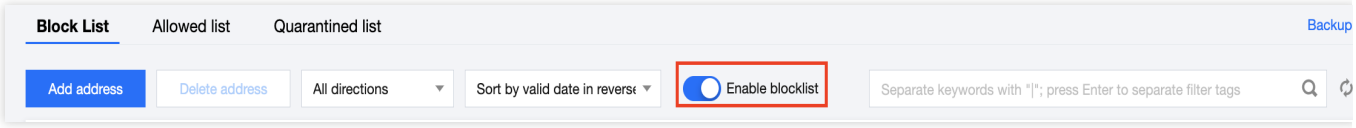


2. In the blocklist, you can view the IP addresses marked as "Blocked" in **Alert Management** -> **Attack alerts** and their information. You can also manually add IP addresses to the blocklist.

Disabling the blocklist

1. In case of emergency, click

to turn off **Enable blocklist**, and then go to **Alert Management** -> **Blocked attacks** to view all blocking statistics and locate the alert source.



2. After the fault is located and fixed, click

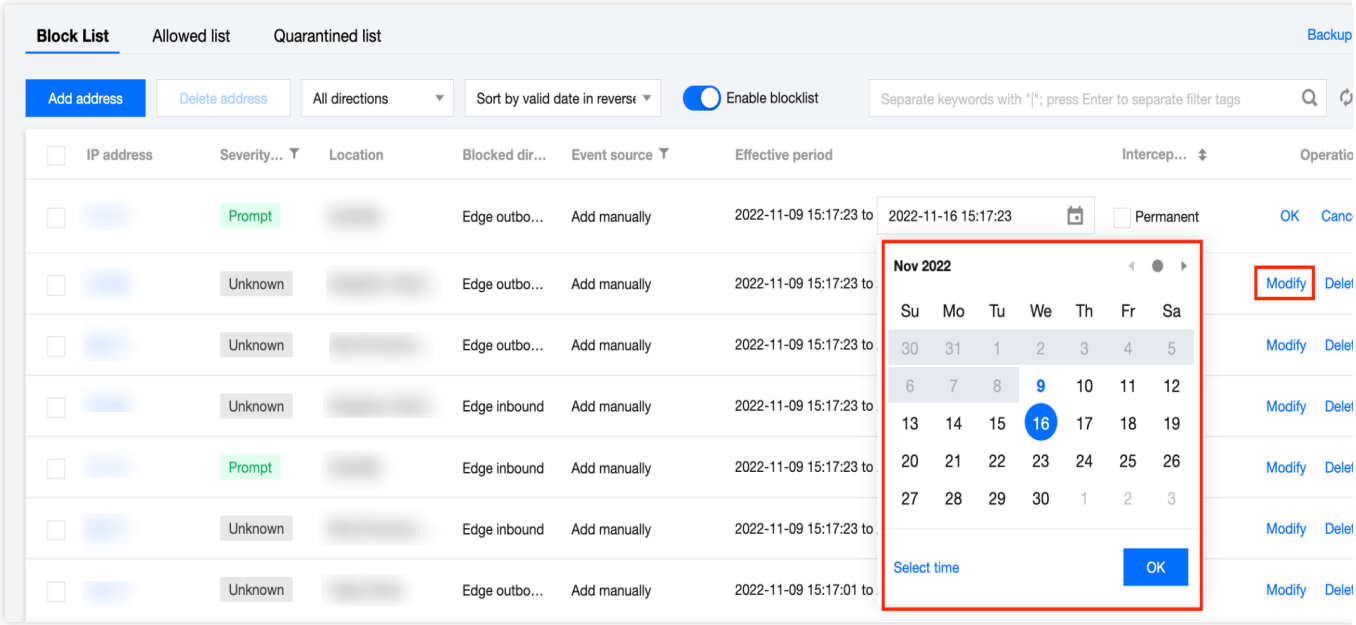
to turn on **Enable blocklist** again.

Managing the effective period in the blocklist

An IP address whose effective period expires will be automatically removed from the blocklist, and traffic of this IP address will not be blocked by the firewall anymore. To prevent risky IP addresses from being automatically removed from the blocklist, you can click **Edit** in the action column on the right side of the blocklist to modify the expiration time for IP addresses.

Note：

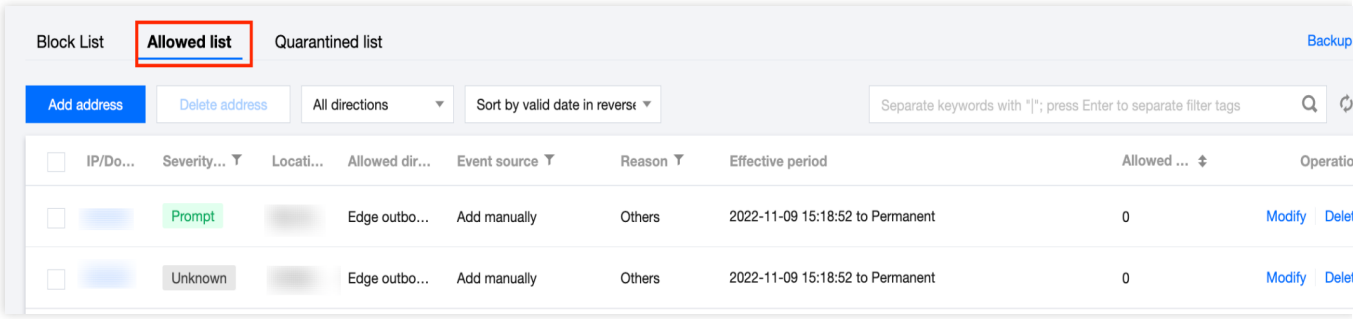
For IP addresses in the blocklist, their inbound or outbound traffic that goes through CFW will be blocked and recorded in **Log Auditing** -> **Intrusion Defense Logs**.



Allowlist

Viewing the allowlist

1. Click **Allowlist** to enter the allowlist.



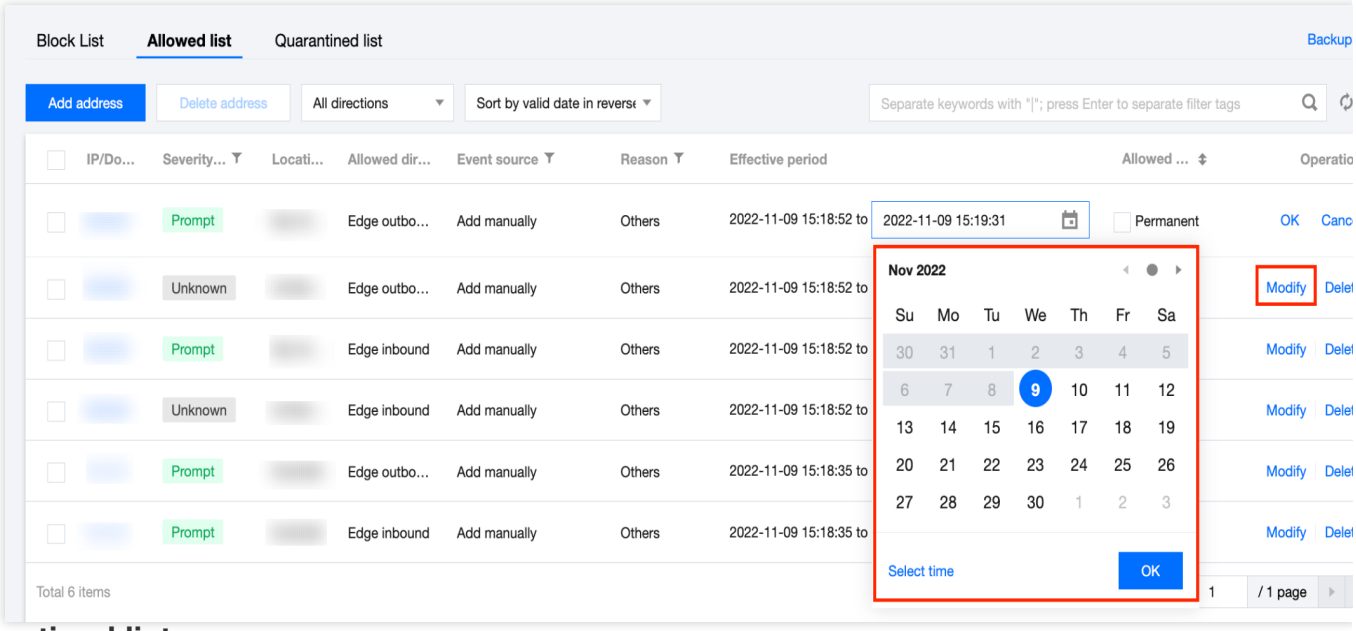
2. In the allowlist, you can view the IP addresses marked as "Allowed" in **Alert Management** -> **Attack alerts** and their information. You can also manually add IP addresses to the allowlist.

Note：

IP addresses in the allowlist will directly bypass the IDPS.

Managing the effective period in the allowlist

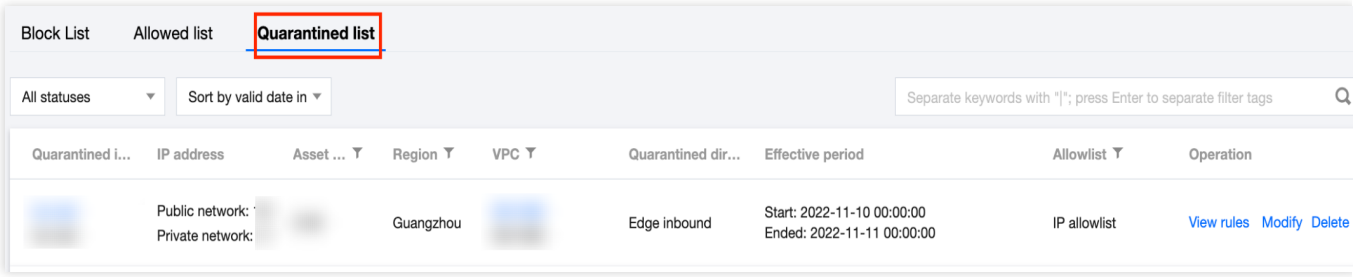
An IP address whose effective period expires will be automatically removed from the allowlist, and traffic of this IP address will not bypass CFW IDPS anymore. To prevent trusted IP addresses from being automatically removed from the allowlist, you can click **Edit** in the action column on the right side of the allowlist to modify the expiration time for IP addresses.



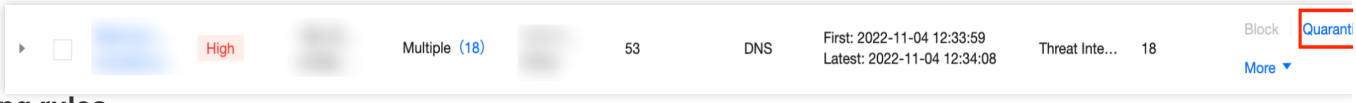
Quarantined list

Viewing the quarantined list

1. Click **Quarantined list** to enter the quarantined list.

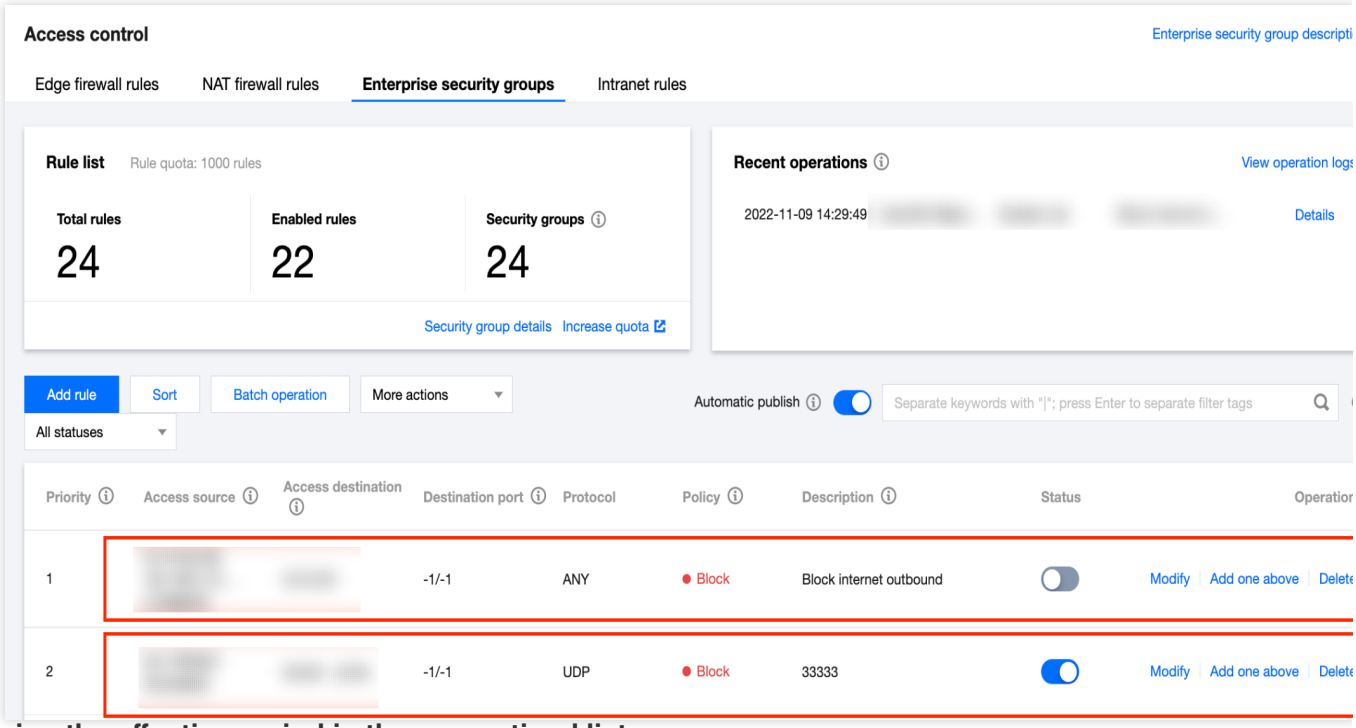


2. In the quarantined list, you can view the IP addresses marked as "Quarantined" in **Alert Management** -> **Attack alerts** -> **Server compromised** and their information.



Viewing rules

IP addresses of compromised servers are quarantined using security groups. Click **View rules** to go to the enterprise security group page and view detailed rule information.

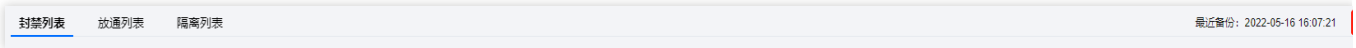


Managing the effective period in the quarantined list

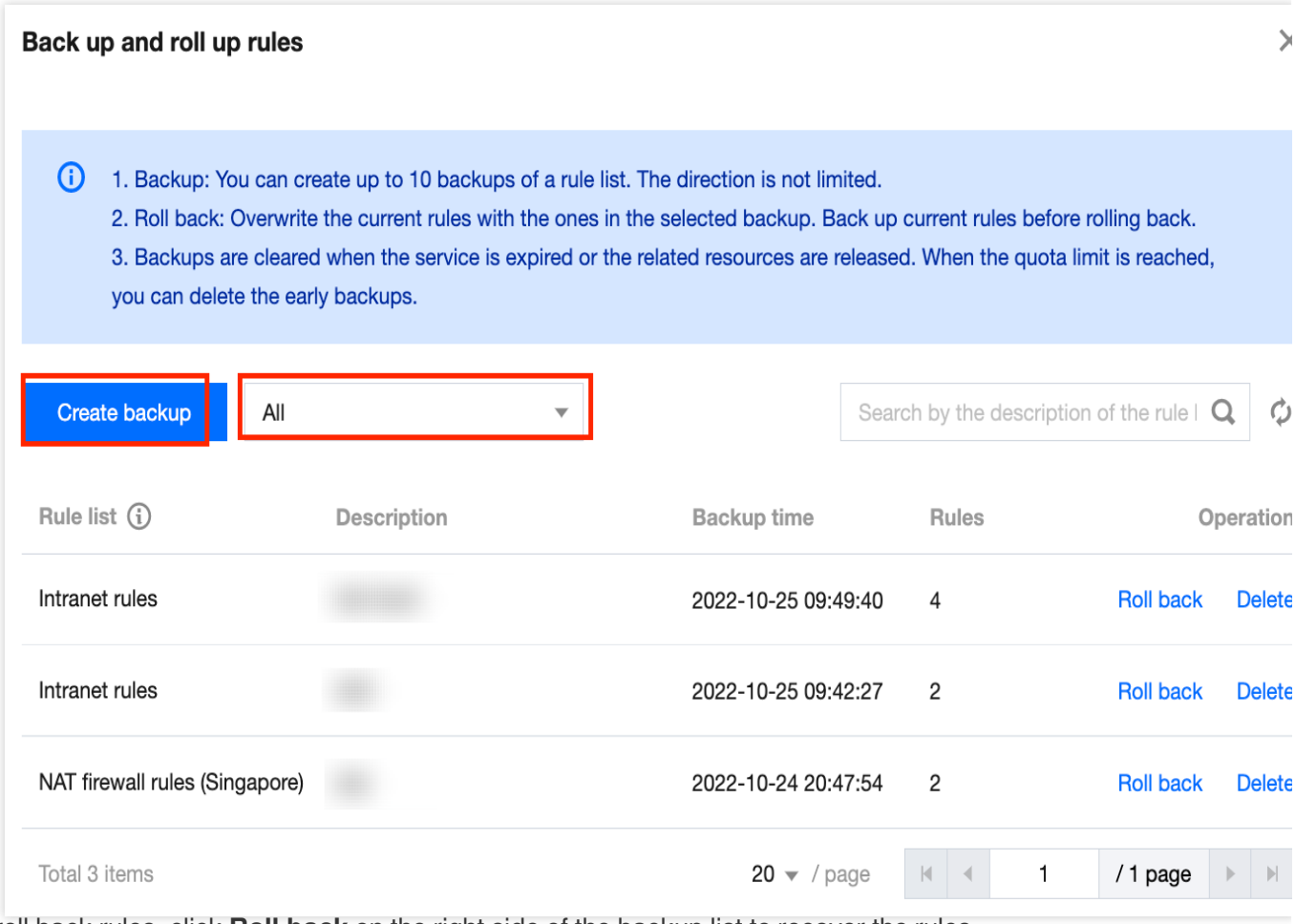
An IP address whose effective period expires will be automatically removed from the quarantined list, and the security group rules of this IP address will be deleted as well. To prevent IP addresses of compromised servers from being automatically removed from the quarantined list, you can click **Edit** in the action column on the right side of the quarantined list to modify the expiration time for IP addresses.

Backing up and rolling back rules

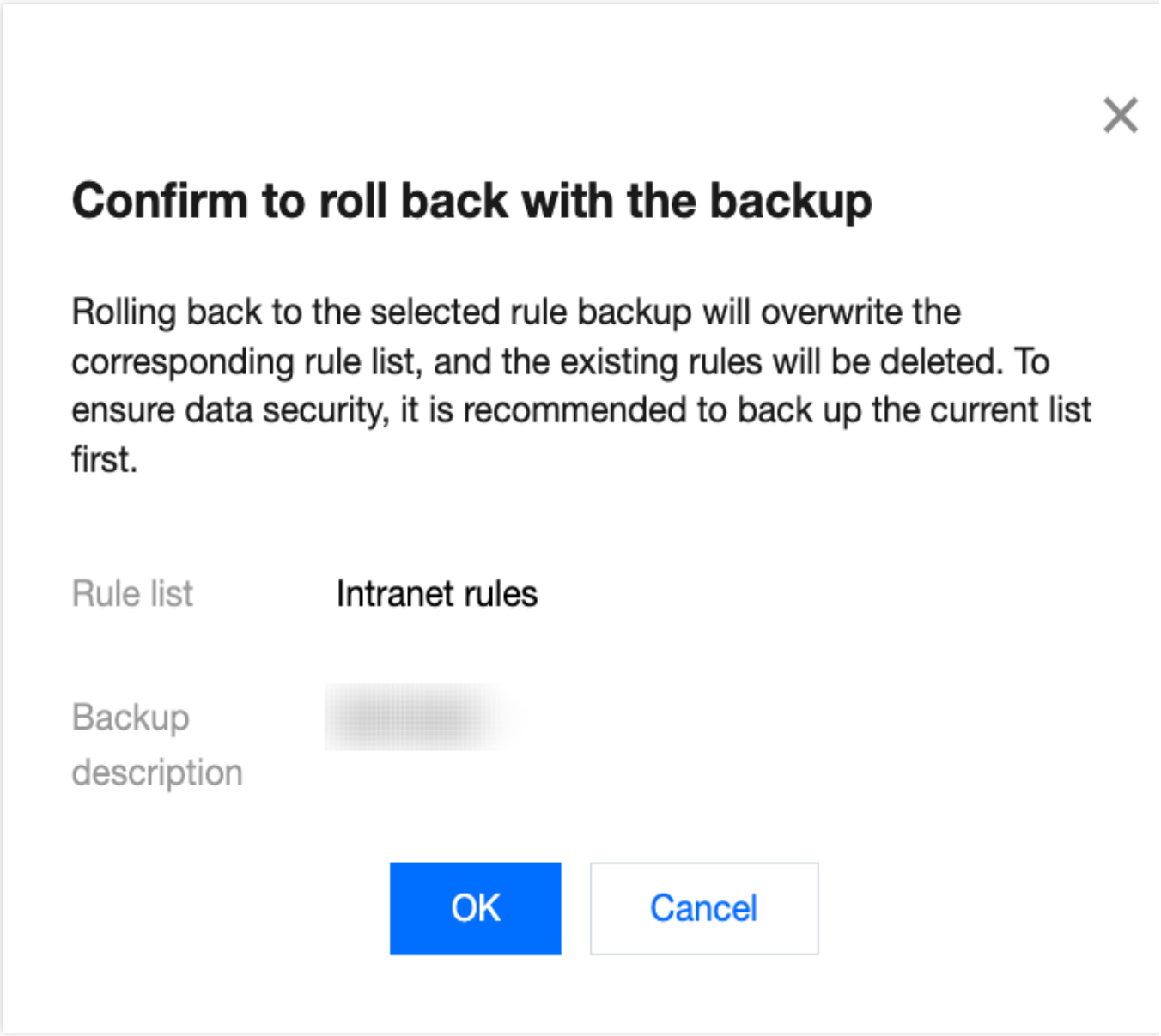
Click **Backup rules** to back up existing blocklist and allowlist rules. When the rules are greatly changed, you can click **Roll back** to the right of the backup file to recover the rules.



1. On the **Back up and roll up rules** page, click **Create backup**, select **Blocklist** or **Allowlist** from the drop-down list, enter a description, and click **OK** to complete the backup.



2. To roll back rules, click **Roll back** on the right side of the backup list to recover the rules.



More information

For questions about intrusion defense, please see Intrusion Protection System.

Honeypot
Overview

Last updated：2024-01-24 16:17:26

What is a network honeypot?

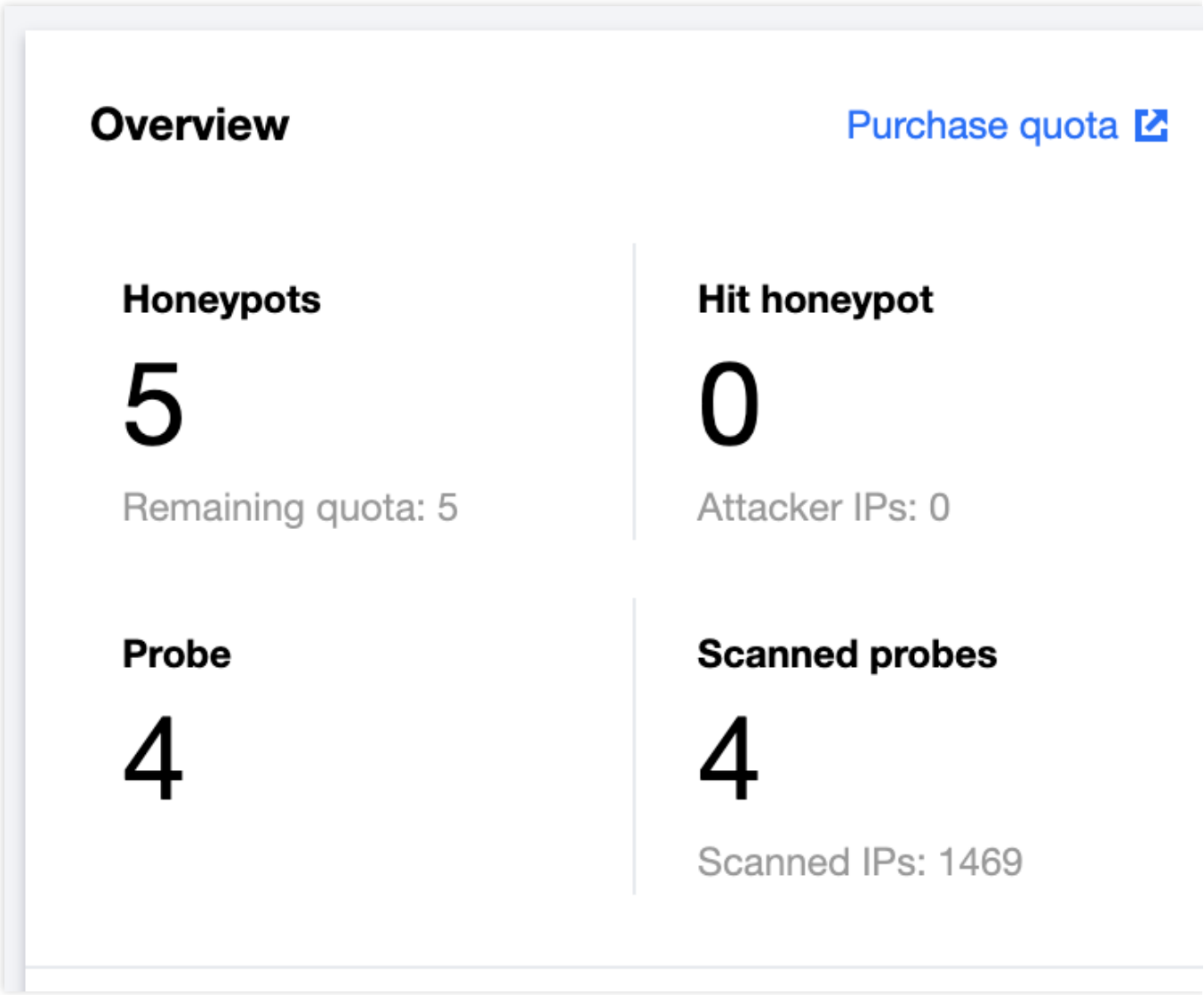
A network honeypot is a network-attached system that simulates businesses. Network honeypots expose probes in your network. When an attacker probes a honeypot, the attacker's information and attack method are traced and recorded, which can help you counter the attack. In prioritized protection scenarios, honeypots buy you time to protect businesses.
The Cloud Firewall honeypot service is deployed in Tencent Cloud's honeynet, and does not occupy your network space. The honeypots are isolated from each other as they are deployed in different VPCs. Thus, attackers will not gain lateral movement. Honeypot probes are deployed in your network based on an IP or domain name. Traffic of the specified ports/paths will be forwarded to different honeypot services so as to **trap** attackers.

Features and principles

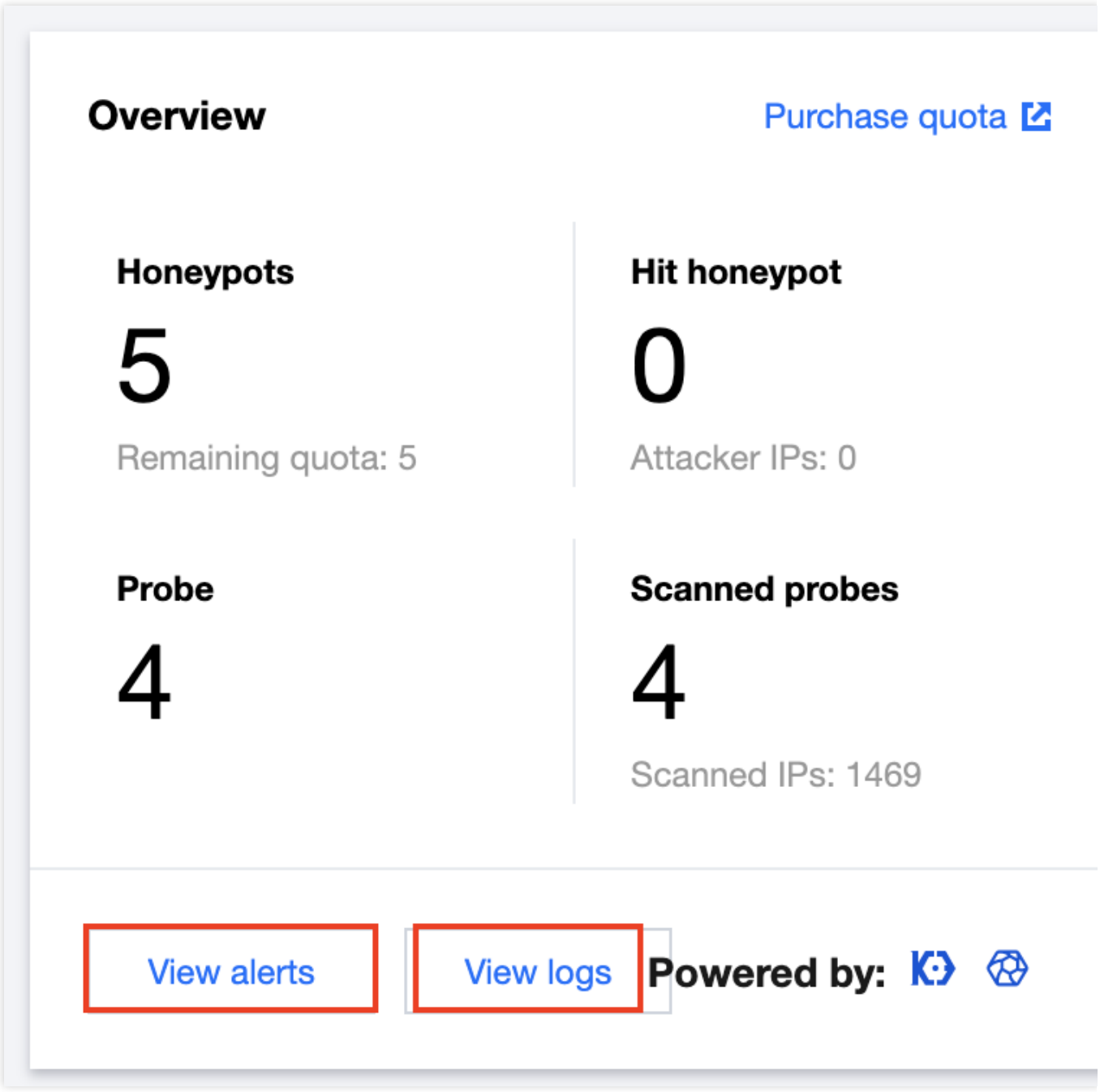
The Cloud Firewall honeypot service has three main features as follows:
Lures attackers with highly realistic simulations.
Collects attacker information to help you counter attacks.
Delays attackers and secures time to protect networks.
Increase your business security by setting more probes, which require little network resources. Using the highly realistic fake services in the honeynet, you can **deceive** attackers.

Checking the overview

1. Log in to the Cloud Firewall console and click **Network Honeypots** in the left navigation pane.
2. On the **Network honeypot** page, the overview will be displayed in the upper left corner, and you can quickly check the number of honeypot services, probes, hit honeypots, scanned probes, attacker IPs, and scanned IPs.



3. In the overview, click **View alerts** to go to the **Honeypot events** page, or click **View logs** to go to the **Honeypots** page of the intrusion defense logs.

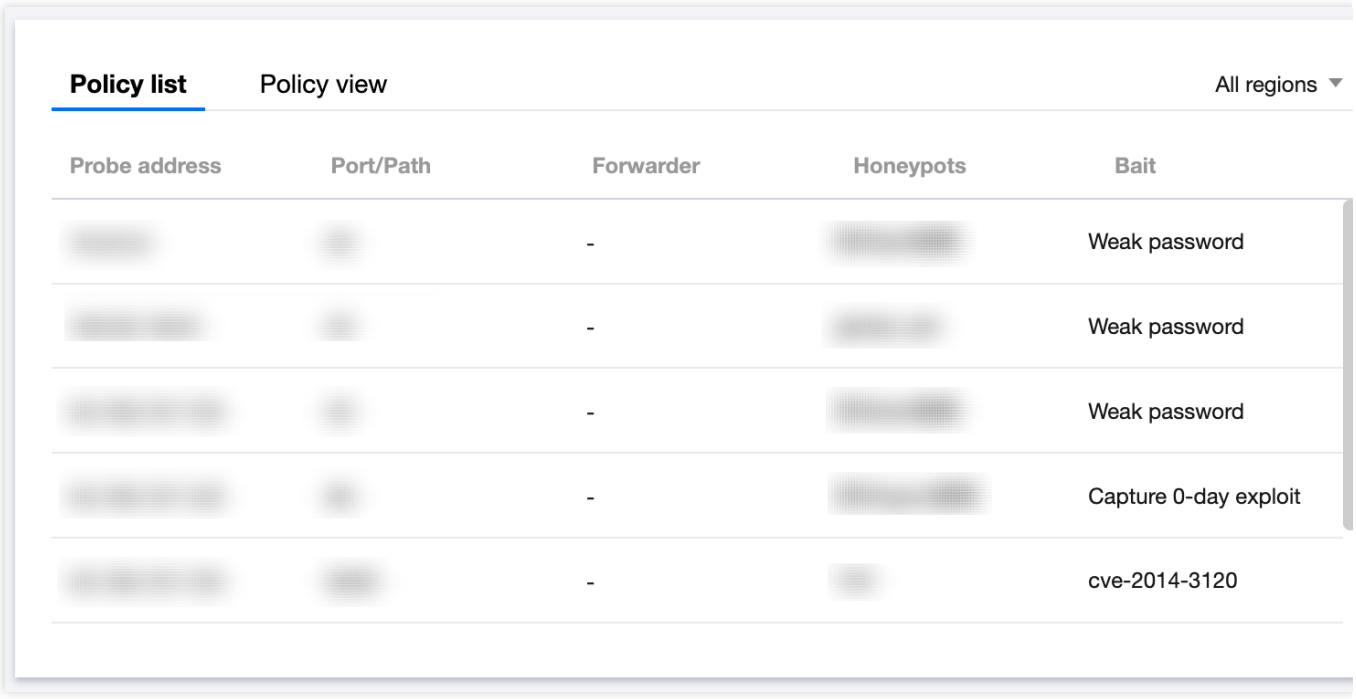


Viewing the honeypot policy map

The honeypot policy map includes a policy list and a policy view, which take the form of a table and a path chart, respectively. It shows the different paths, honeypot service types, and bait types corresponding to different probe addresses.

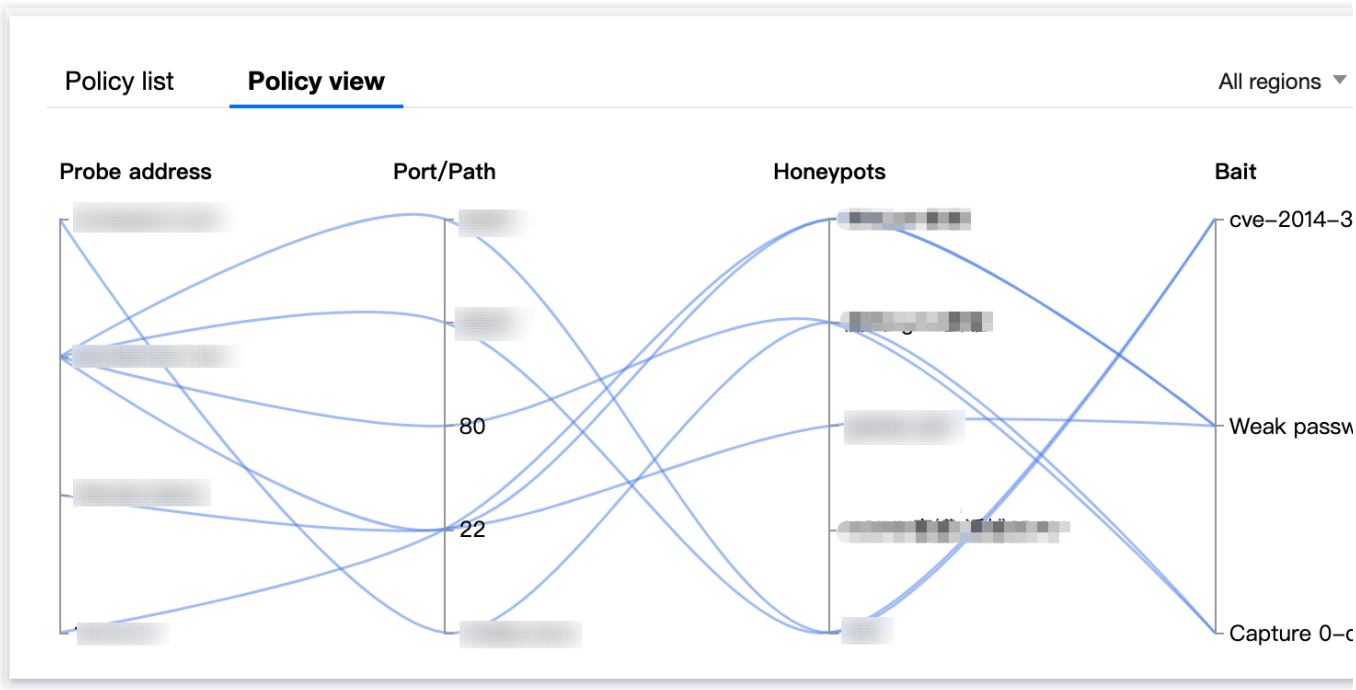
Policy list

The policy list shows the honeypot information corresponding to different probe addresses in detail.



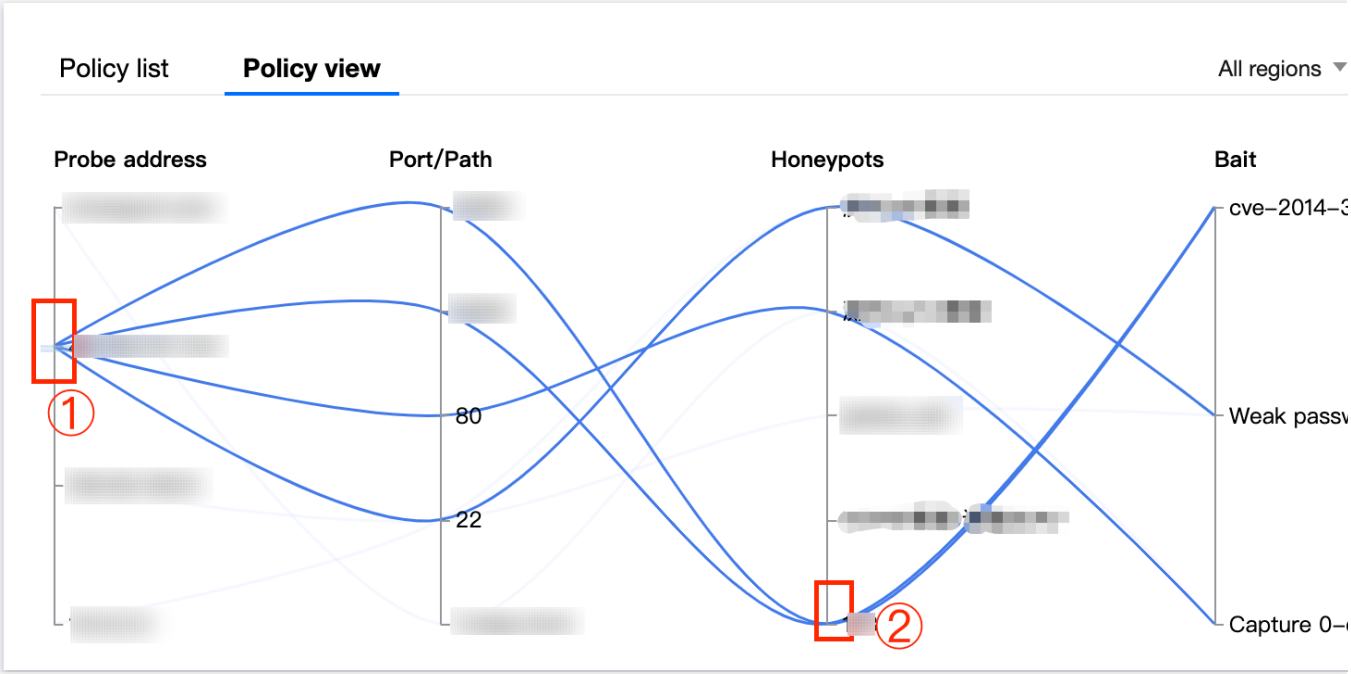
Policy view

The policy view intuitively displays the honeypot information corresponding to different probe addresses in different regions.



You can query specific probe addresses in the view by honeypot filter conditions. For example, you can hover the mouse cursor over ①**Probe address** and ②**Honeypot service** to find the corresponding probe and bait of the

honeypot. You can select the checkbox for any condition on this page to find the corresponding service and visualize the information.



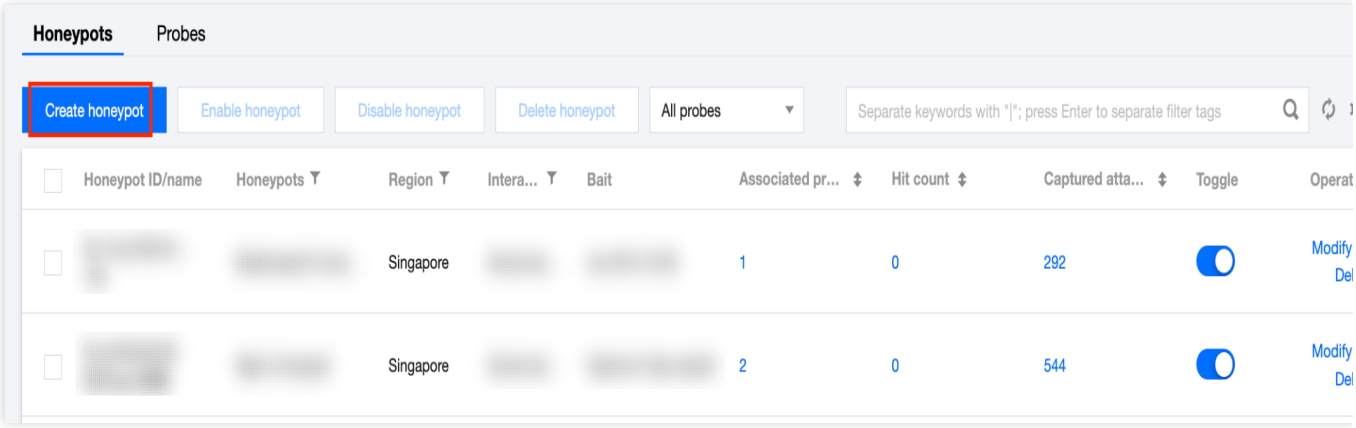
Honeypot Service

Last updated：2024-01-24 16:17:26

The network honeypot service must be associated with a probe to run properly. The **Probes** page is displayed by default after you enter the network honeypot console. You are advised to create a probe first, and then create a honeypot and associate it with the probe.

Creating a honeypot

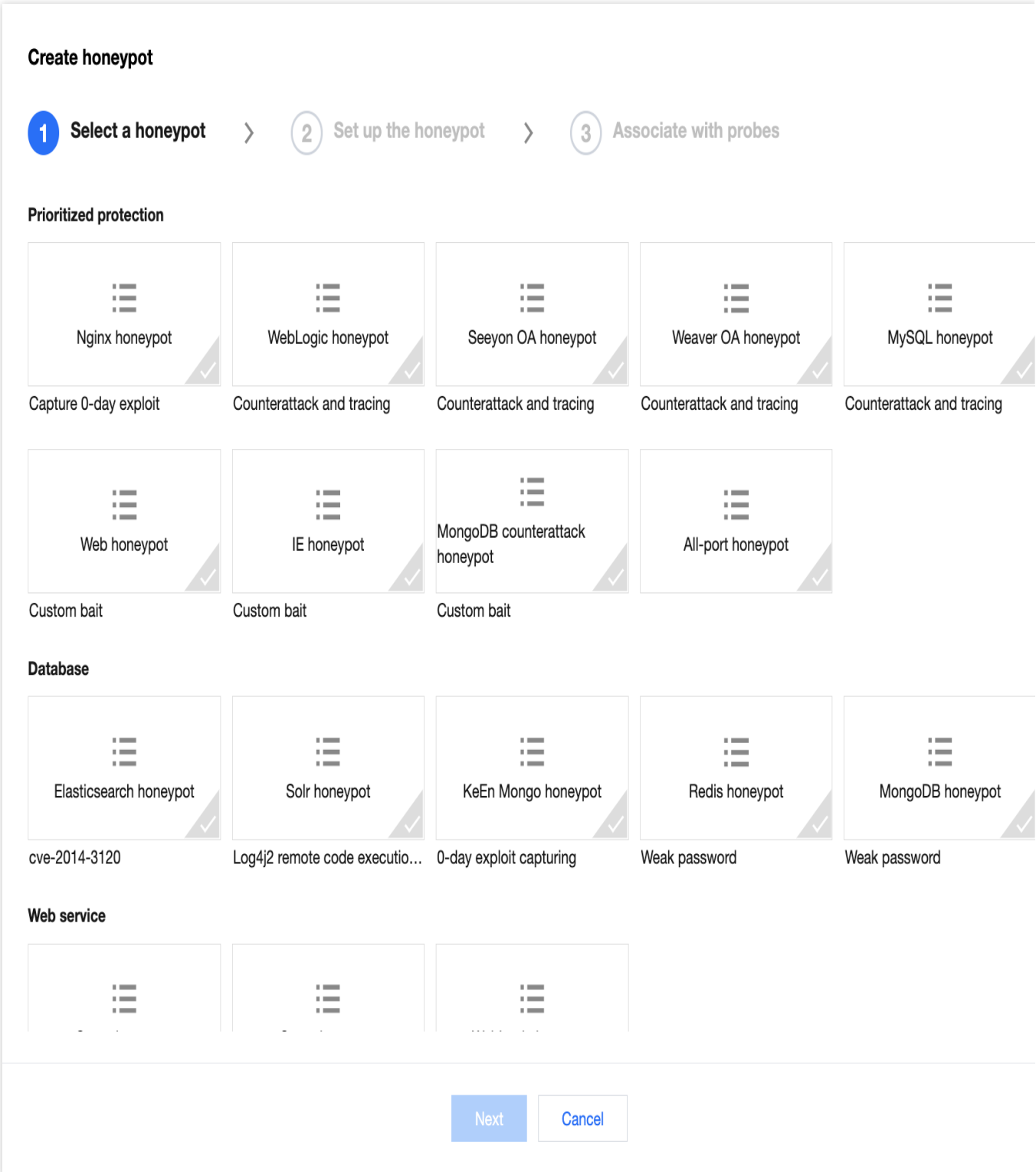
1. Log in to the Cloud Firewall console and click **Network Honeypots** in the left navigation pane.
2. On the **Network honeypots** page, select **Honeypots**, and then click **Create honeypot**.



3. In the **Create honeypot service** window displayed, configure the parameters, and then click **OK**.

Note

Parameters to be configured vary with the honeypot service selected. For more information, please see Parameters.



Parameters

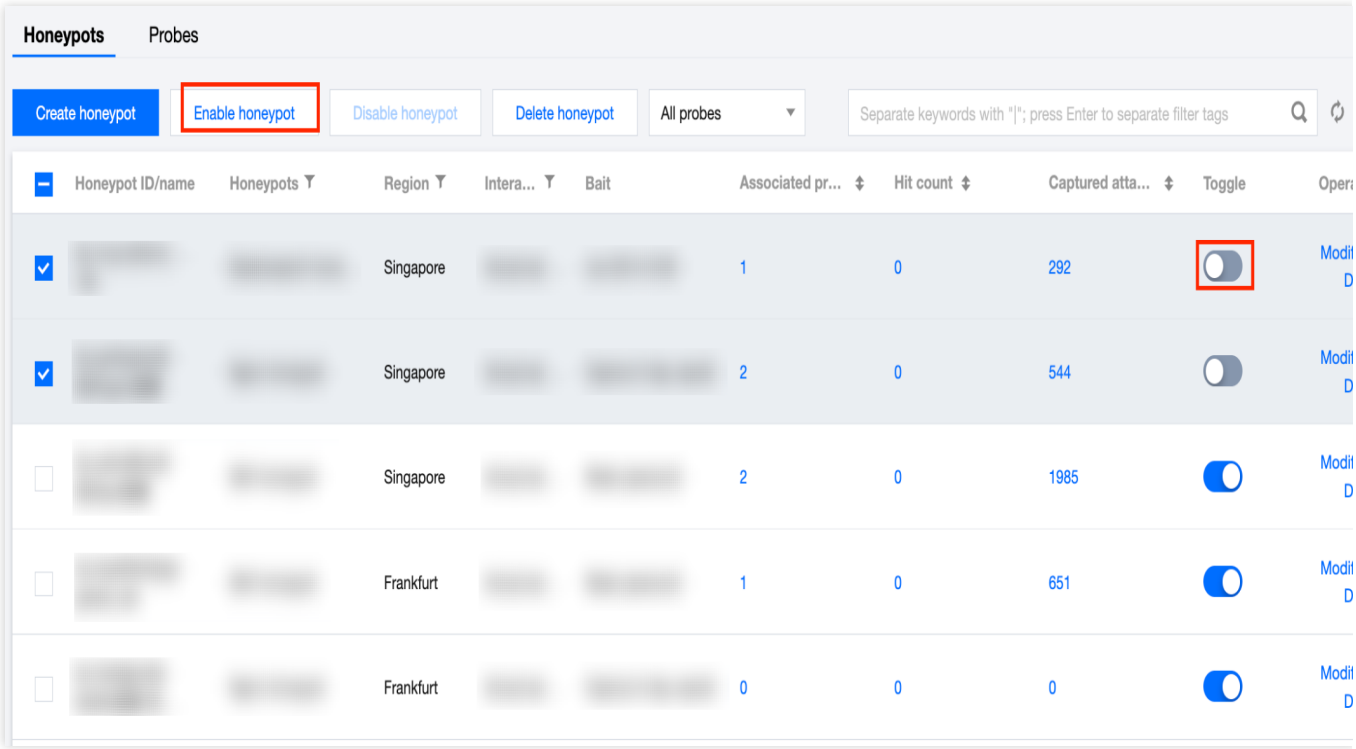
Region: All regions in China are available. The region cannot be modified after the instance is created.

Instance name: Custom instance name.

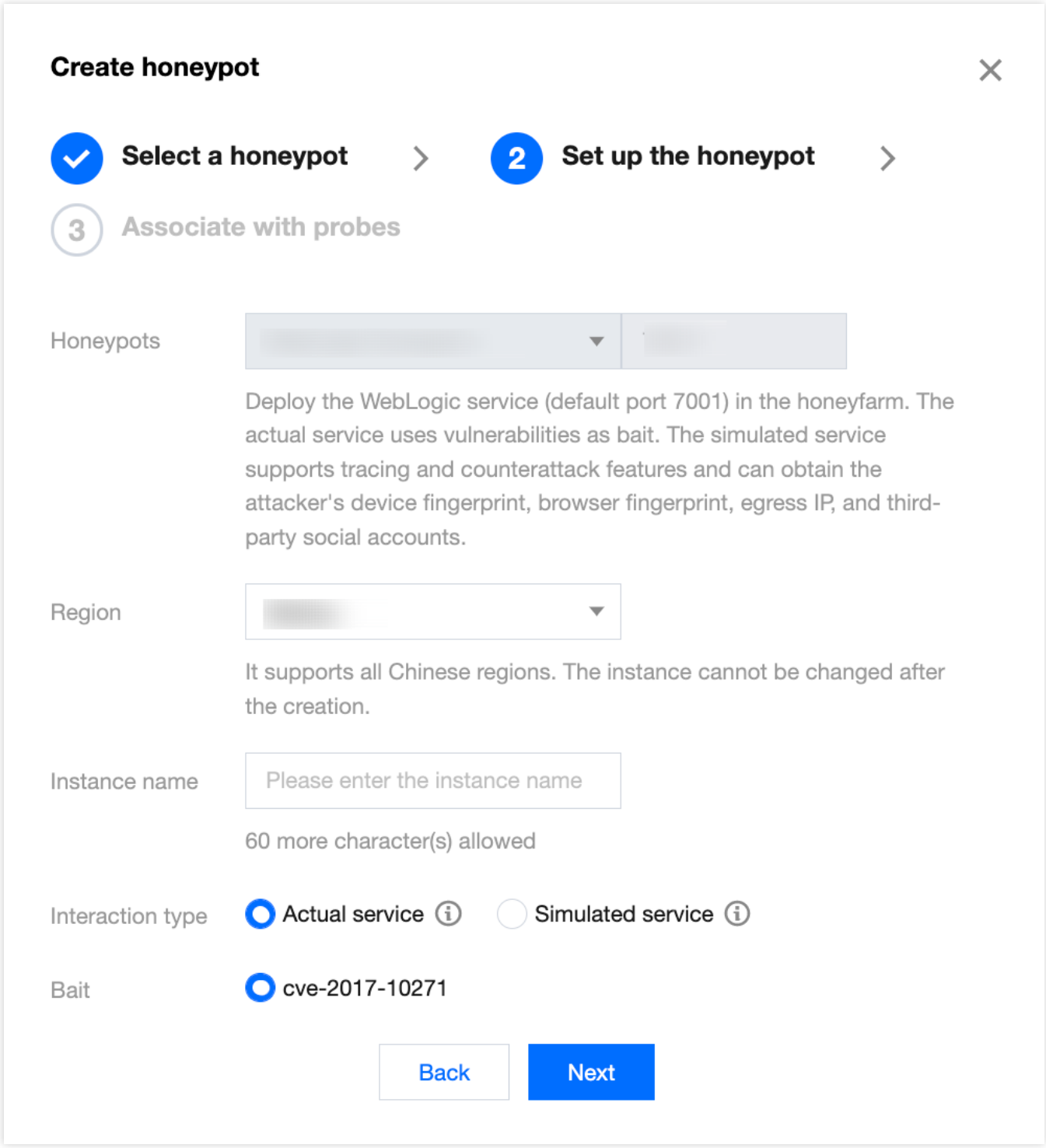
Honeypot service: Honeypots include ELASTICSEARCH, MYSQL, NGINX, SALTSTACK, SSH, STRUSTS, WEBLOGIC, and WEB honeypots. Except for the WEB honeypot, all the other honeypots have built-in baits and vulnerabilities.

Interaction type

Real service: High interaction. Real services and baits run on the backend, which actually respond to every request of attackers to deceive attackers, allowing you time to deploy protection measures.
Fake service: Medium interaction. Fake services and baits run on the backend, which generate simulated responses to some requests of attackers and induce attackers to continue their operations, allowing you time to deploy protection measures.
Bait
ELASTICSEARCH honeypot: cve-2014-3120.
SALTSTACK honeypot: cve-2020-11651.
SSH honeypot: weak token.
STRUSTS honeypot: cve-2017-12611.
WEBLOGIC honeypot: cve-2017-10271.
Other honeypots: none.
Custom bait
MYSQL honeypot, SSH honeypot: You can select a login token and set a password.
WEB honeypot: You can select an existing SSH or MySQL honeypot as a custom bait. If you have no SSH or MySQL honeypot, create one and associate it with a probe.
Other honeypots: none.
Associated probe: You can add an existing probe or create one.
Add existing: Click **Add existing**, and then select the required probe instance and port number.



Create: Click **Create**, configure the parameters, and click **OK** to add the probe to the **Create honeypot service** window.



Managing honeypots

Filtering/Sorting

On the **Network honeypots** page, click the search box to filter honeypot service events by keywords such as **Honeypot ID** or **Honeypot name**.

Click **Honeypots**, **Region**, or **Interaction type** in the header of the honeypot list to filter honeypot service events.

Click **Associated probes** or **Hit count** in the header of the honeypot list to sort honeypot service events in ascending or descending order.

Enabling honeypots

1.1 On the **Network honeypots** page, you can enable honeypots individually or in batch as follows.

Select a honeypot ID and click

or **Enable honeypot**.

Select multiple honeypot IDs and click **Enable honeypot**.

1.2 In the confirmation window displayed, click **OK** to enable the honeypot(s).

Note

When a honeypot is enabled, the traffic of associated probes will be forwarded to it.

Disabling honeypots

1.1 On the **Network honeypots** page, you can disable honeypots individually or in batch as follows.

Select a honeypot ID and click

or **Disable honeypot**.

Select multiple honeypot IDs and click **Disable honeypot**.

1.2 In the confirmation window displayed, click **OK** to disable the honeypot(s).

Note

When a honeypot is disabled, the traffic of associated probes will not be forwarded to it.

Editing honeypots

1. On the **Network honeypots** page, select **Honeypots**, and then click **Edit**.

2. In the **Modify honeypot service** window displayed, modify the instance name and associated probes, and then click **OK** to save the modification.

Deleting honeypots

1. On the **Network honeypots** page, you can delete honeypots individually or in batch as follows.

Select a honeypot ID and click **Delete** or **Delete honeypot**.

Select multiple honeypot IDs and click **Delete honeypot**.

2. In the confirmation window displayed, click **OK** to delete the honeypot(s).

Note

After a honeypot is deleted, the virtual environment in which the service runs and related resources will be deleted, and traffic forwarding by associated probes will be automatically canceled. Please proceed with caution.

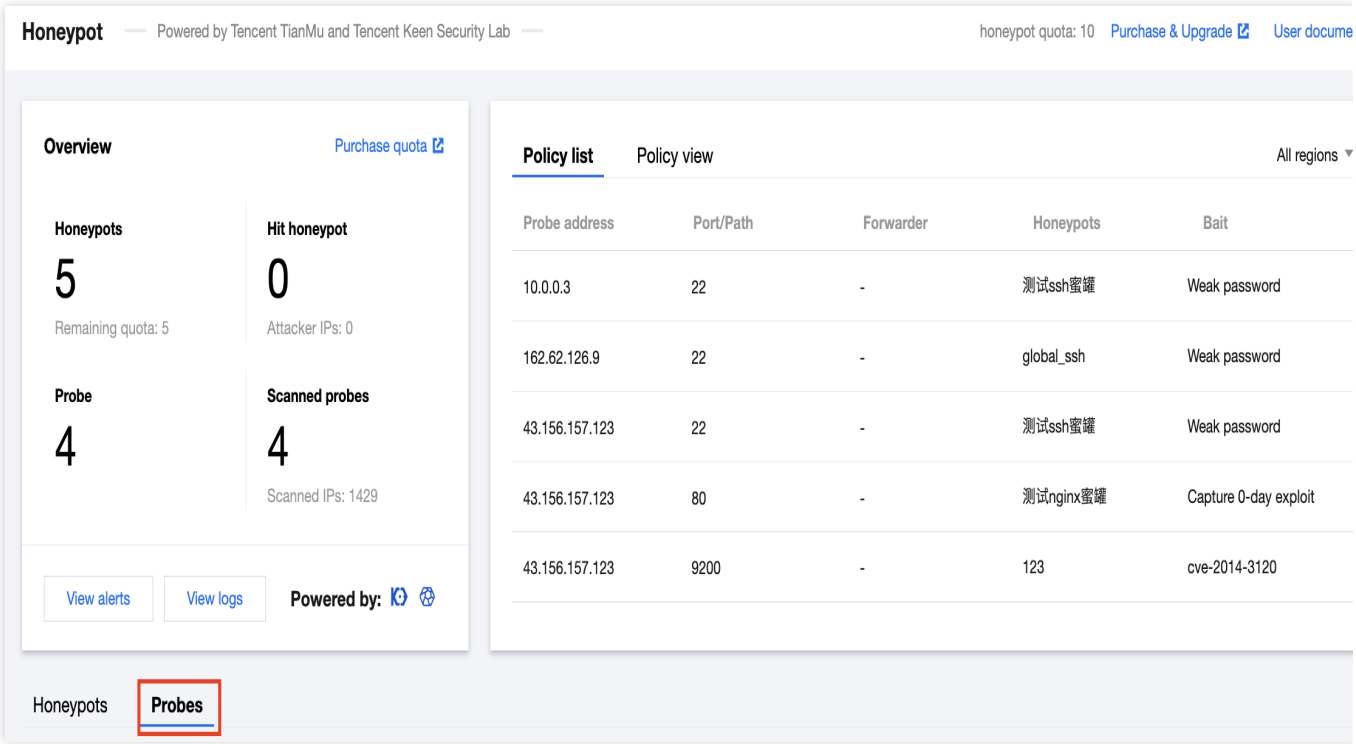
Probe

Last updated：2024-01-24 16:17:26

To use the network honeypot service, please associate probes first. You can create probes as follows.

Creating probes

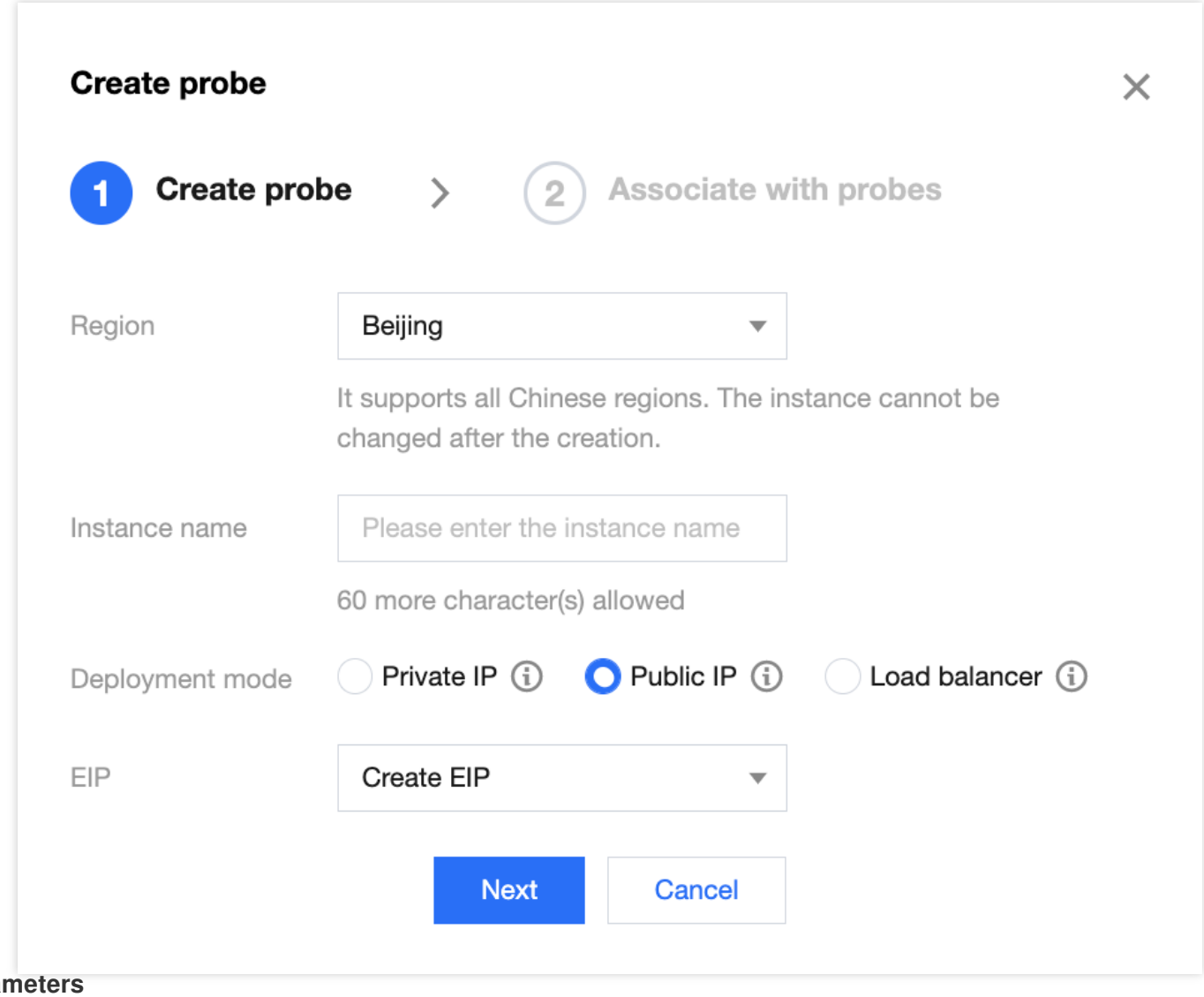
1. Log in to the Cloud Firewall console and click **Network Honeypots** in the left navigation pane.
2. On the **Network honeypot** page, click **Probes**.



3. On the **Probes** page, click **Create probe**.
4. In the **Create probe** window displayed, select a region, instance name, deployment mode, and honeypot service, and then click **OK**.

Note

Different deployment modes require different parameters. For more information, please see Parameters.



Parameters

Region: All regions in China are available. The region cannot be modified after the instance is created.

Instance name: Enter the name of the instance.

Deployment mode

Private IP: Select a subnet, and an ENI and private IP will be created. You can set the specified port of this IP to forward traffic to the honeypot service.

Public IP: Deploy a probe on an existing public IP to forward all traffic to the specified port of this IP to the honeypot service.

Load balancer: Deploy a probe on an existing CLB instance to forward all traffic of the path on the specified domain name to the honeypot service.

Select a subnet: This should be set when the deployment mode is private IP.

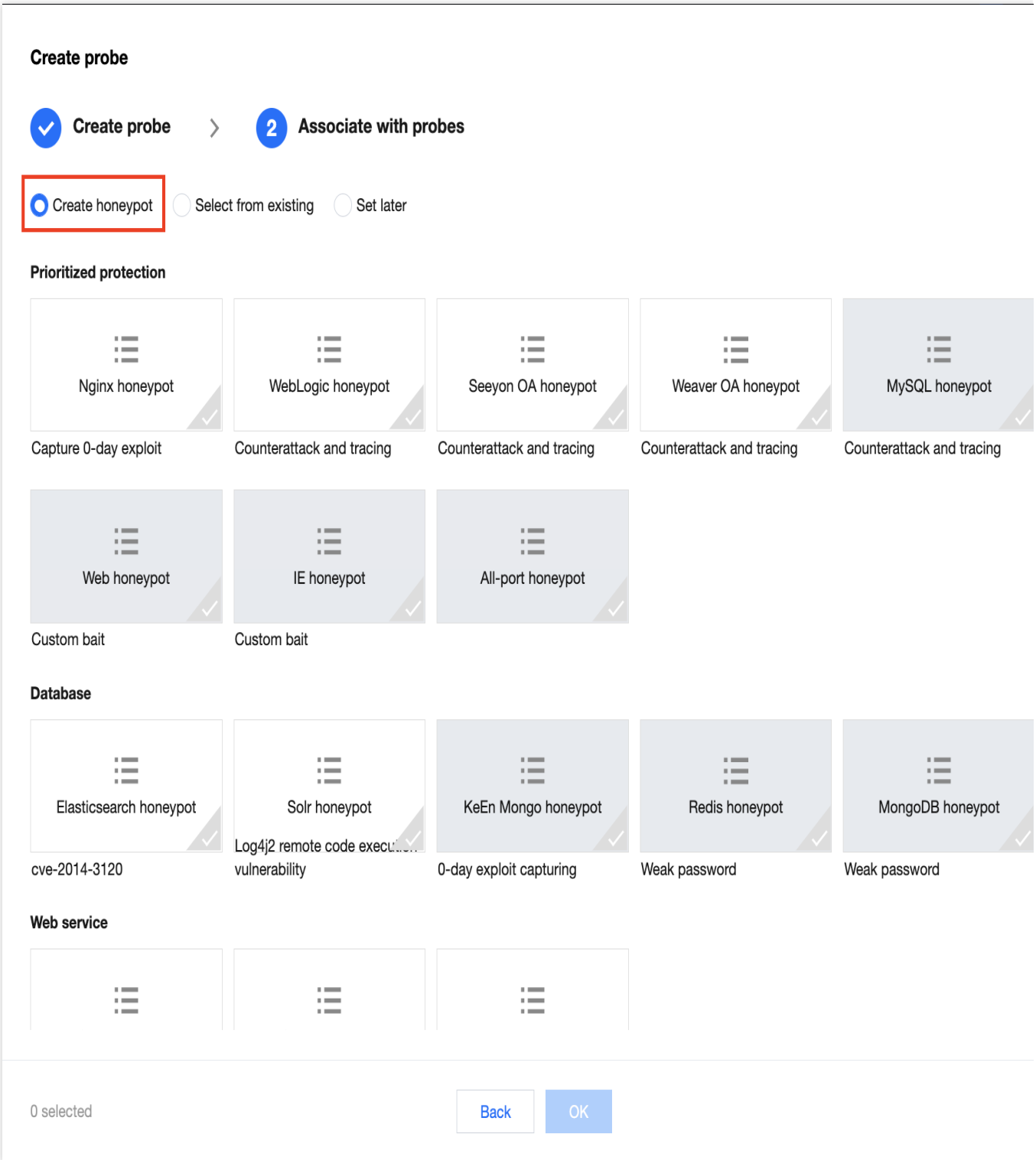
IP address: This should be set when the deployment mode is private IP.

Elastic IP: This should be set when the deployment mode is public IP. Select **Create EIP**.

Deployment instance: This should be set when the deployment mode is load balancer. Set this as needed.

Domain name: This should be set when the deployment mode is load balancer. Set this as needed.

Forwarder: This should be set when the deployment mode is load balancer. Select a CVM instance in the VPC of the current CLB instance as the backend service of the current listener. Only Linux CVMs are supported.
Honeypot service: Choose **Quick select** or **Advanced settings**.
Quick select: Click **Quick select** and select the desired honeypot service.
Note
As the web honeypot service needs to use an existing SSH/MySQL honeypot as bait, the web honeypot will not automatically associate bait after quick selection. If you click **Quick select** and select the web honeypot when creating a probe, the honeypot service will not be effective right away. You need to find the corresponding web honeypot editor and associate it with an SSH/MySQL honeypot, and then the web honeypot service will take effect.



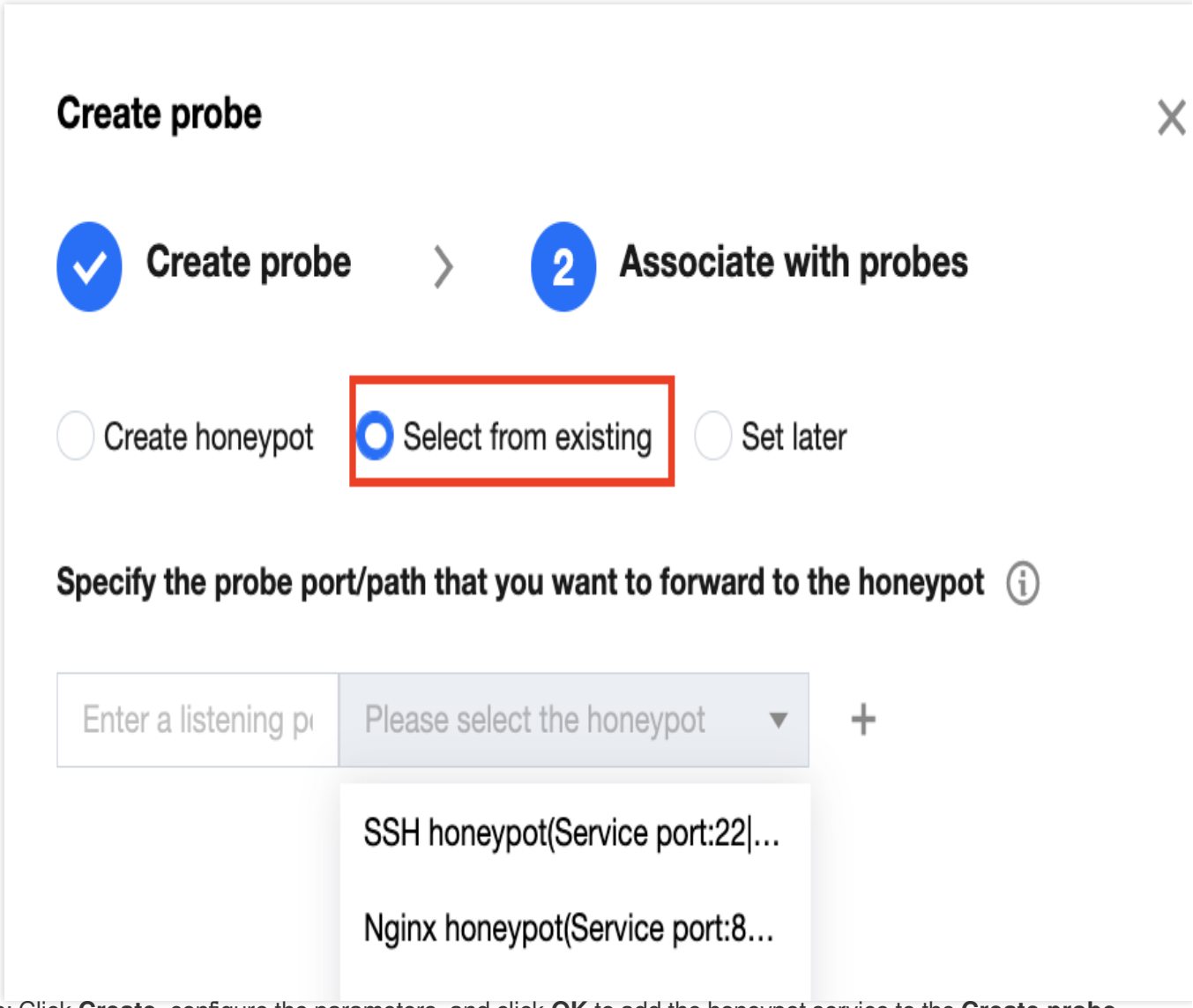
Advanced settings: You can add an existing honeypot or create one to associate.

Add existing: Click **Add existing**, select the desired honeypot, and modify the listening port or input path as required.

Note

When the deployment mode is public IP, you can modify the listening port.

When the deployment mode is load balancer, you can modify the input path.



Create: Click **Create**, configure the parameters, and click **OK** to add the honeypot service to the **Create probe** window.

Managing probes

Filtering/Sorting

On the **Probes** page, click the search box to filter probe events by keywords such as **probe ID** or **probe name**.

Click **Region**, **VPC**, **Deployment method**, **Deployment instance**, and **Forwarder** in the header of the probe list to filter probe events.

Click **Forward to honeypot** and **Hit count** in the header of the probe list to display probe events in ascending or descending order.

Enabling probes

1.1 On the **Probes** page, you can enable probes individually or batch enable probes as follows.

Select a probe ID and click


or **Enable probe**.

Select multiple probe IDs and click **Enable probe**.

1.2 In the confirmation window displayed, click **OK** to enable the probe(s).

Disabling probes

1.1 On the **Probes** page, you can disable probes individually or batch disable probes as follows.

Select a probe ID and click


or **Disable probe**.

Select multiple probe IDs and click **Disable probe**.

1.2 In the confirmation window displayed, click **OK** to disable the probe(s).

Modifying probes

1. Log in to the Cloud Firewall console and click **Network Honeypots** in the left navigation pane.
2. On the **Network honeypot** page, click **Probes**.
3. On the **Probes** page, select a probe event and click **Modify**.
4. In the **Modify probe** window displayed, modify the instance name and honeypot service type, and then click **OK** to save the modifications.

Deleting probes

1. Log in to the Cloud Firewall console and click **Network Honeypots** in the left navigation pane.
2. On the **Network honeypot** page, click **Probes**.
1. On the **Probes** page, you can delete probes individually or batch delete probes.

Select a probe ID and click **Delete** or **Delete probe**.

Select multiple probe IDs and click **Delete probe**.

2. In the confirmation window displayed, click **OK** to delete the probe(s).

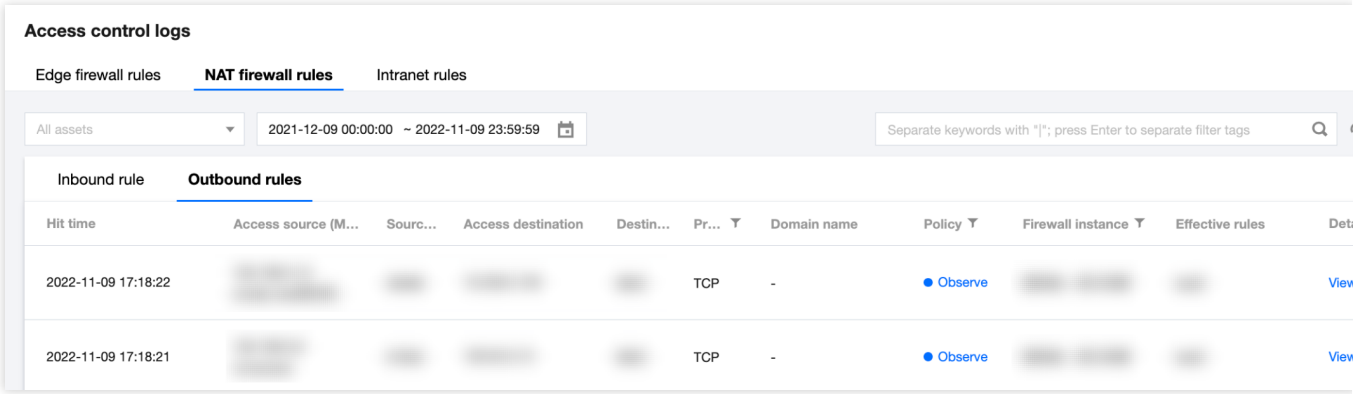
Log Audit

Last updated：2024-01-24 16:17:26

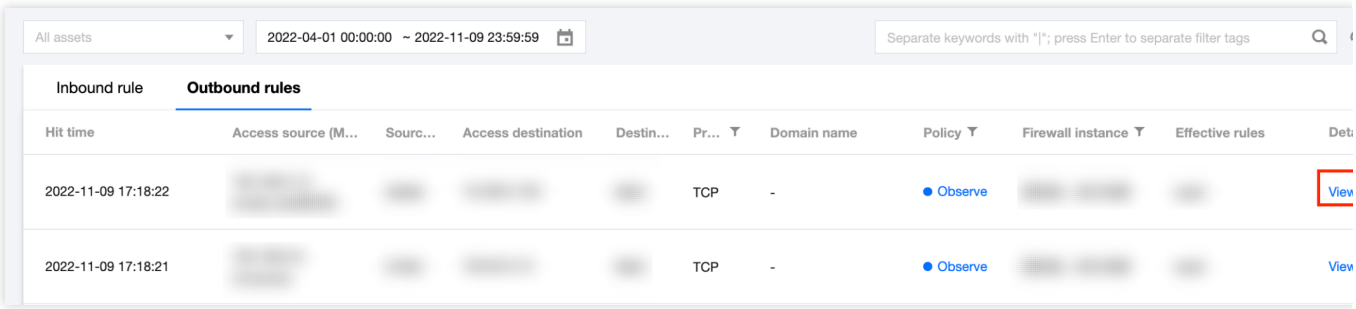
This topic describes how to view Cloud Firewall logs.

Viewing access control logs

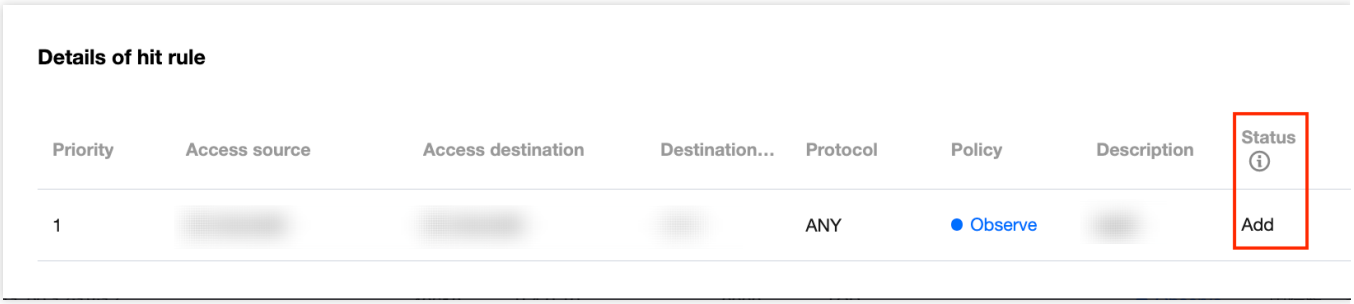
1. Log in to the Cloud Firewall console and select **Log Auditing** -> **Access Control Logs** in the left navigation pane.
2. On the **Access control logs** page, you can view the rule hit logs generated by Cloud Firewall based on the configured access control rules for edge firewalls, NAT firewalls, inter-VPC firewalls, and enterprise security groups. On the **Edge firewall** and **NAT firewall** pages, you can view two hit lists for inbound rules and outbound rules.



3. Click **View** in the action column on the right side of the rule hit list.



4. On the **Details of hit rule** page, you can view the hit details of the rule.



Note

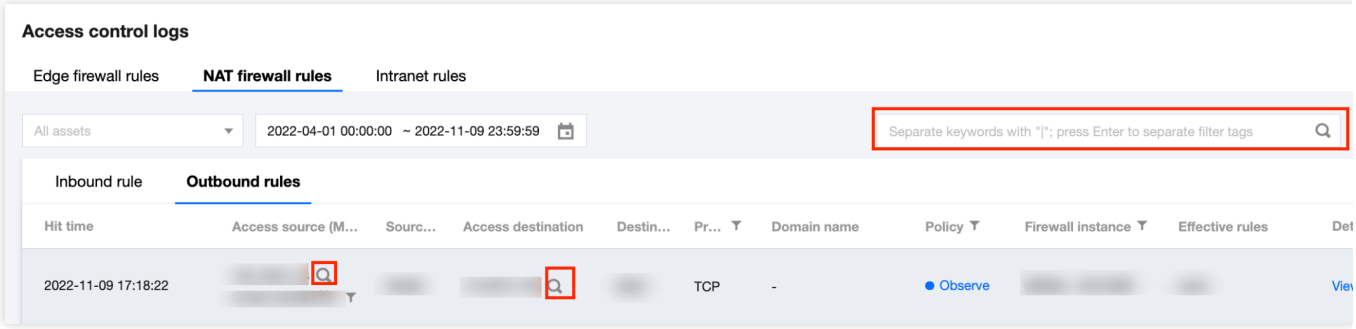
If the rule is deleted after generation of the log, the status is **Deleted**.

If the rule is modified after generation of the log, the status is **Modified**.

If the rule is not modified or deleted after generation of the log, the status is **New**.

5. To retrieve and filter access control logs more quickly, you can click

on the right of an access source or access destination to view all rule hits from or to an IP address.

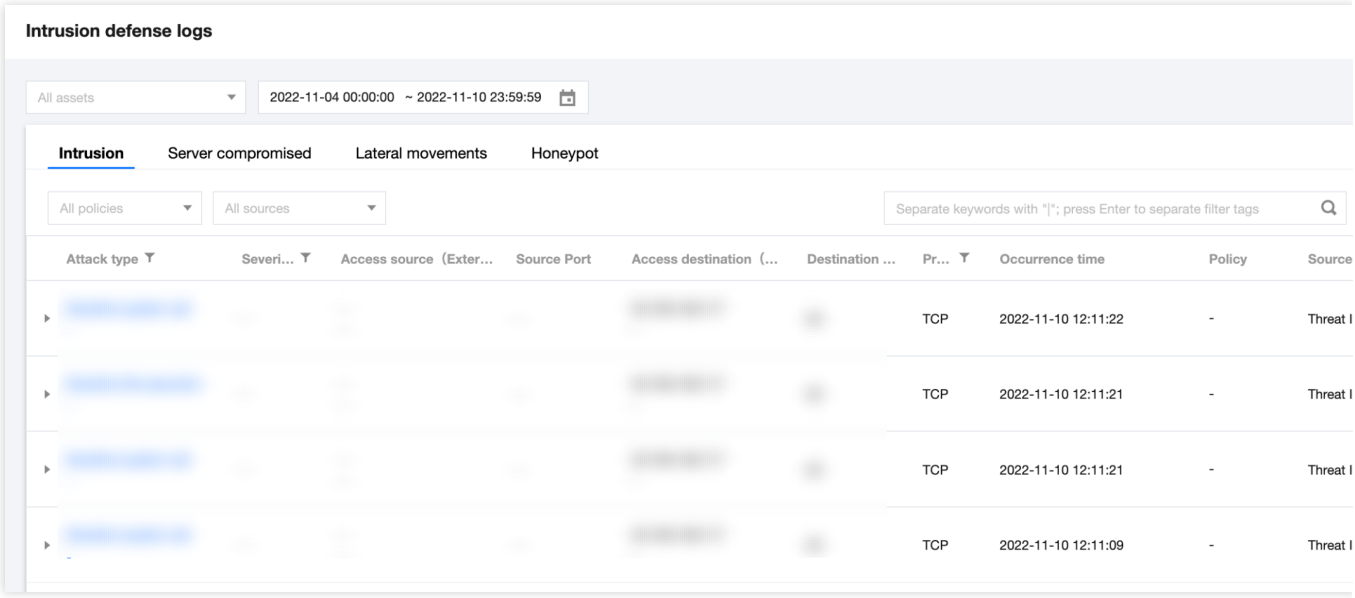


6. Click

on the right side of the page to download the logs. You can also set filters, and download up to 60,000 records each time.

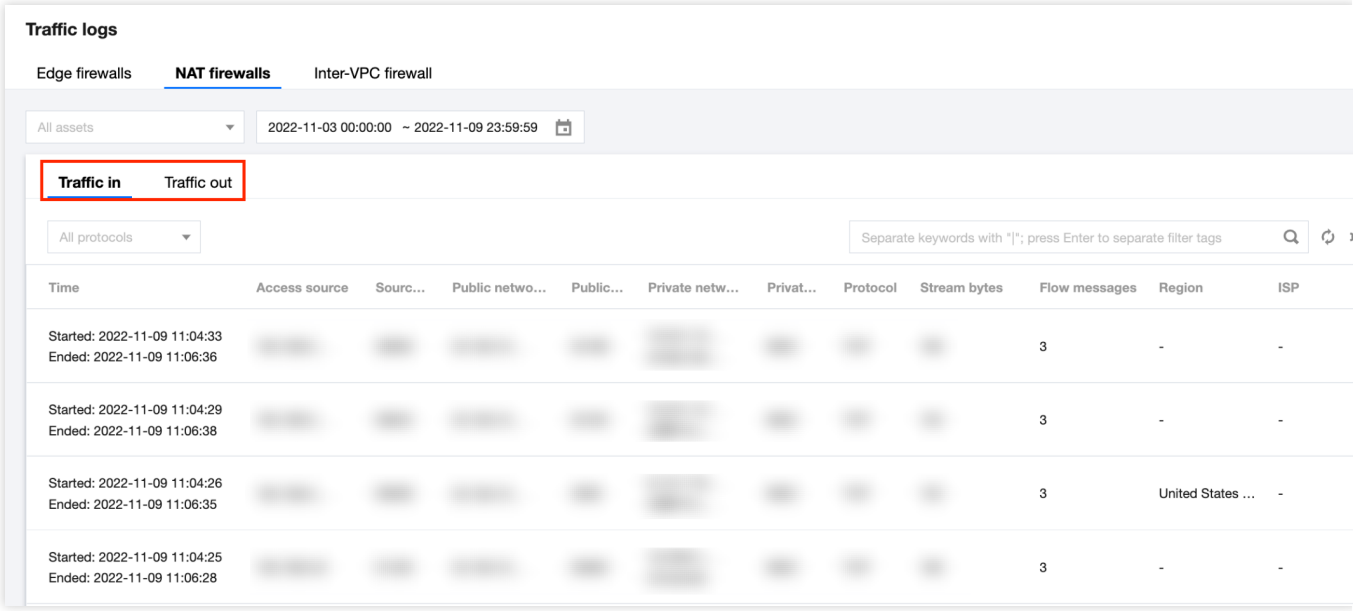
Viewing intrusion defense logs

1. Log in to the Cloud Firewall console and select **Log Auditing** -> **Intrusion Defense Logs** in the left navigation pane.
2. On the **Intrusion defense logs** page, you can view all the security events generated and recorded by Cloud Firewall in the **Observe** and **Block** modes. There are four lists for intrusions, compromised servers, lateral movements, and network honeypots, and you can view details of inbound and outbound security events.

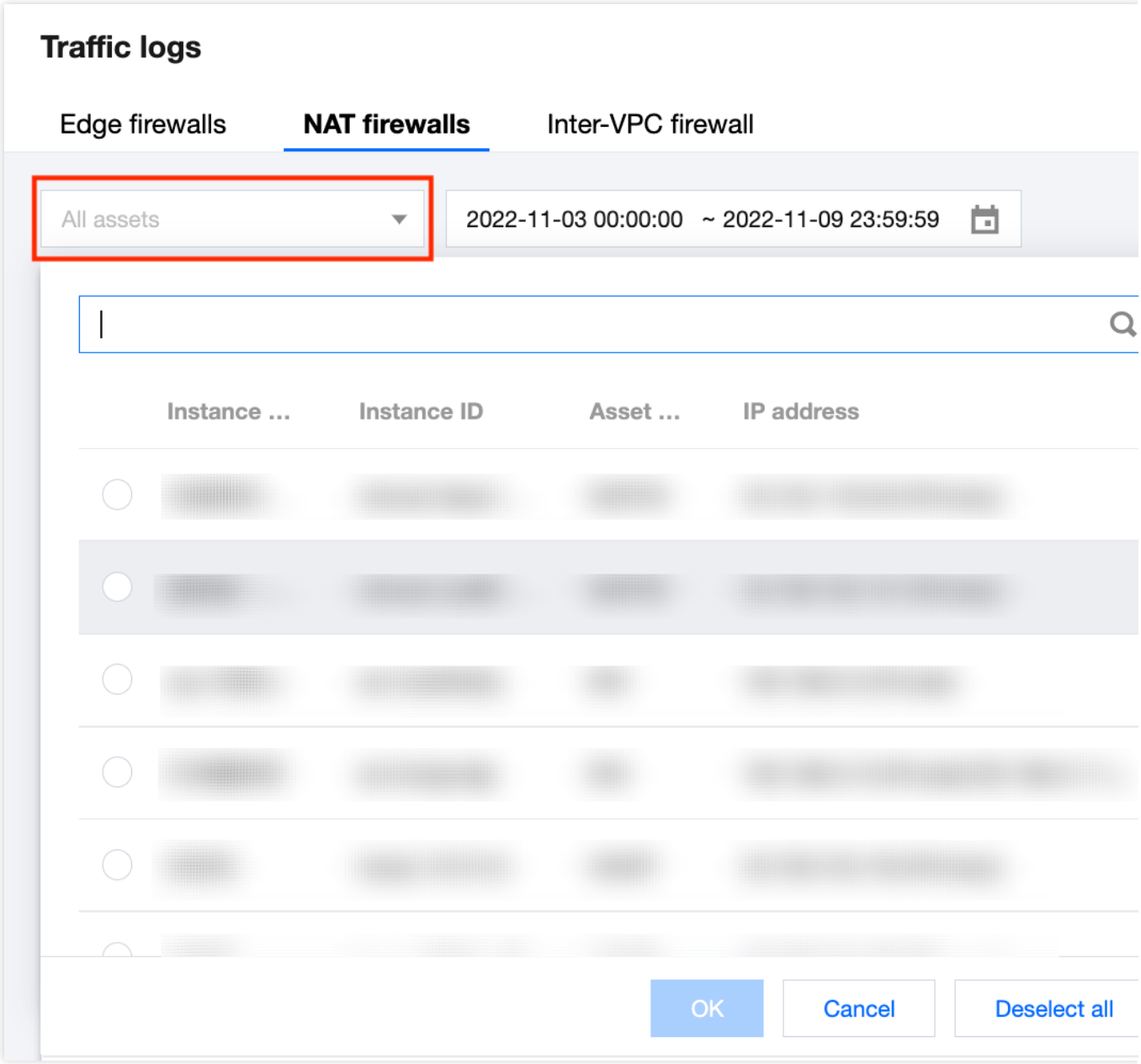


Viewing traffic logs

1. Log in to the Cloud Firewall console and select **Log Auditing** -> **Traffic Logs** in the left navigation pane.
2. On the **Traffic logs** page, you can view the 10-tuple information of north-south traffic generated by edge firewalls and NAT firewalls based on outbound and inbound traffic, as well as east-west traffic between VPCs.

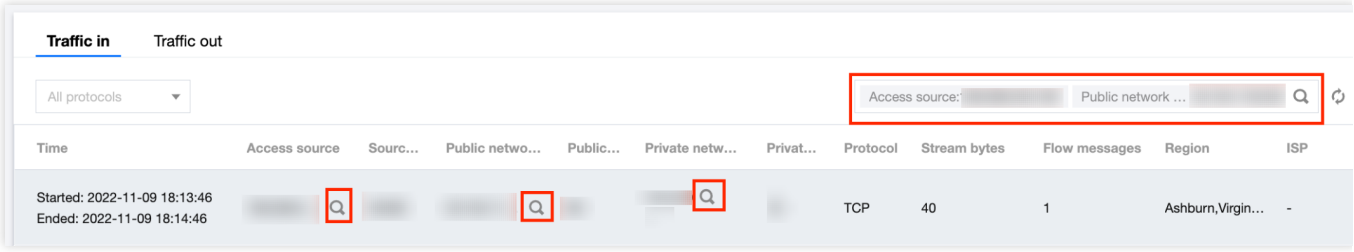


3. Query and filter logs by asset instance name. You can click **All assets** in the upper left corner, and select an asset instance name in the drop-down list to filter the logs and query all traffic logs of the asset.



4. To retrieve and filter logs more quickly, you can click

on the right of an access source or access destination to view all traffic from or to an IP address.

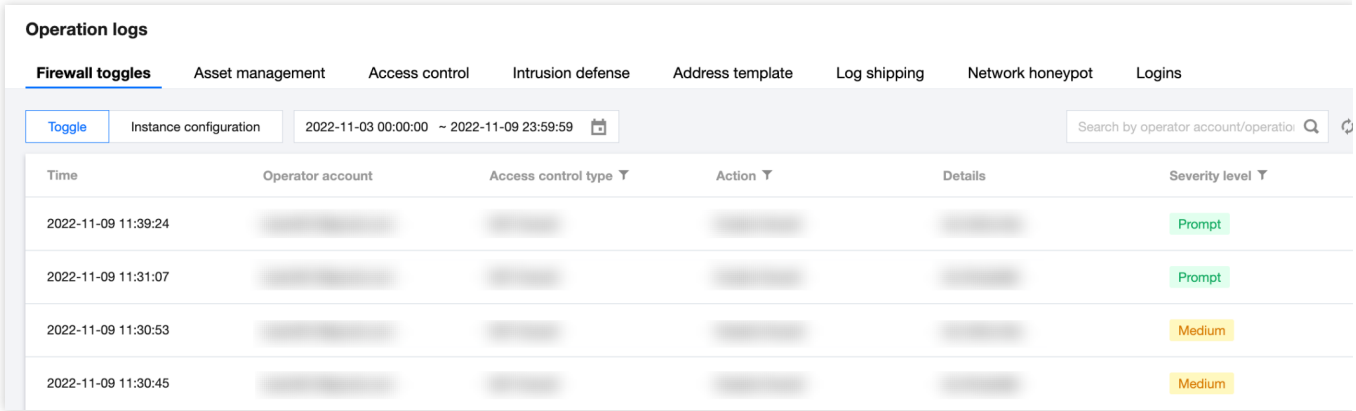


Authorizing private network traffic logs

1. Log in to the Cloud Access Management console, and select **Roles** in the left navigation pane.
2. On the **Roles** page, click **Create Role**, select your Tencent Cloud account, and enter the role creation page.
3. On the page, select **Other root account**, enter the traffic log public account **91000000202**, and click **Next**.
4. Search for the keyword **log service**, authorize full read/write permissions for the log service **QcloudCLSFullAccess**, and click **Next**.
5. Enter the role name **FlowLogClsRole**, and click **Complete** to create the role.

Viewing operation logs

1. Log in to the Cloud Firewall console and select **Log Auditing** -> **Operation Logs** in the left navigation pane.
2. On the **Operation logs** page, you can view all actions performed on the **Security Policies** and **Toggles** pages of the account and their details.



Tabs:

Firewall toggles: Records firewall toggle operations.

Instance configuration: Records the configuration details of instances.

Access control: Records add, modify, and delete operations on access control rules.

Intrusion defense: Records the operation details of intrusion defense modules.

Security baseline: Records security baseline operations.

Address templates: Records the operation details of address templates.

Enterprise security groups: Records the operations on enterprise security groups.

Log shipping: Records the details of log shipping operations.

Logins: Records the login status of all accounts of the user.

More information

For questions about log auditing, please see Log.

Log Analysis

Last updated：2024-01-24 16:17:26

Log Analysis allows you to view details of all traffic logs of the login account stored in Cloud Firewall for the past 6 months, query logs with search statements, and use reporting and analysis services. This topic describes how to use Log Analysis.

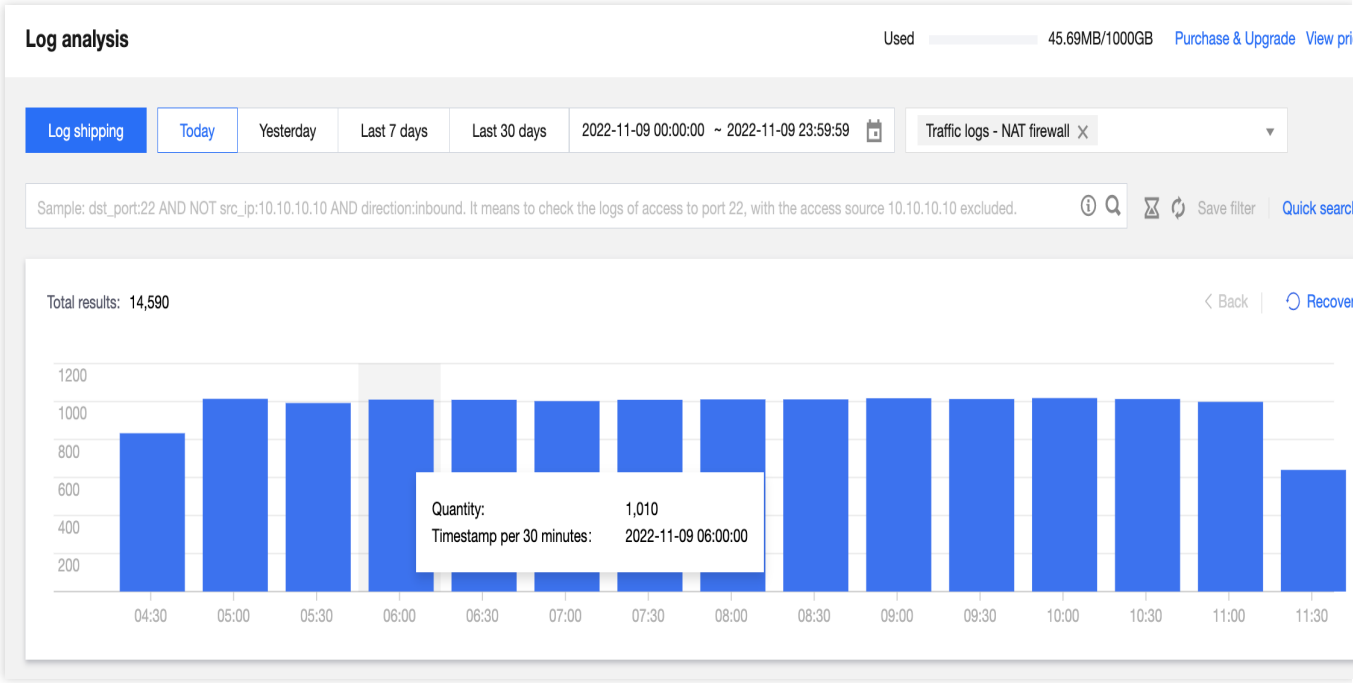
Viewing log analysis data

1. Log in to the Cloud Firewall console and click **Log Analysis** in the left navigation pane.
2. Drag your mouse on the bar chart in blue to quickly select a time range to search and click a bar to check the logs.

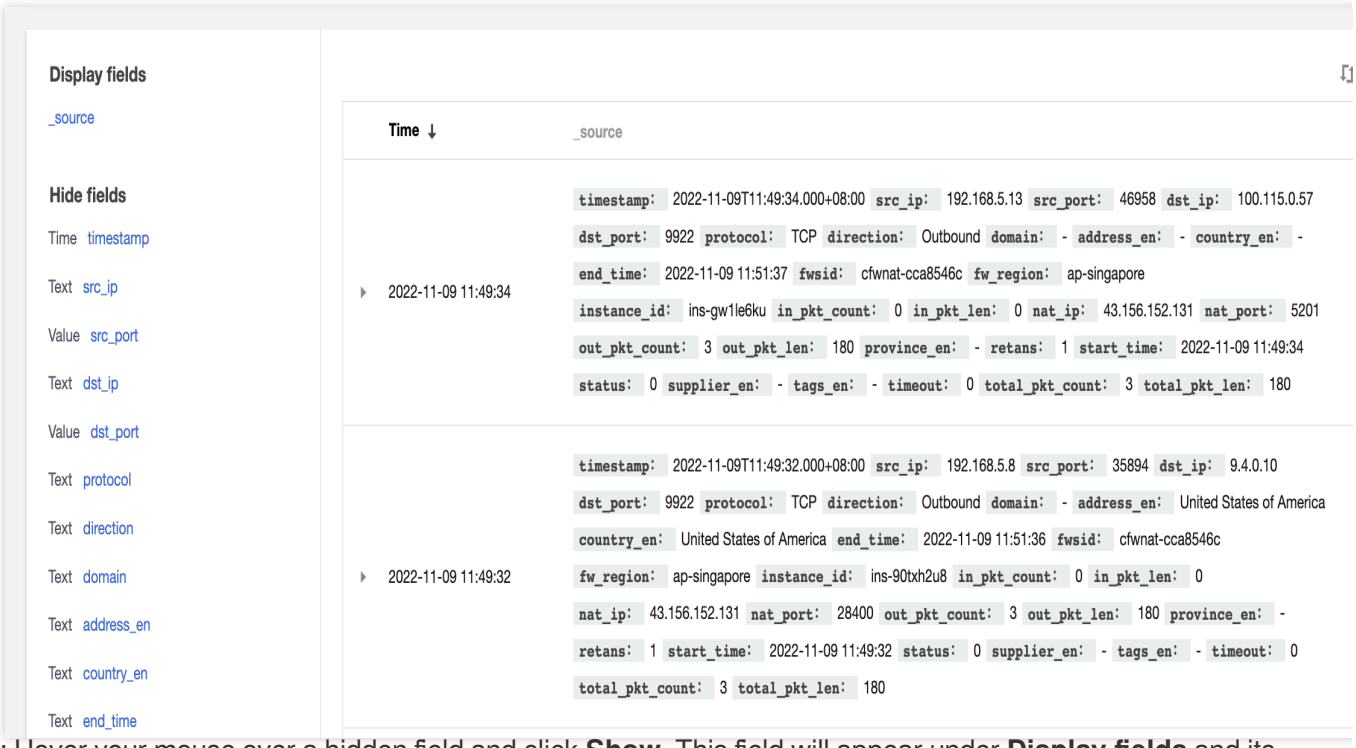
Note

Cancel: Click **Cancel** in the upper right corner of the bar chart and the bar chart will show the number of logs for today by default.

If you change the time and log type or enter new keywords to search again, the bar chart will show the number of logs for today by default.

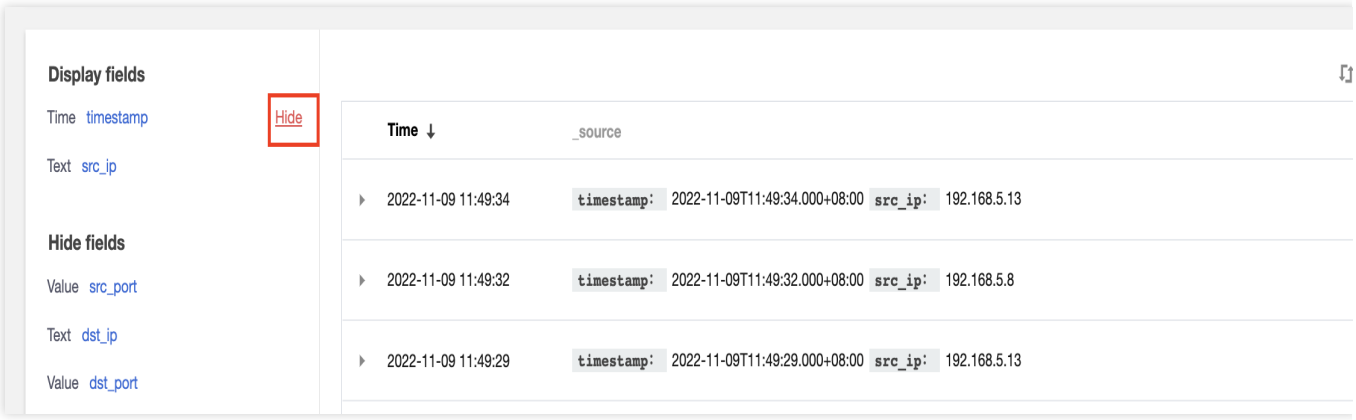


3. The log list displays the field details of each traffic log in the order the fields appear in **Display fields**. When the **Display fields** module only contains **source**, the list displays the field details of each traffic log in the order the fields appear in **Hide fields**.



Show: Hover your mouse over a hidden field and click **Show**. This field will appear under **Display fields** and its details will be displayed in the log list on the right.

Hide: Hover your mouse over a displayed field and click **Hide**. This field will be deleted from **Display fields**and its details will not be displayed in the log list on the right.



Log shipping

You can use log shipping to automatically ship Cloud Firewall logs to specified Cloud Kafka (CKafka) instances. This section describes how to use the log shipping feature of Log Analysis.

Background

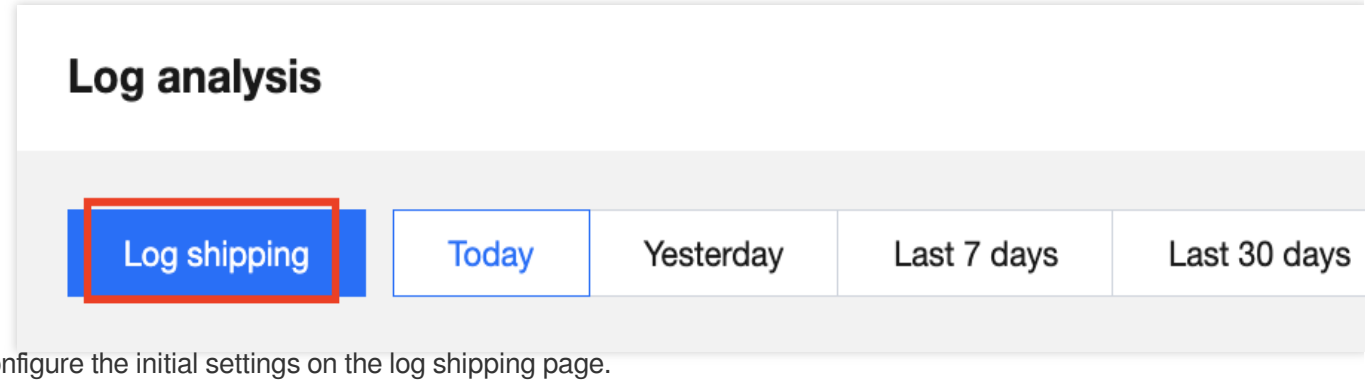
You can ship logs to specified CKafka topics based on Cloud Firewall log types.
Log shipping supports two network access methods: public domain name and supported environment.
For access via public domain name, logs are shipped through the public network.
For access via supported environment, logs are shipped through Tencent Cloud private network, which effectively enhances the performance.

Prerequisites

You need to purchase Cloud Kafka instances first, and set the bandwidth of the CKafka instance based on the Cloud Firewall bandwidth.
Please see Cloud Kafka for more information, and contact us to enable the allowlist for "access via public domain name" or "access via supported environment".
You can only use one CKafka account for log shipping.

Configurations

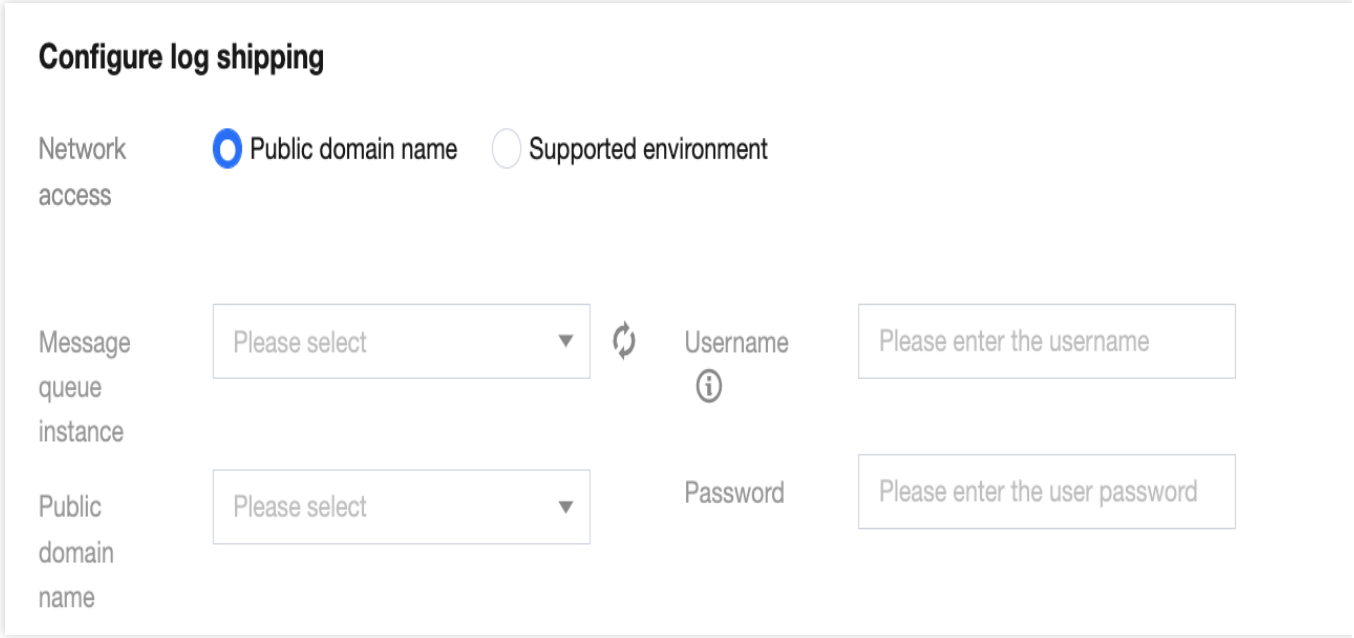
1. Log in to the Cloud Firewall console and click **Log Analysis** in the left navigation pane.
2. Click **Log shipping** in the upper left corner.



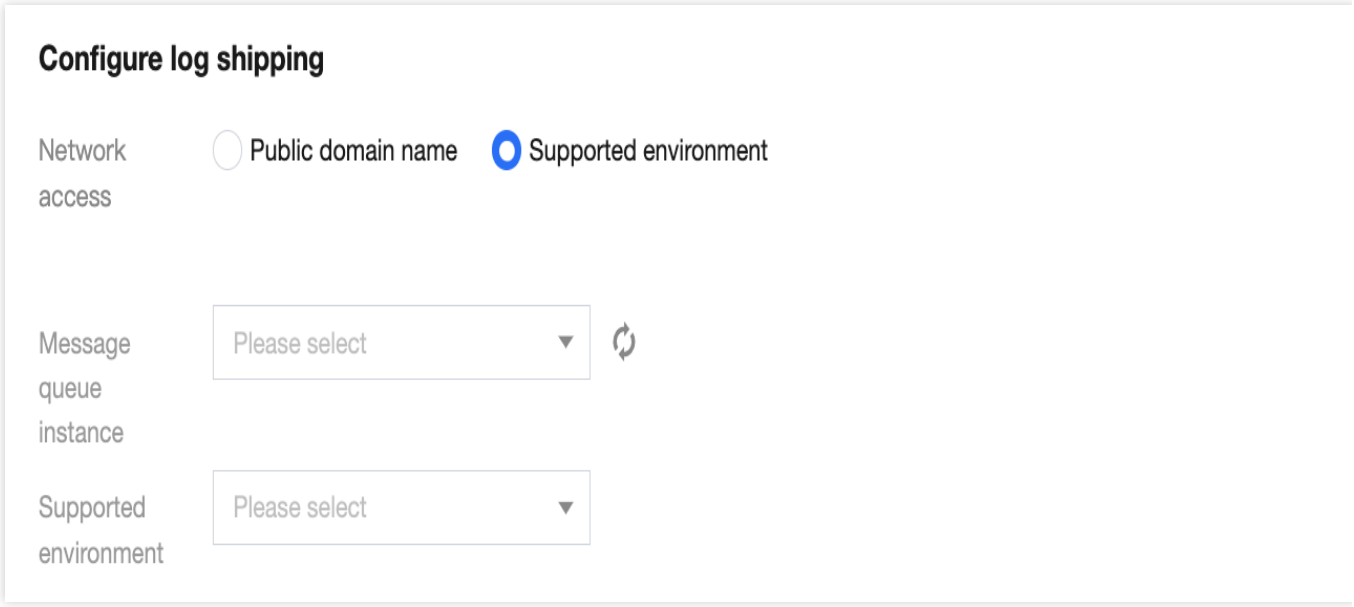
3. Configure the initial settings on the log shipping page.

3.1 Select the network access method: public domain name or supported environment.

Method 1: Select **Public domain name** and then select the message queue instance and public domain name. Enter the user name and password of the selected instance.



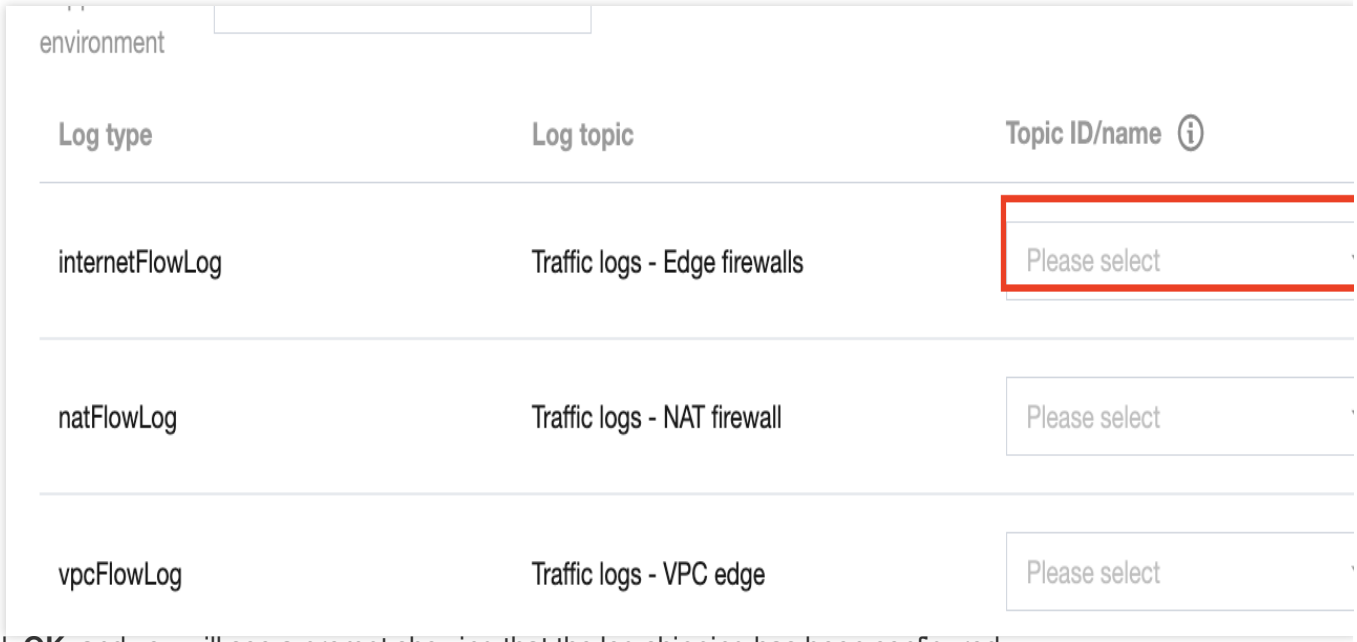
Method 2: Select **Supported environment** (Tencent Cloud products that you purchased and can be used with CKafka), and then select the message queue instance and IP port.



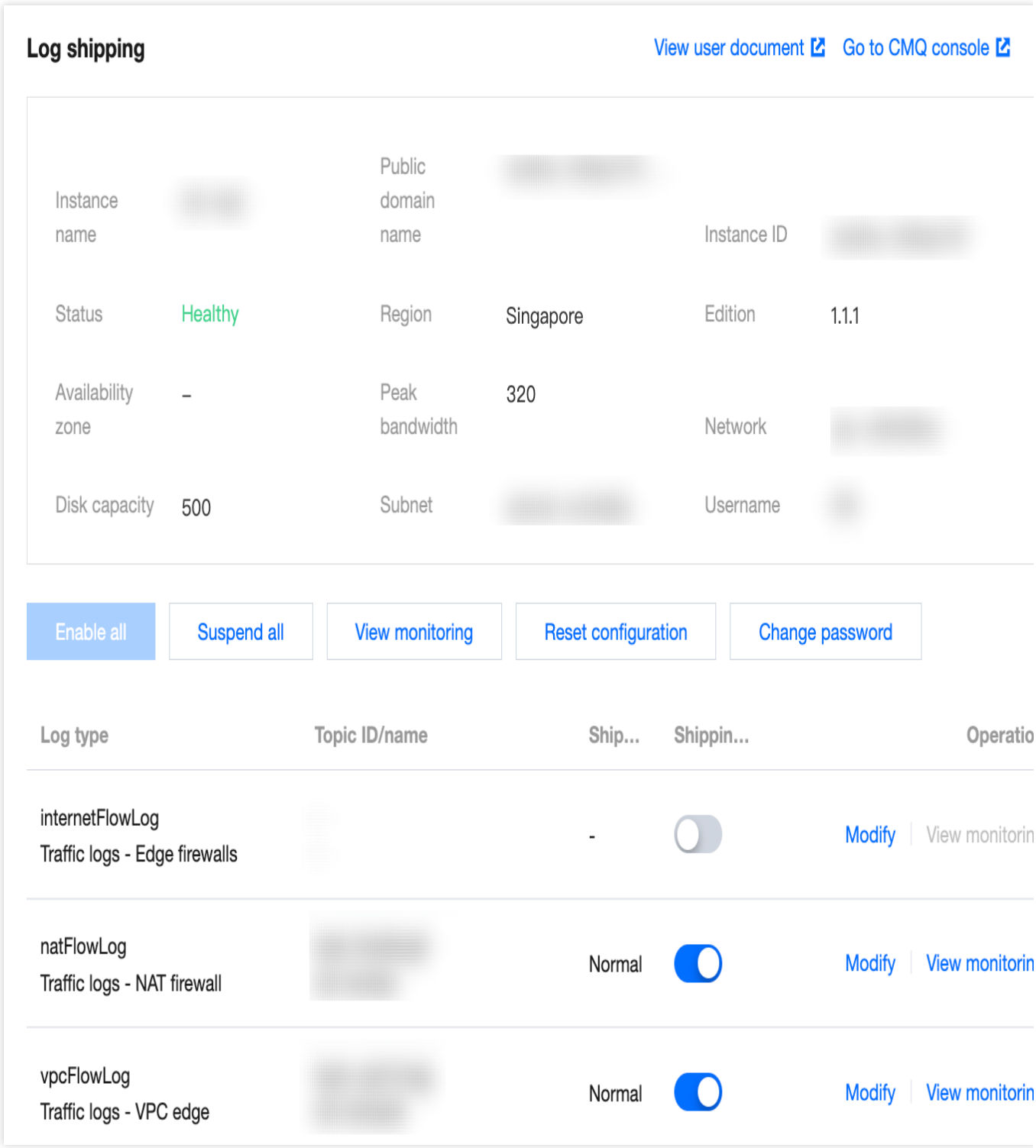
3.2 Associate a CKafka topic on the log shipping page.

Note

You can ship multiple types of Cloud Firewall logs to their specified CKafka topics. One CKafka topic can only be associated with one Cloud Firewall log type.



4. Click **OK**, and you will see a prompt showing that the log shipping has been configured.
5. After configuration, you can view the log shipping details.



Basic info: shows the basic information of CKafka instances.

Note

When you see **Unhealthy** in the **Status** field, click **View monitoring** to check whether CKafka is abnormal or whether the quota is insufficient.

Shipping status: Toggles the log shipping on/off to control a specified log type.

Method 1: Toggle on or off under **Shipping status** on the right side of each log type.

Method 2: Disable/enable in batch. You can select **Enable all** or **Disable all**.

Change CKafka topic: In the action column on the right side of a log type, click **Edit** to configure it individually. You can select a CKafka topic not associated with other Cloud Firewall log types in the specified CKafka instance.

Note

One CKafka topic can only be associated with one Cloud Firewall log type.

View monitoring: In the action column on the right side of a log type, click **View monitoring** to go to the monitoring page of the CKafka console, where you can view network traffic, peak bandwidth, message quantity, disk usage, etc.

Change configuration: Click **Change configuration** above the log type list, and then select the message queue instance to ship, network access method, and user name/password.

Note

This will interrupt the current shipping process.

Change password: click **Change password** above the log type list to modify the user name and password of CKafka.

Log Fields
Log Subfield

Last updated：2024-09-06 17:46:24

Log Type ID	Log Type Name
CFWRuleAcl	Access control logs - Edge Firewall
CFWRuleVpcAcl	Access control logs - NAT Firewall and Inter-VPC Firewall
HoneyPotHost	Intrusion defense logs - honeypot - host logs
HoneyPotNetwork	Intrusion defense logs - honeypot - network logs
BlockList	Intrusion defense logs - interception list logs
IdsLog	Intrusion defense logs - virtual patches and basic defense logs
TiLog	Intrusion defense logs - threat intelligence logs
BaseLineLog	Intrusion defense logs - security baseline logs
CFWOnline	Traffic logs - Edge Firewall
CFWNetflowVpc	Traffic logs - VPC
CFWNetflowNat	Traffic logs - NAT
CFWNetflowFl	Traffic logs - private network traffic
CFWOperateLogAll	Operation logs

Access Control Logs

Last updated：2024-09-06 17:47:53

Field Identifier	Field Type	Field Name	Field Description	Reference Values	Specific Types
src_ip	string	Source IP	-	192.168.0.1	CFWRuleAcl,CFWRuleVpcAc
dst_ip	string	Destination IP	-	192.168.0.1	CFWRuleAcl,CFWRuleVpcAc
src_port	uint16	Source port	-	22	CFWRuleAcl,CFWRuleVpcAc
dst_port	uint16	Destination port	-	22	CFWRuleAcl,CFWRuleVpcAc
protocol	string	Protocol	-	tcp	CFWRuleAcl,CFWRuleVpcAc
info	string	URL information	URL of HTTP hit log	domain/testphp	CFWRuleAcl
direction	int8	Direction	Specify the traffic direction of a rule	Outbound	CFWRuleAcl,CFWRuleVpcAc
detail	string	Rule alarm description (including rule description)	Alarm details information	-	CFWRuleAcl,CFWRuleVpcAc
rule_info	string	Rule alarm details (for associating with rules)	-	-	CFWRuleAcl
strategy	string	Policies	Action policy for rule execution		CFWRuleAcl,CFWRuleVpcAc
time	int64	Events	Time of rule hit	-	CFWRuleAcl,CFWRuleVpcAc

appid	string	appid	Account appid	-	CFWRuleAcl
instance_id	string	Victim-related asset ID	Victim-related asset ID	-	CFWRuleAcl,CFWRuleVpcAc
uuid	string	Unique ID of the original alarm log	Unique ID of the original alarm log	-	CFWRuleAcl
uid	int64	Unique ID of the rule	Unique ID of the rule (for internal use)	-	CFWRuleAcl
insert_time	int64	Log insertion time	Time of recording this log	-	CFWRuleAcl,CFWRuleVpcAc
mode	uint8	Firewall attributes	0: bypass 1: serial	-	CFWRuleAcl
type	uint8	Protocol TYPE	Protocol TYPE: 1: TCP 3: HTTP	-	CFWRuleAcl
fw_type	string	Firewall type	Firewall type to which the rule belongs	NAT Firewall	CFWRuleAcl,CFWRuleVpcAc
timestamp	string	Timestamp	Current time	-	CFWRuleAcl,CFWRuleVpcAc
fws_id	string	Engine instance ID		cfwnat-fd7f678e	CFWRuleVpcAcl
nat_ins_name	string	NAT instance name	-	-	CFWRuleVpcAcl
log_type	uint8	Log type (for internal	Current log type fixed	-	CFWRuleVpcAcl

		use)	value: 5		
dst_vpc	string	Victim assets VPCID	-	-	CFWRuleVpcAcl
fws_name	string	Engine instance name	-	-	CFWRuleVpcAcl
src_vpc	string	Attacker assets VPCID	-	-	CFWRuleVpcAcl
region	string	Region	-	-	CFWRuleVpcAcl
dst_domain	string	External domain name	External domain name information	-	CFWRuleVpcAcl
l7proto	string	Seven-Layer protocol name	-	DNS,SMTP,HTTP	CFWRuleVpcAcl
src_vpc_name	string	Access source VPC name	-	-	CFWRuleVpcAcl

dst_vpc_name	string	Access destination VPC name	-	-	CFWRuleVpcAcl
ew_ins_id	string	VPC wall instance ID	-	-	CFWRuleVpcAcl
ew_ins_name	string	VPC wall instance name	-	-	CFWRuleVpcAcl
src_ins_id	string	Access source asset ID	-	-	CFWRuleVpcAcl
dst_ins_id	string	Access destination asset ID	-	-	CFWRuleVpcAcl

src_ins_name	string	Access source instance name	-	-	CFWRuleVpcAcl
dst_ins_name	string	Access destination instance name	-	-	CFWRuleVpcAcl

Intrusion Defense Logs

Last updated：2024-09-06 17:49:46

Field Identifier	Field Type	Field Name	Field Description	Reference Values
instance_id	string	Victim-related asset ID	-	-
time	int64	Alarm occurrence time	-	-
src_ip	string	Source IP	-	192.168.0.1
dst_ip	string	Destination IP	-	192.168.0.1
src_port	int64/int	Source port	-	-
dst_port	int64/int	Destination port	-	-
direction	int64	Direction	0: outbound 1: inbound	-

			TCP protocol alarm: session direction Session protocol: traffic direction	
protocol	string	Protocol	-	TCP
strategy	string	Alarm action	Handling action for alarms 0: observe 1: block 2: allow 3: deceive	0
strategy_res	string	Alarm action identification ID	-	strage_alert
event_name	string	Attack event type	-	Log4j2 vulnerability exploitation
eventname_res(event_name_res)	string	Attack event type identification ID	-	log4j2_exploit
dst_domain	string	External domain name	-	-
level	string	Alarm level	Alarm severity level	Critical
level_res	string	Alarm level	-	level_serious

		identification ID		
level_int	int	Alarm level number	-	5
address	string	City where the attack IP is located	-	Shenzhen, Guangdong Province, China
address_en	string	City where the attack IP is located	-	Shenzhen, China
insert_time	int64	Alarm storage time	-	2023/1/1 0:00:00
service_id	string	Honeypot ID	-	-
type	string	Alarm sub-type identification	-	ti
sub_source_type	string	Alarm sub-type	Alarm classification, including Virtual Patching, Basic Defense, Ban List, Network Honeypot, etc.	Virtual Patching
sub_source_type_res	string	Alarm sub-type identification ID	Alarm sub-type identification ID, source_virtualpatch Virtual Patching, source_basicrule Basic Defense, etc.	source_virtualpatch

payload	string	Attack payload	Payload information of attack traffic	-
cmdline	string	Command	Network honeypot host event, sensitive command executed in the honeypot	bash -c ifconfig execve /bin/bash|m=100755|o=
template_id	string	Network honeypot template ID	-	-
docker_id	string	Unique ID of network honeypot	-	-
proc_chan	string	Process tree	Process tree of the network honeypot host event	bashP{
kill_chain	string	Attack chain	Attack chain, attack phase of the alarm event	Vulnerability exploitatio
kill_chain_res	string	Attack chain identification ID	-	kill_chain_exploit
event_id	string	Alarm ID	-	-
exe	string	Executable file path	-	/sbin/ifconfig
probe_id	string	Probe ID	-	probe-id
service_type	string	Network honeypot type	Network honeypot type	SSH Honeypot
service_type_res	string	Network honeypot type	-	ssh_honeypot

		identification ID		
script_name	string	Network honeypot script name	-	-
log_source	string	Data source	The alarm values for Inter-VPC Firewalls and intranet honeypots are set to move. The alarm value for honeypot hosts is set to host. The alarm value for public network honeypots is set to network.	move
login_user	string	Attack a logged-in user	-	[root, 1qaz!QAZ]
visible_tag	int	Visibility	-	-
timestamp	string	Alarm timestamp	-	2023-01-01T00:00:00+08:00
ti_type	string	Associated intelligence threat type tag (included in the alarm)	-	["SSH Honeypot Attack","Conventional Network Brute Force","Brute Force Attack"]
ti_type_en	string	Associated intelligence threat type tag (included in the alarm)	-	["SSH honeypot attack","General netwo cracking","Brute force"]

ti_white	string	Allowlist tag (included in the alarm)	-	Intelligence allowlist
ti_white_res	string	Allowlist tag (included in the alarm) identification ID	-	intelligence_allowlist
src_country	string	Source country	The country where the source IP is located	United States of Americ
src_country_en	string	Source country - English	The country where the Source IP is located - English	United States of Americ
dst_country	string	Destination country	The country where the destination IP is located	United States of Americ
dst_country_en	string	Destination country - English	The country where the destination IP is located - English	United States of Americ
attack_vector	string	Attack exploitation method	-	code-exec
attack_count	int	Number of alarms	-	-
nat_ip	string	NAT IP	NAT public IP address	8.8.8.8
nat_port	int	NAT port	NAT public network port	-
fws_id	string	Firewall ID	-	-
fw_type	string	Firewall type	Firewall type, including: vpc: Inter-VPC Firewall nat: NAT Firewall	nat

			sg: enterprise security group empty: edge firewall	
src_vpc	string	ID of the VPC where the attacker asset is located	-	-
dst_vpc	string	ID of the VPC where the victim asset is located	-	-
src_ins_id	string	Attacker-related asset ID	-	-
dst_ins_id	string	Victim-related asset ID	-	-
nat_ins_id	string	NAT instance ID	-	-
nat_ins_name	string	NAT instance name	-	-

Traffic Logs

Last updated：2024-09-06 17:50:48

Field Identifier	Field Type	Field Name	Field Description	Reference Values	Specific Types	Rema
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-wa
dst_domain	string	Access	-	-	CFWOnline,	-

		destination domain name			CFWNetflowNat	
in_pkt_count	uint64	Number of inbound packets	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat, CFWNetflowFl	-
in_pkt_len	uint64	Inbound packet size	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat, CFWNetflowFl	-
out_pkt_count	uint64	Number of outbound packets	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat, CFWNetflowFl	-
out_pkt_len	uint64	Outbound packet size	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat, CFWNetflowFl	-
total_pkt_count	uint64	Number of total packets	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat, CFWNetflowFl	-
total_pkt_len	uint64	Total packet size	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat, CFWNetflowFl	-
ti_tag	string	Associated intelligence tags (included in the alarm)	-	-	CFWOnline, CFWNetflowNat	-
start_time	int64	Session start time	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat, CFWNetflowFl	-
end_time	int64	Session end time	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat, CFWNetflowFl	-

supplier	string	ISP	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
supplier_en	string	ISP - English	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
src_country	string	Source country	The country where the source IP is located	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
src_country_en	string	Source country - English	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
dst_country	string	Destination country	The country where the destination IP is located	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
dst_country_en	string	Destination country - English	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
src_province	string	Source province	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
src_province_en	string	Source province - English	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
dst_province	string	Destination province	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
dst_province_en	string	Destination province - English	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
src_city	string	Source city	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
dst_city	string	Destination	-	-	CFWOnline,	sd-wa

		city			CFWNetflowVpc, CFWNetflowNat	
district	string	Region	-	-	CFWOnline, CFWNetflowNat	-
address	string	Detailed address	Inbound is the source detailed address Outbound is the destination detailed address	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
address_en	string	Detailed address - English	Inbound is the source detailed address - English Outbound is the destination detailed address - English	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
src_lat	float32	Source dimension	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
dst_lat	float32	Destination dimension	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
src_lon	float32	Source longitude	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
dst_lon	float32	Destination longitude	-	-	CFWOnline, CFWNetflowVpc, CFWNetflowNat	sd-wa
insert_time	int64	The time when the log is generated and written into the database	-	-	CFWOnline, CFWNetflowNat	-

count	uint64	Number of alarms	-	-	CFWOnline	-
url	string	Layer-7 URL	-	-	CFWOnline	-
domain_flag	uint8	Whether the domain name exists	1: exist 0: not exist	-	CFWOnline	-
port_status	uint8	Port status	1: open 0: close	-	CFWOnline	-
bot_flag	uint8	Reserved field	-	-	CFWOnline	-
mode	uint8	Firewall attributes	1: serial 0: bypass	-	CFWOnline	-
argus_ip	uint32	Reserved field	-	-	CFWOnline	-
tcp_flag	uint8	TCP label	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-wa
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 (for internal use)	Current log type fixed value: 2	-	CFWNetflowVpc	-

if_pair_key	string	Reserved field	-	-	CFWNetflowVpc	-
uuid	int64	Unique ID of original alarm log	-	-	CFWNetflowVpc	-
flow_id	int65	Internal field	-	-	CFWNetflowVpc	-
src_vpc	string	ID of the VPC where the attacker asset is located	-	-	CFWNetflowVpc	-
dst_vpc	string	ID of the VPC where the victim asset is located	-	-	CFWNetflowVpc	-
dst_vpc_name	string	Destination VPC name	-	-	CFWNetflowVpc	-
src_vpc_name	string	Source VPC name	-	-	CFWNetflowVpc	-
retans	int8	Is there a retransmission	1: retransmission 0: no retransmission	-	CFWNetflowVpc, CFWNetflowNat	-
status	uint8	Disposition status	-	-	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 name	-	-	CFWNetflowVpc	-

is_out	int8	Identifier of SD-WAN firewall accessing the public network	1: access public network 0: normal access	-	CFWNetflowVpc	sd-wa
ti_tag_en	string	Attacker IP intelligence tag - English	-	-	CFWNetflowNat	-
fw_type	string	Alarm sub-type	-	-	CFWNetflowNat	-
fw_region	string	Region where the firewall is located	-	-	CFWNetflowNat	-
nat_ip	string	NAT IP	NAT IP address	-	CFWNetflowNat	-
nat_port	uint16	NAT port	-	-	CFWNetflowNat	-
if_id	string	Network interface ID	-	-	CFWNetflowFl	-
action	string	Alarm action	Alarm handling action	Block, allow	CFWNetflowFl	-

Operation Logs

Last updated：2024-09-06 17:52:07

Field Identifier	Field Type	Field Name	Specific Types
level	string	Danger level	CFWOperateLogAll
operator	string	Operator	CFWOperateLogAll
result	string	Operation result	CFWOperateLogAll
fw_type	string	Firewall type	CFWOperateLogAll

action	string	Firewall switch - operation behavior Asset center operation - operation behavior Access control operation - operation behavior Zero trust protection operation - operation behavior Intrusion defense operation - operation type Address template operation - operation behavior Network honeypot operation - operation behavior General settings operation - operation behavior	CFWOperateLogAll
opt_type	string	Operation	CFWOperateLogAll

		logs category	
detail	string	Firewall Switch - operation details Asset center operation - operation details Access control operation - operation details Zero trust protection operation - operation details Intrusion defense operation - operation behavior Address template operation - template description Network honeypot operation - operation details General settings operation -	CFWOperateLogAll,CFWOperateWebAccess

		operation details	
time	string	Occurrence time	CFWOperateLogAll
app_id	string	Unique ID of the tenant	CFWOperateLogAll
info	string	Access control operation - rule description Intrusion defense operation - operation details Address template operation - operation details	CFWOperateLogAll
longitude	float32	Source longitude	CFWOperateLogAll

address	string	Source city	CFWOperateLogAll,CFWOperateRemoteOM
district	string	District and county of the source city	CFWOperateLogAll
more_info	string	Additional information	CFWOperateLogAll
rule	string	Rule list	CFWOperateLogAll

instance_region	string	Asset instance region	CFWOperateLogAll
public_ip	string	Honeypot public IP	CFWOperateLogAll
remote_type	string	Operation type General settings operation - log type	CFWOperateLogAll
services	string	Honeypot detailed information	CFWOperateLogAll

template_id	string	Honeypot template ID	CFWOperateLogAll
region	string	Asset region	CFWOperateLogAll,CFWOperateWebAccess
instance_id	string	Related asset ID	CFWOperateLogAll,CFWOperateRemoteOM
asset_type	string	Asset classification	CFWOperateLogAll

addr_name	string	Template name	CFWOperateLogAll
base_type	string	Baseline type	CFWOperateLogAll
timestamp	string	Alarm timestamp	CFWOperateLogAll,CFWOperateRemoteOM,CFWOperateW
level_res	string	Danger level identification ID	CFWOperateLogAll

action_res	string	Operation behavior identification ID	CFWOperateLogAll
detail_res	string	Operation detail identification ID	CFWOperateLogAll
rulelist	string	Rule list	CFWOperateLogAll

appid	string	appid	CFWOperateLogAll,CFWOperateWebAccess
instance_region_res	string	Asset instance region identification ID	CFWOperateLogAll

rule_res	string	Rule list identification ID	CFWOperateLogAll
natinsid	string	NAT instance ID	CFWOperateLogAll

remote_type_res	string	Operation type identification ID	CFWOperateLogAll
detail_id	string	Operation details asset ID	CFWOperateLogAll
base_type_res	string	Security baseline type	CFWOperateLogAll

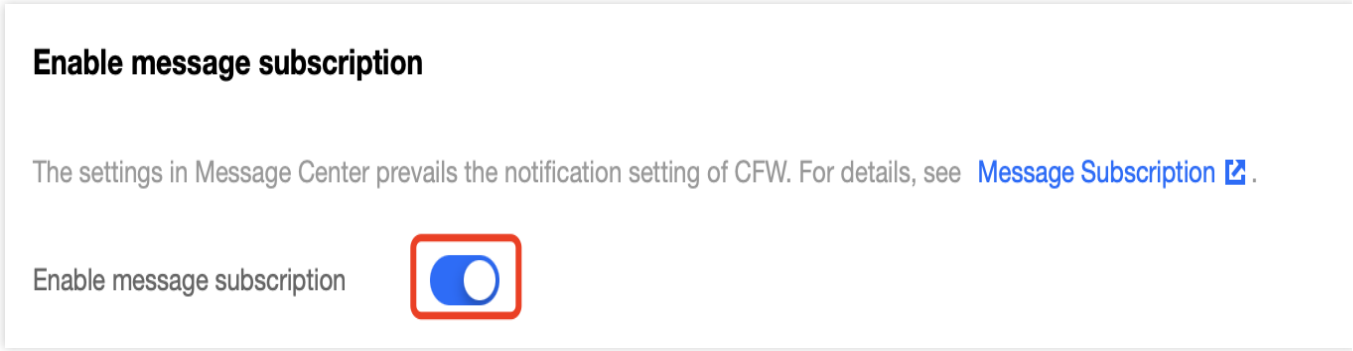
Notifications and Settings

Last updated：2024-09-06 17:53:51

Subscribing to Message Center

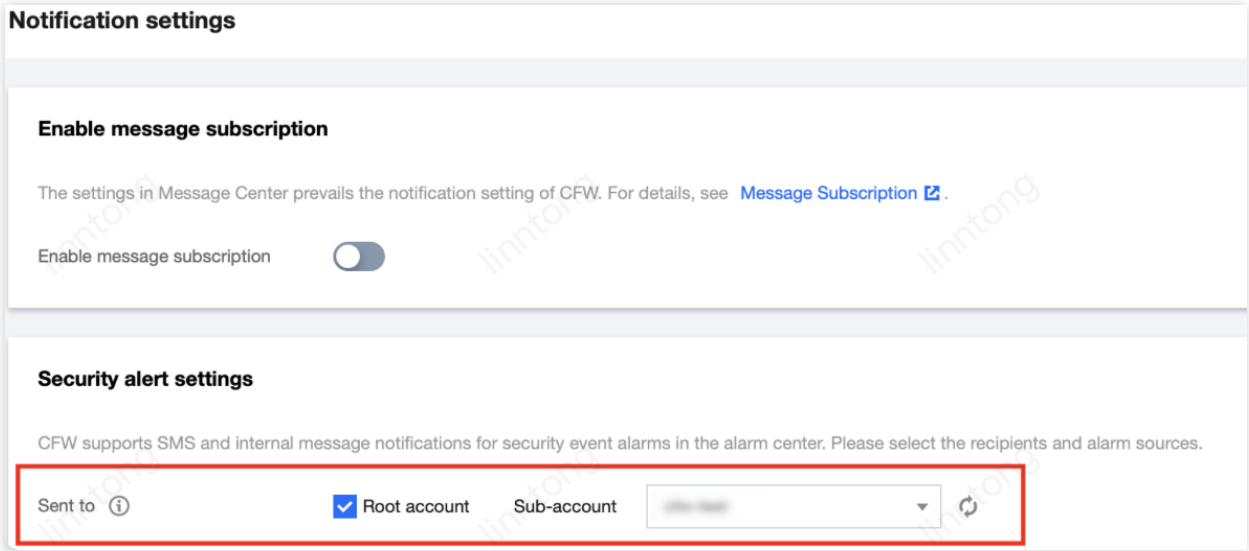
CFW adopts non-subscription push by default. Refer to the Notification Settings for the Notification Account configuration. CFW will automatically recognize accounts used for login to the CFW console and add them to the optional list.

1. Log in to the CFW console, and click **Notification Settings** in the left sidebar.
2. On the Notification Settings page, configure push notifications for the firewall. If you need to switch to subscription-based push or enable Message Center configurations, you can click the the **Switch** of the **Enable message subscription** .



Note:

After the Message Center is enabled, **all alert objects in the Notification Settings for all alarm types will be invalid**. Details are subject to the Message Center settings.



Configure Notification Settings

On the Notification Settings Page, you can configure common firewall alarms and notifications.

Notification Type	Notification Content	Supported Configuration Items
Security Alarm Notification	CFW supports SMS, message center, and WeChat notifications for security event alarms in the Alarm Center. You can configure objects and alarm sources in the console.	Supports configuring Tencent Cloud security WeChat service account alarms. Supports triggering notifications based on alarm type.
Bandwidth Alarm Notification	We provide three-tier bandwidth alarms. When the firewall bandwidth reaches the threshold percentage you set, it will trigger alarm notifications via SMS, message center, and WeChat for the selected account.	Supports distinguishing different cascaded alerts based on firewall type.
Capacity Alarm Notification	We provide two-tier storage alarms. When the firewall storage reaches the threshold percentage you set, it will trigger alarm notifications via SMS, message center, and WeChat for the selected account.	Supports configuring cascaded alarms.
Disaster Recovery Alarm Notification	When your NAT Firewall or Inter-VPC Firewall triggers BYPASS, it will trigger alarm notifications via SMS, message center, and Email for the selected account.	-
Enterprise Security Group Changes Notification	When changes are detected in your account's Enterprise Security Group, we will send you relevant notifications regardless of whether you have enabled automatic delivery.	-
Automatic Task Exception Notification	When an exception is detected in your automatic task, we will send you relevant notifications.	-
System Log Shipping Notification	When new system logs are generated, we will notify you according to your settings.	Supports triggering notifications by system log event type.

General Settings

On the General Settings page, the general settings consolidate some commonly used configurations.

Configuration Item Name	Configuration Item Description	Notes
Log Storage Settings	The users of Enterprise Edition and later can modify the log storage type and storage duration. This can be done only once every 2 months. Expired logs will be automatically deleted. You can also manually clear logs, but please note that each user is limited to 4 manual clearances per natural month.	After the log settings are changed, the historical logs will not be affected. Only new logs starting from the time of the editing will be effective. For example, if you change the log storage time from 180 days to 90 days, the historical logs will still be stored for 180 days, while new logs will be stored for 90 days.
Access Control Rules Settings	In the access control rule list, each time you add, insert, or import control rules, the startup status of the rule should be set.	-
Honeypot Auto-rebuild Settings	In the Network Honeypot, if the honeypot is compromised, you can choose whether to automatically rebuild the honeypot and set the interval time.	-
Tag Settings	CFW has no resource attributes. It only supports adding Tags to billing resources associated with the account. You can modify the Tag values here.	-

Common Tools
Address Template

Last updated：2024-01-23 17:37:00

This topic describes how to batch manage IP addresses in an address template and match the created templates with access control rules.

Operation guide

1. Log in to the Cloud Firewall console, and then click **Address template** in the left navigation pane.
2. On the **Address template** page, you can create and modify templates, and call templates to add rules on the **Access Control** page.

Create template

a. On the **Address template** page, click **Create template**.

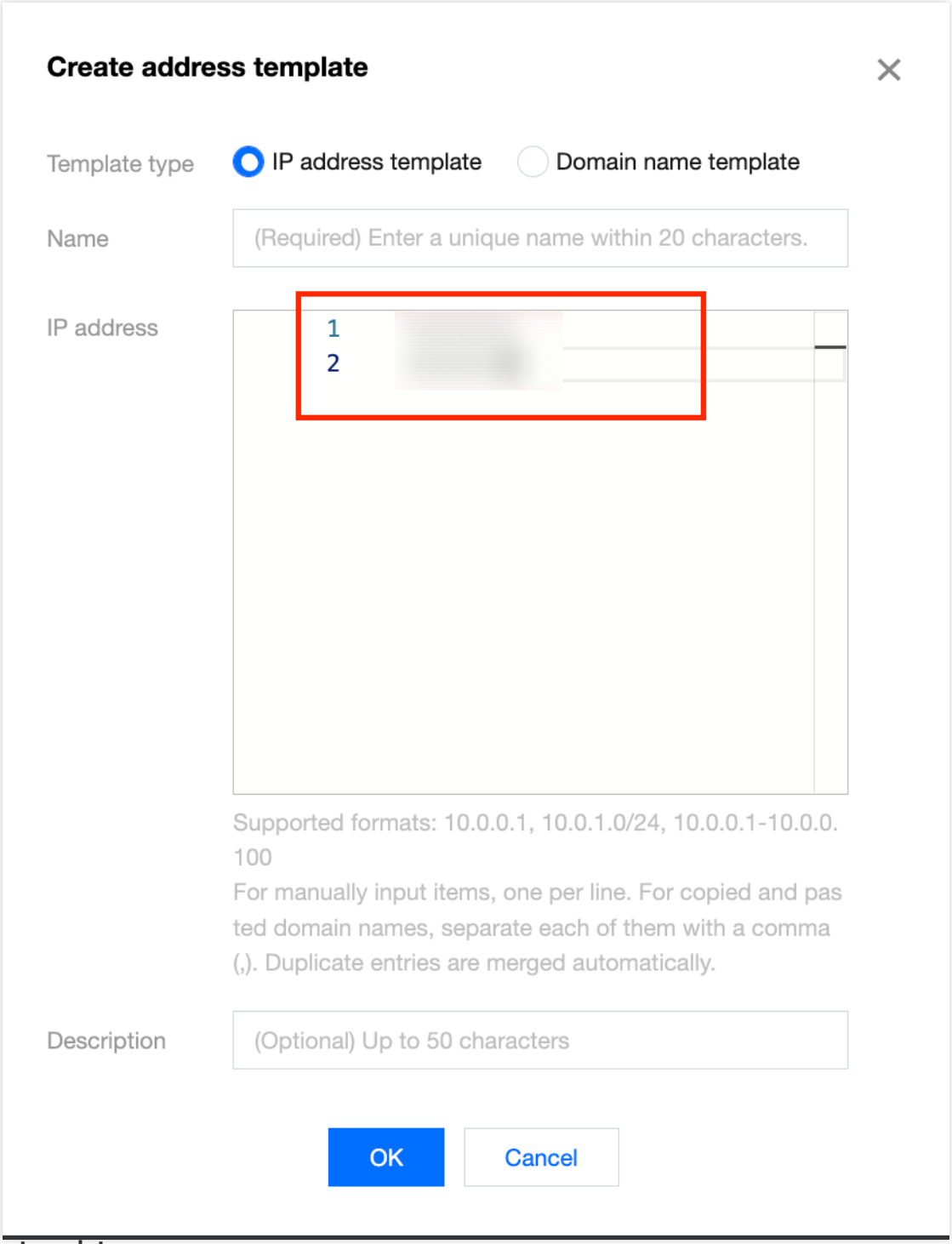
b. In the **Create address template** window displayed, enter the address template name and IP address, and then click **OK** to complete the template creation.

Note

For a single IP address, Press Enter.

For multiple IP addresses, separate them with commas before pasting.

Duplicate IP addresses are merged automatically.

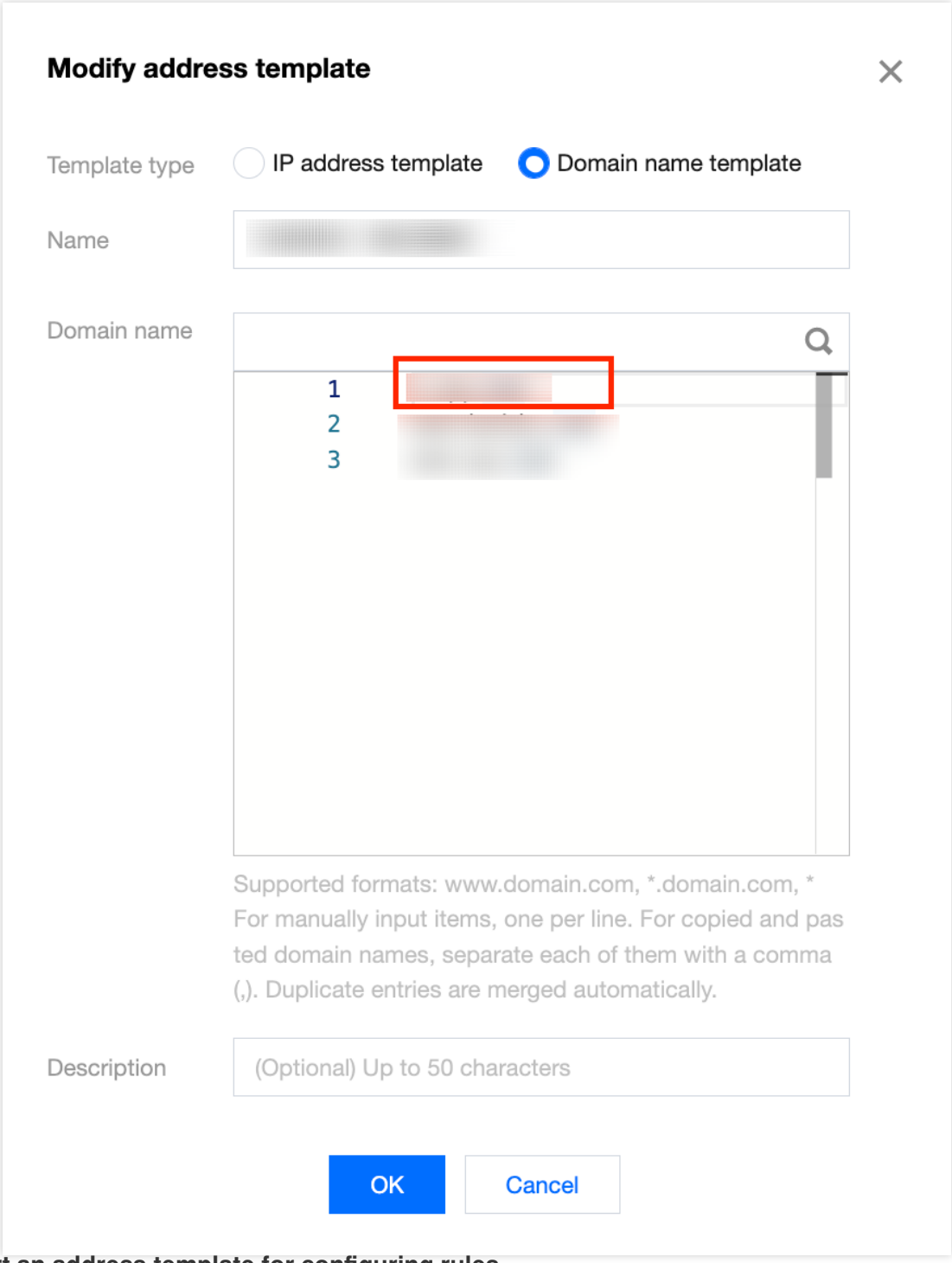


Modify template

After a template is created, it will be displayed in the address template list, and you can add, delete, or modify IP addresses in the list.

a. In the action column on the right of the destination address template, click **Modify**.

b. Select the IP address to modify or delete in the **Modify address template** window displayed, or enter the IP address in the search box, and then click **OK** to complete the modification.



Import an address template for configuring rules

After creating an address template, you can go to the Edge firewall rules or NAT firewall rules page to call the template for configuring access control rules. The following example shows how to import an address template for configuring edge firewall rules. This also applies to NAT firewall rules.

Note

The access rules configured with the address template are valid for all IP addresses in the template.

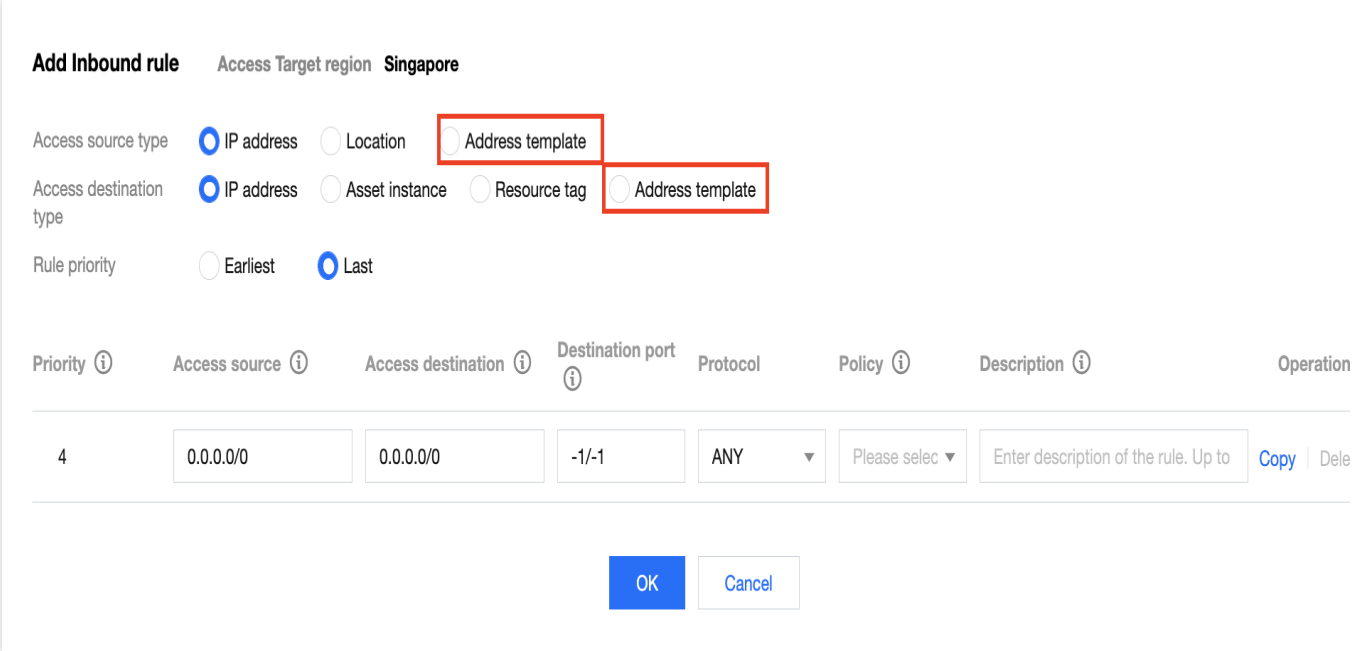
Address templates can only be used to configure edge firewall rules and NAT firewall rules, rather than inter-VPC firewall rules.

Inbound rules only allow importing address templates for **Access source**, while **Outbound rules** only allow importing templates for **Access destination**.

Import an address template for inbound rules

a. On the Edge firewall rules page, select **Inbound rules** -> **Add rule**.

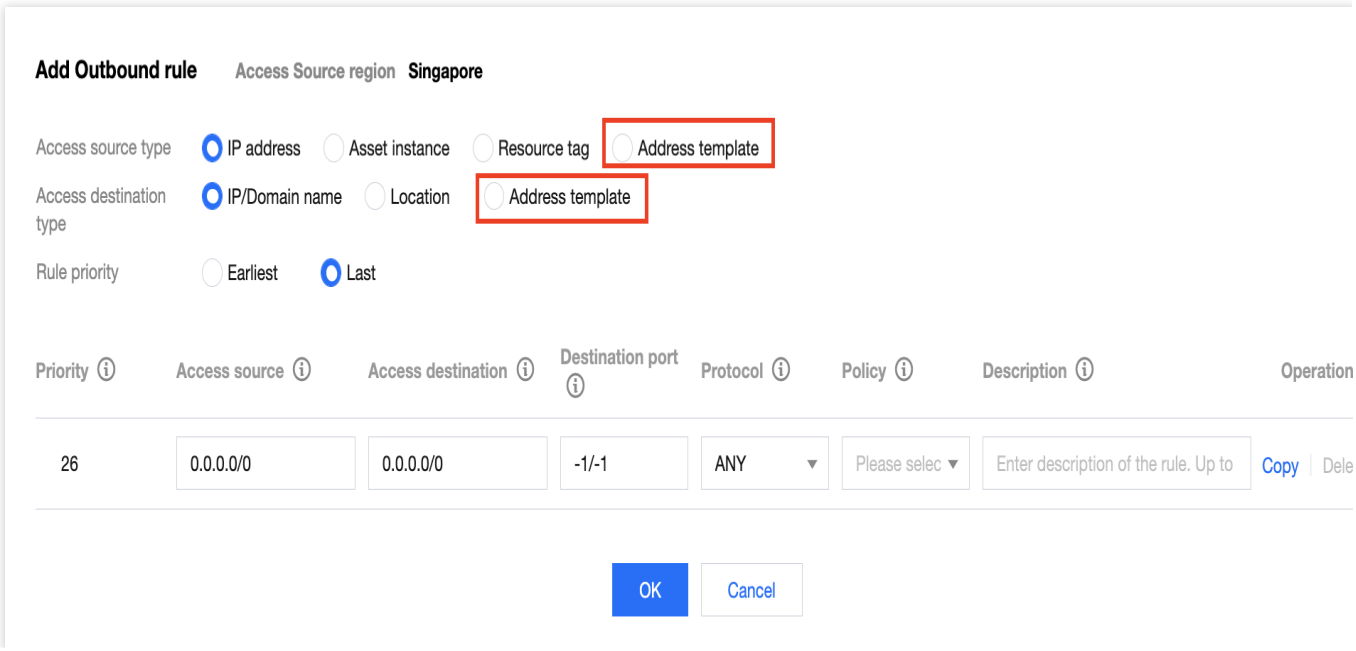
b. In the "Add inbound rule" window displayed, select "Address template" for "Access destination type", and click the "Access source" drop-down list to select an existing address template for configuring rules.



Import an address template for outbound rules

a. On the Edge firewall rules page, select **Outbound rules** -> **Add rule**.

b. In the "Add outbound rule" window displayed, select "Address template" for "Access destination type", and click the "Access destination" drop-down list to select an existing address template for configuring rules.


Add Outbound rule
Access Source region Singapore
Access source type
IP address
Asset instance
Resource tag
Address template
Access destination type
IP/Domain name
Location
Address template
Rule priority
Earliest
Last
Priority
Access source
Access destination
Destination port
Protocol
Policy
Description
Operation
26
0.0.0.0/0
0.0.0.0/0
-1/-1
ANY
Please selec
Enter description of the rule. Up to
Copy
Dele
OK
Cancel

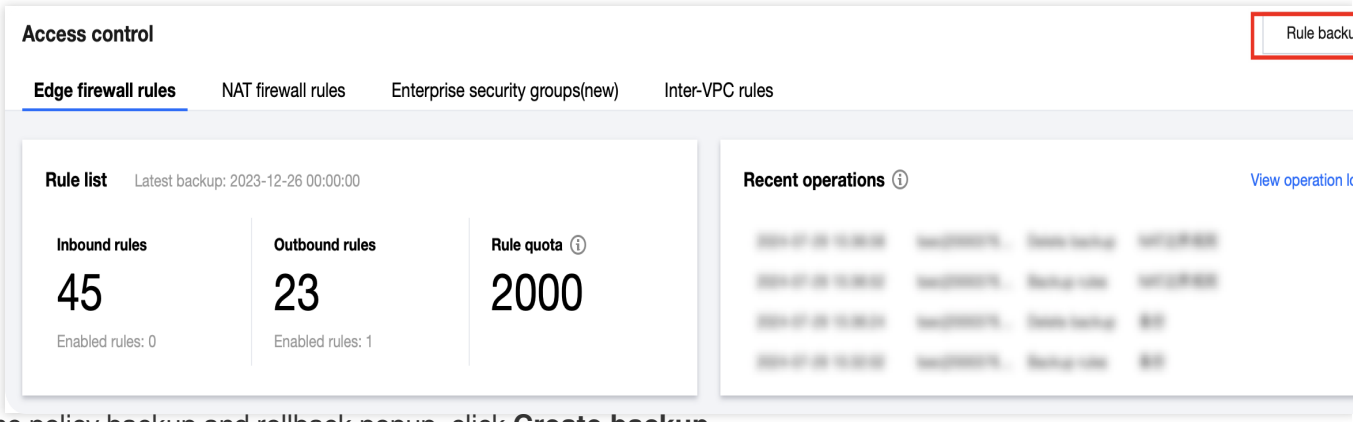
Rule Backups

Last updated：2024-09-06 17:56:10

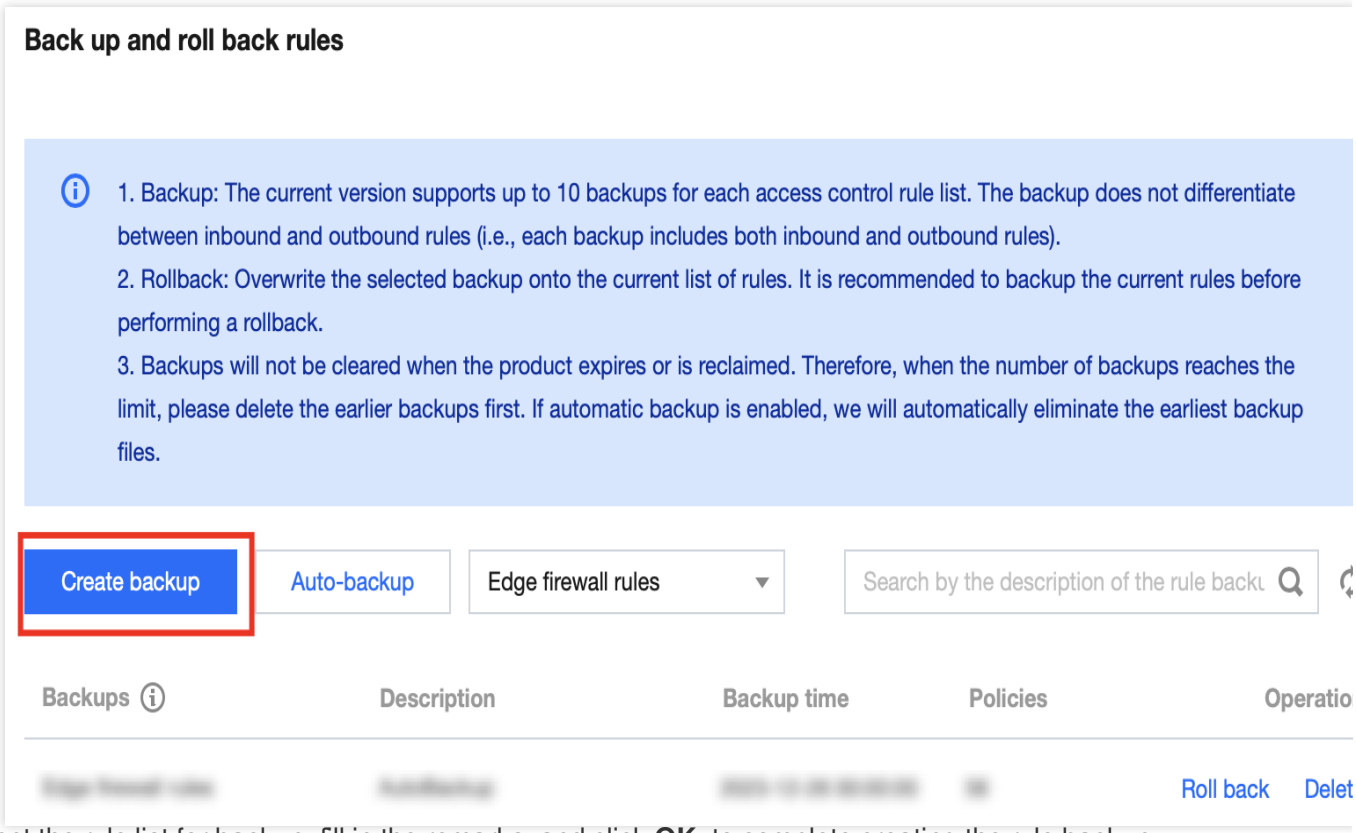
When modifying access control rules, you can back up existing rules and roll back rules in different defense statuses.

Creating Backup

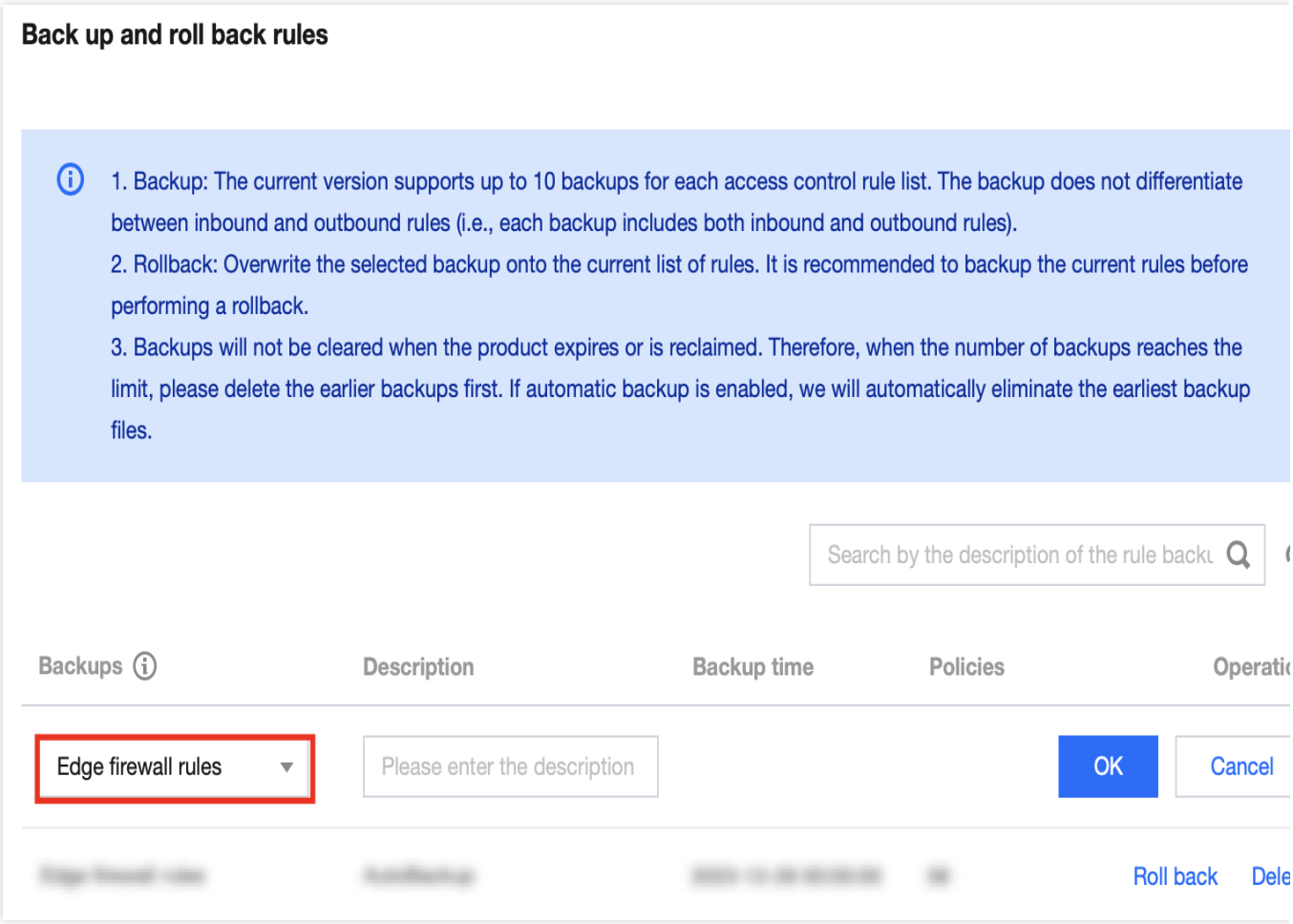
1. Log in to the Cloud Firewall console, and click **Access Control** in the left sidebar.
2. On the Access Control page, click **Rule backups** in the upper right corner to open the Policy Backup and Rollback Popup.



3. In the policy backup and rollback popup, click **Create backup**.

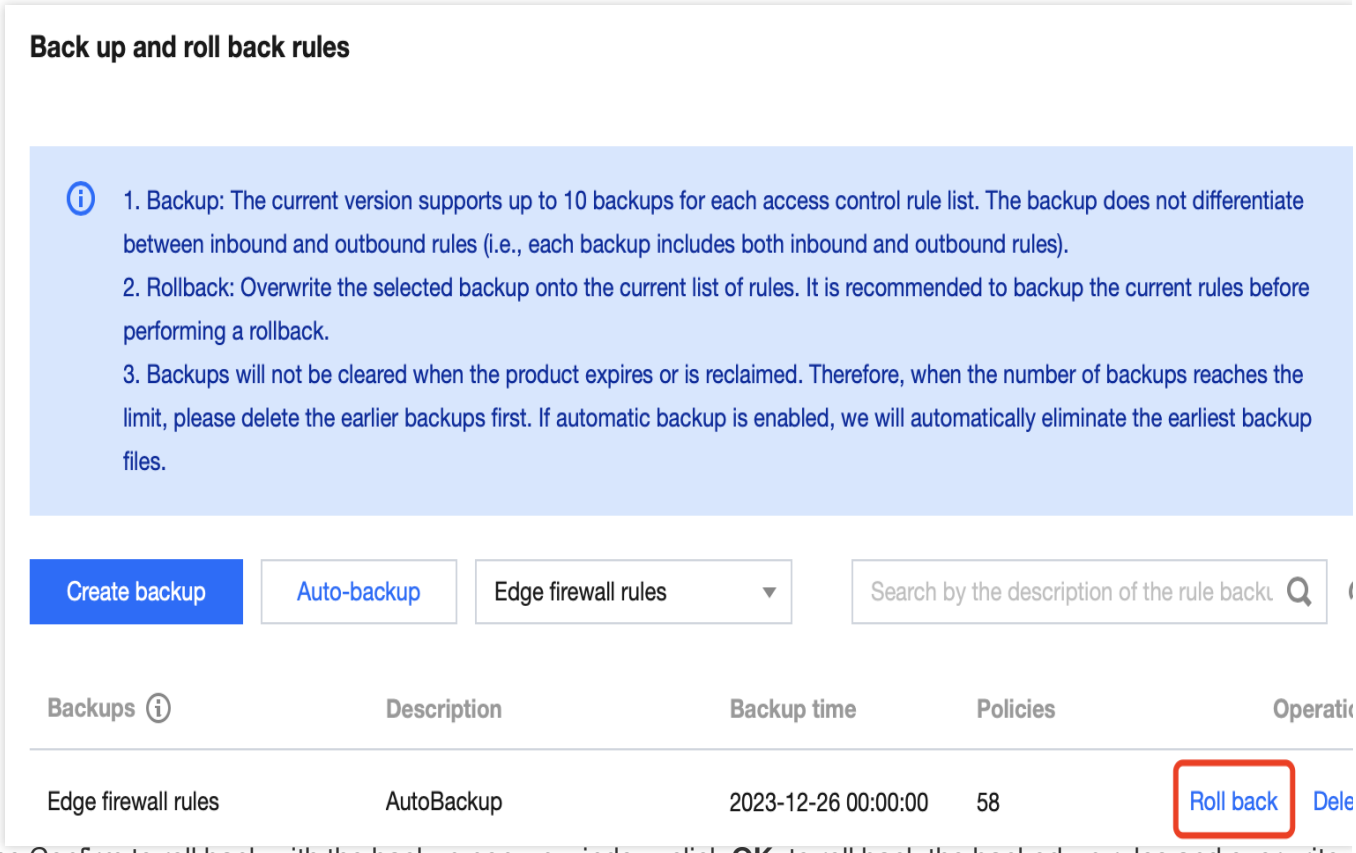


4. Select the rule list for backup, fill in the remarks, and click **OK** to complete creating the rule backup.



Rollback from Backup

1. On the Access Control Page, click **Rule backups** in the upper right corner to open the Policy Backup and Rollback Popup.
2. Select the backed-up rule, and click **Roll back**.



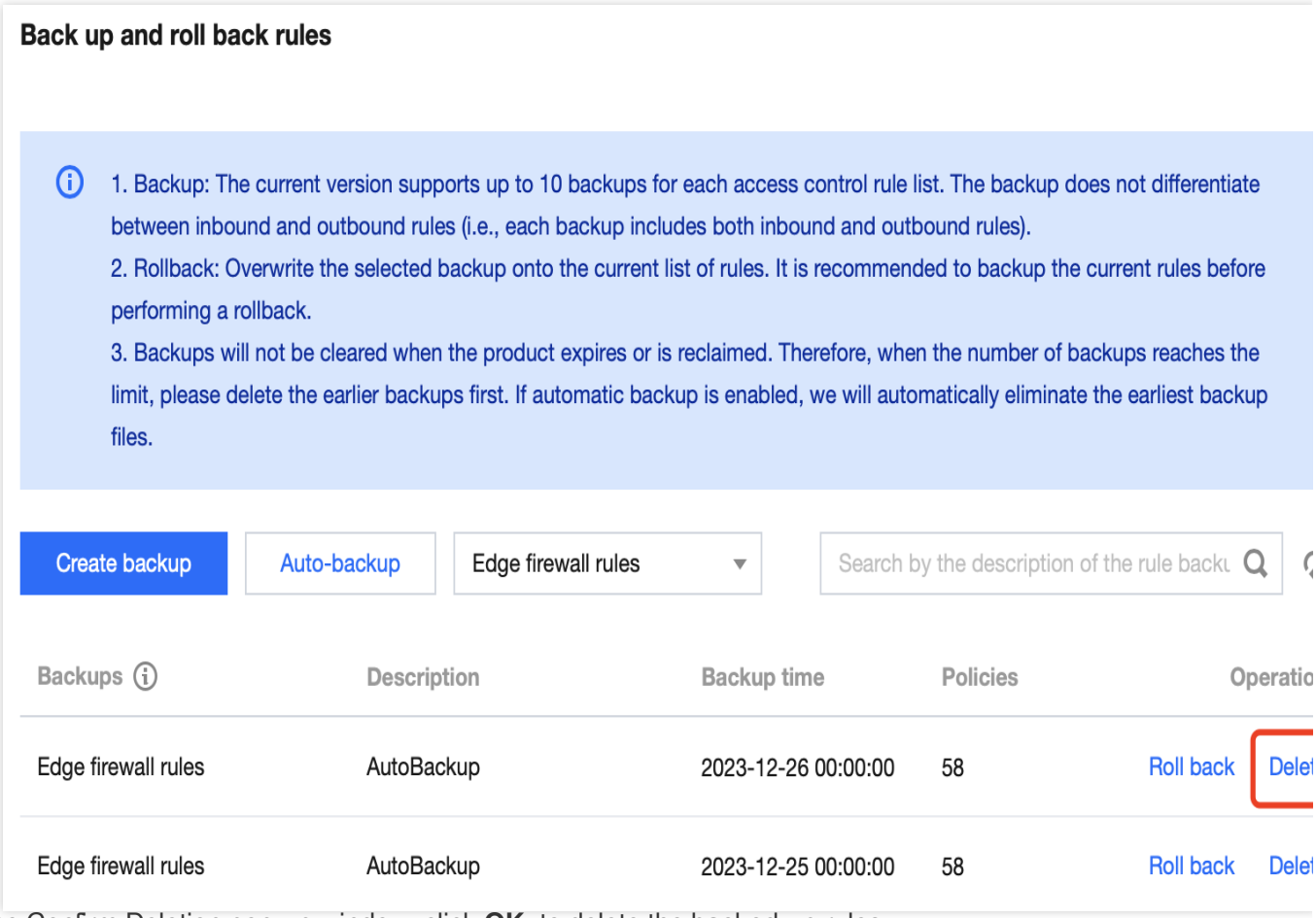
3. In the Confirm to roll back with the backup pop-up window, click **OK** to roll back the backed-up rules and overwrite the current rule list.

Caution

The rule rollback operation will overwrite the corresponding rule list. The current policies will be deleted. To ensure data security, it is recommended to back up the current list first.

Deleting Backup

1. On the Access Control Page, click **Rule backups** in the upper right corner to open the Policy Backup and Rollback Popup.
2. Select the backed-up rule, click **Delete**.



3. In the Confirm Deletion pop-up window, click **OK** to delete the backed-up rules.

Caution

Once the rule backup is deleted, it cannot be retrieved/recovered. Please proceed with caution.