Cloud Firewall

FAQs

Copyright Notice

Trademark Notice

Service Notice

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

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

Contact Us

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

Contents

FAQs
Basic Introduction

Last updated: 2025-05-20 14:40:43

What Is CFW?

Tencent Cloud Firewall (CFW) is a SaaS-based firewall in the public cloud environment. It mainly provides Internet boundary protection for users and meets the security and management needs of unified management of access control, log audit, etc. on the cloud. CFW not only has features of traditional firewalls, but also supports cloud multi-tenancy and elastic scale-out features. It is the first network security infrastructure for user business cloud migration.

Is It Possible for CFW to Protect Assets on Non-Tencent Cloud?

The firewall can only protect IP assets under Tencent Cloud accounts and does not support assets on Non-Tencent Cloud.

Can CFW Be Deployed on Private Cloud?

Starting from version 380, TCE supports the cloud firewall service.

What Are the Differences between CFW and Security Group?

CFW and security group are two independent systems. When the Internet switch of the public network EIP is turned on and the policy is enabled at the same time, the traffic will be allowed.

- The objectives controlled by the two are different. The Internet edge firewall controls the access traffic of public IP addresses, and the security group controls all traffic of the CVM network interface card.
- The granularity of the functions of the cloud firewall and security group is different. The security group acts on instances, and the cloud firewall acts on public IPS, NAT Boundary Protection, peering connections between VPCs or Cloud Connect Network.
- Security group ACL is merely the most basic feature of CFW. More importantly, CFW has the capacity for real-time blocking of intrusion detection/prevention (IPS) and full traffic log audit.

Differences between CFW and WAF Products?

- The Web Application Firewall (WAF) only provides protection for web business. It has no protection capability for non-web business and only protects against attacks from outside

to inside. It has no monitoring and protection capabilities for malicious outgoing requests from the business.
- CFW includes all business protection. It supports basic protection for Web vulnerabilities and simultaneously supports active detection of outbound traffic from internal to external. It supports automatic interception of compromised hosts and malicious outbound connections.

Both CFW and SOC Have Traffic Threat Awareness Functionality. What Are the Differences between Them?

CFW integrates enterprise-level IPS functionality and IDS functionality. It has hour-level virtual patching capabilities for 0day vulnerabilities. There is no need to restart the business after an upgrade. These capabilities are not available in SOC.

Can CFW Protect CDN or COS?

CFW does not support the protection of SaaS services such as CDN, COS, Anti-DDoS IP, SaaS-WAF, and CDB.

Does Traffic Transit through the Firewall before Going through Other Products? Will CDN Traffic Be Protected by the Firewall?

- CDN node IPs belong to CDN carriers and are not within the protection scope of your Cloud Firewall.
- For the serial firewall, traffic will be detected by Cloud Wall only when CDN sources back to CLB/CVM. High-defense IP sourcing back to CLB will also pass through the Cloud Wall, but what is seen is the source address of the high-defense IP.
- The bypass firewall cannot obtain CDN origin-pull traffic due to architectural reasons. It is recommended to switch to a serial firewall.
- The public IP type supported in the current version is BGP IP. Three-network IPs are not supported yet. When identifying user assets, CFW will automatically filter three-network IPs.

Does CFW Have a QPS Limit?

CFW is a SaaS feature. It has no limit on the concurrency, new connection creation, QPS, etc. of traditional hardware firewalls. The only performance metric to measure CFW is the actual bandwidth throughput.

Does External Inbound Traffic Go through CFW or WAF First?

For Inbound Traffic

- The Web Application Firewall (WAF) and CFW jointly compose the overall boundary protection of cloud cybersecurity. WAF tends to provide protection for encrypted HTTPS traffic. Unencrypted traffic is protected by the basic rules and virtual patching of the IPS (Intrusion Prevention System) integrated in CFW.
- For different types of WAF and different types of Internet edge firewalls, their working modes are as shown in the table below:

Firewall Type	Internet Boundary Bypass Firewall	Internet Boundary Serial Firewall
SaaS-WAF	Work in parallel, traffic will not pass through firewall	Work in serial, traffic first passes through WAF, then through the firewall, and all firewall source IPs are origin-pull IPs.
CLB-WAF	Work in serial, traffic first passes through the firewall, then through CLB-WAF.	Work in serial, traffic first transits the firewall, then transits CLB-WAF.

For Outbound Traffic

- Can implement Proactive Outbound Connection Control based on the granularity of Cloud Virtual Machine (CVM) through NAT boundary firewall, and support access control based on the domain name. Combined with Tencent Threat Intelligence, malicious IPs and domain names of proactive outbound connections can be automatically intercepted.
- If the NAT boundary firewall is not enabled, access control can only be performed on the traffic behind the NAT gateway at the Internet edge firewall. At this point, the CFW sees the public IP.

Cloud Firewall False Alarm and Misinterception Emergency Plan

Last updated: 2025-09-23 17:59:02

What Is Bandwidth? How Do Users Select Suitable Bandwidth?

- The bandwidth of CFW is independent of that of other network products. Therefore, the bandwidth of CFW needs to be purchased separately.
- Internet edge firewall bandwidth: Trial use CFW, enable the internet boundary firewall switch for about 7 days, and purchase based on the peak bandwidth of outbound/inbound traffic statistics in the console.

> **Note:**
> CFW provides a 7-day free trial activity for eligible Tencent Cloud users. Your Tencent Cloud account needs to meet the following conditions:
> 1. Completed enterprise authentication and not participated in the CFW free trial activity.
> 2. A root account and its sub-accounts can only apply for a free trial once in total.

- NAT and CFW are independent of each other and connected in series. Therefore, it is necessary to select a CFW bandwidth with the same or higher capacity as that of the NAT gateway.
- Cloud Connect Network (CCN) and CFW are independent of each other and connected in series. Therefore, it is necessary to select a CFW bandwidth with the same or higher capacity as that of the Cloud Connect Network (CCN).

What Is Peak Bandwidth? Is It Uplink Bandwidth or Downstream Bandwidth?

Peak bandwidth refers to the maximum value of uplink and downstream bandwidth. For example, if you purchase 100 Mbps bandwidth, then CFW can process uplink 100 Mbps and downstream 100 Mbps simultaneously.

Will My Business Be Affected If My Business Bandwidth Exceeds the Bandwidth Limit of the Internet Edge Firewall?

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

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

- Partially disable the internet boundary firewall switches, Bypass some traffic, and only protect the traffic within the protection bandwidth specification.
- The disposal methods in serial and bypass modes are the same. Disable some switches to limit traffic.
- Supports configuring the firewall switch weight and sets the priority for automatically shutting down the firewall switch.

> **Note:**
> After the automatic switch-off, you can manually enable the Internet edge firewall switch. If the business exceeds the bandwidth of the Internet edge firewall, continue to take the above measures.

Example:

- Internet edge bandwidth is 1000Mbps, of which 600Mbps is allocated in bypass mode, and 5 Internet boundary switches are turned on; when the total protection business bandwidth in bypass mode reaches 610Mbps, turn off 1 Internet boundary switch, and the CFW protection business bandwidth remains at 600Mbps.
- Internet edge bandwidth is 1000Mbps, of which 400Mbps is allocated in serial mode, of which 200Mbps is in the Guangzhou region, and 4 Internet boundary switches are turned on in the Guangzhou region; when the business bandwidth in the Guangzhou region reaches 310Mbps, turn off 2 Internet boundary switches, and the CFW protection business bandwidth in the Guangzhou region remains at 200Mbps.

After the cooldown period, if the business bandwidth is lower than the bandwidth of the Internet edge firewall, the firewall switch automatically restores to on.

Excess Count (Month)	Cooldown Duration
3 times and below	2 hour
4 to 7 times	1 day
8 times or more	3 days

Example:

- North-south bandwidth is 1000Mbps, of which 600Mbps is allocated in bypass mode, and 5 Internet boundary switches are turned on; when the business bandwidth reaches 610Mbps, turn off 1 Internet boundary switch and only turn on 4 Internet boundary switches. The CFW protection business bandwidth remains at 600Mbps. Exceeded 2 times

in the last month, and the Internet boundary switches will be restored 2 hours later, with 5 Internet boundary switches turned on.

- North-south bandwidth is 1000Mbps, of which 600Mbps is allocated in bypass mode, and 5 Internet boundary switches are turned on; when the business bandwidth reaches 610Mbps, turn off 1 Internet boundary switch and only turn on 4 Internet boundary switches. The CFW protection business bandwidth remains at 600Mbps. Exceeded 10 times in the last month, and the Internet boundary switches will be restored 3 days later, with 5 Internet boundary switches turned on.

Continue to monitor CFW bandwidth alarms. When the bandwidth is high, turn off part of the CFW switches, or expand the bandwidth to ensure all traffic is protected, to ensure business security.

Will My Business Be Affected If My Business Bandwidth Exceeds the Bandwidth Limit of the NAT Edge Firewall?

- The NAT boundary firewall belongs to inline mode. The protection bandwidth depends on the instance specification. When the business bandwidth exceeds 100% of the NAT boundary firewall bandwidth, it can lead to increased network delay or congestion and packet loss. Pay attention to the firewall bandwidth in time based on business needs.
- Continue to monitor CFW bandwidth alarms. When the bandwidth is high, turn off part of the CFW switches, or expand the bandwidth to ensure normal monitoring and ensure business security.

Will My Business Be Affected If My Business Bandwidth Exceeds the Bandwidth Limit of the VPC Boundary Firewall?

- The VPC boundary firewall belongs to inline mode. The protection bandwidth depends on the instance specification. When the business bandwidth exceeds 100% of the VPC boundary firewall bandwidth, it can lead to increased network delay or congestion and packet loss. Pay attention to the firewall bandwidth in time based on business needs.
- Continue to monitor CFW bandwidth alarms. When the bandwidth is high, turn off part of the CFW switches, or expand the bandwidth to ensure normal monitoring and ensure business security.

Will the Internet Edge Bandwidth of CFW Limit Traffic?

CFW will not limit traffic.

Is the Inbound and Outbound Bandwidth Calculated Separately? If the Outbound Bandwidth Exceeds the Purchase Specification, Will It Impact

the Rule-Based Matching of Inbound Traffic?

- Yes, the inbound and outbound bandwidth is calculated separately.
- The way for the Internet edge firewall and NAT edge firewall to calculate the peak value of traffic is to fetch the maximum value of outbound/inbound traffic.

Is the Bandwidth of the Internet Edge Firewall and NAT Edge Firewall Calculated Separately?

Yes, the bandwidth of the Internet edge firewall and NAT boundary firewall is calculated separately.

> **Note:**
> Use NAT edge firewall bandwidth. Consumption of general North-South bandwidth is required. If you need to expand, just expand the general North-South bandwidth.

Does the Bandwidth of CFW Support Arbitrary Upgrade and Downgrade?

Bandwidth supports scale-out. Capacity downgrade requires submitting a ticket for review.

Does the Bandwidth Limit of CFW Depend on the Bandwidth of the Integrated CVM?

No. The firewall bandwidth specification of CFW is set quotas according to the actually used bandwidth by users. That is, it is ensured that the consumed traffic bandwidth value at the same time cannot exceed the bandwidth parameter of CFW.

Firewall-Related Cloud Firewall (CFW)

Last updated: 2025-05-20 14:41:56

Which Protocols Does CFW Support for Protection?

- Internet edge firewall (bypass mode) currently supports TCP protocol.
- Internet edge firewall (serial mode) currently supports TCP, UDP, ICMP, HTTP, HTTPS, SMTP, SMTPS, TLS/SSL, DNS and FTP protocols.
- NAT boundary firewall supports TCP, UDP, ICMP, HTTP, HTTPS, SMTP, SMTPS, DNS and FTP protocols.
- Inter-VPC firewall supports TCP, UDP, ICMP, HTTP, HTTPS, SMTP, SMTPS, DNS and FTP protocols.

How Does CFW Protect the UDP Protocol?

- Internet edge firewall (serial mode) supports protection for UDP protocol.
- Internet edge firewall (bypass mode) does not support protection for UDP protocol.

What Are the Differences between the Traffic Threat Awareness Feature of CFW and SOC?

CFW rules = basic rules (SOC) + CFW custom rules, which means CFW rules are more various than SOC rules.
Alarms detected by basic rule detection methods can be seen in CFW and SOC, while alerts generated by custom rules can only be seen in CFW.

Does CFW Have Redundancy?

The Internet edge firewall uses a cluster deployment method, while the NAT edge firewall and inter-VPC firewall default to a primary/secondary deployment method.

Does CFW Support Single-Region High Availability?

There are two cases: The Internet boundary uses clustered physical machine deployment to implement an active-active mechanism, which is not affected by the availability zone. The NAT edge firewall and VPC boundary firewall use virtualization technology and currently support cross-regional availability zone deployment. During disaster recovery switch, we will synchronize the session table to ensure that the connection will not be interrupted. The latency of the connection is about 10 seconds. This is mainly because it takes several seconds to determine whether there is an AZ abnormality through the heartbeat mechanism.

After Purchasing CFW, Unable to Enter the CFW Console and the Webpage Keeps Refreshing. How to Resolve?

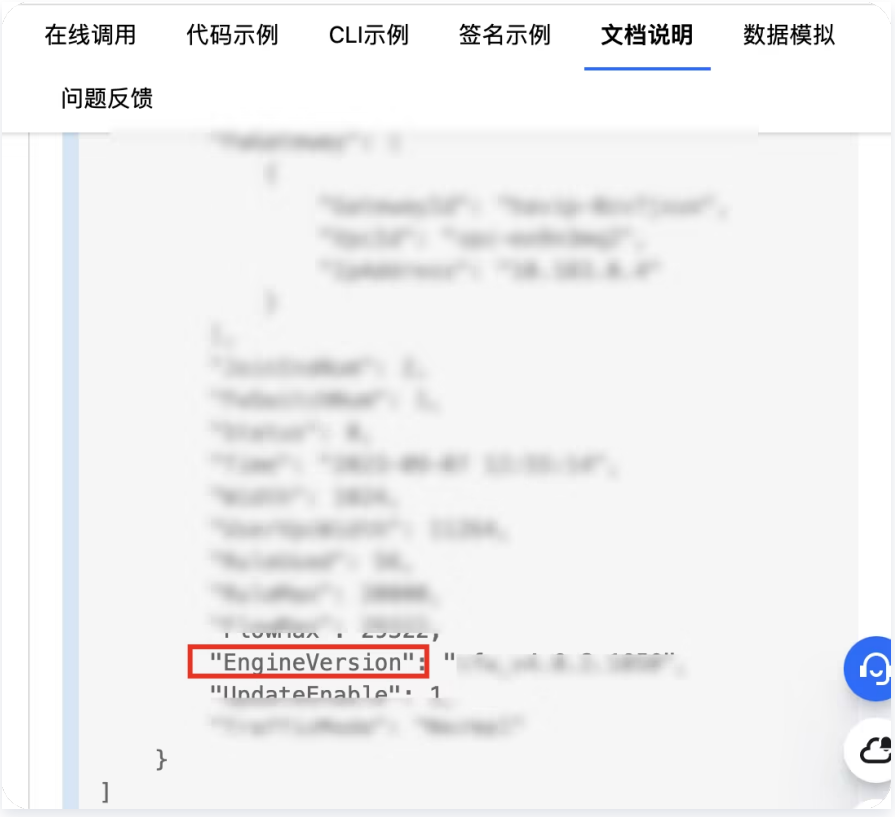
For users who attempt to authorize for the first time, they can try to access the Asset Center Page. At that time, a prompt dialog box will pop up on the page to guide users to complete role authorization. After authorization completion, they can access the Cloud Firewall console normally.

Does CFW Support Protection From Tencent Cloud Direct Connect to IDC Computer Rooms and Whether It Supports Deployment in Physical Server Rooms?

Tencent Cloud Firewall is SaaS-based and does not support deployment in physical server rooms.

How Can I Check the Current Cloud Firewall Version Number?

- Inter-VPC firewall: You can query through the API DescribeFwGroupInstanceInfo, use F12 to access the corresponding firewall switch, and view the "EngineVersion": "cfw_v3.7.0.1009" information (located on the second-to-last line of the response).



- NAT boundary firewall: Query the corresponding NatinsName (NAT instance name) and EngineVersion (engine version) through the DescribeNatFwInstancesInfo API.

Internet Boundary Firewall

Last updated: 2025-05-20 14:42:14

What Is an Internet Boundary Firewall?

- The Internet boundary refers to the boundary between the Internet and Tencent Cloud private network. Internet boundary traffic is the traffic for communication between your cloud assets and the Internet, also known as north-south traffic.
- The Internet Boundary Firewall is a firewall that detects north-south traffic and is a clustered firewall.
- The Internet Boundary Firewall takes effect between your EIP's associated assets and the external Internet.

What Assets Can the Internet Boundary Firewall Support Protection For?

The asset types currently supported by the current version are: Cloud Virtual Machine (CVM), Cloud Load Balancer (CLB), NAT Gateway, and VPN Gateway. Currently, it supports assets in the Chinese mainland and Hong Kong (China).

What Type of Public IP Address Will Not Appear in the Switch List of the Internet Boundary Firewall?

The public IP type currently supported by the current version is BGP IP. CTCC/CUCC/CMCC IP is not currently supported. When identifying user assets, CFW will automatically filter CTCC/CUCC/CMCC IP.

How to Expand Quota and Improve Protection When the Public IP Quota Is Insufficient?

Advanced edition, enterprise edition and flagship edition can enhance specifications through elastic scaling. For each 1 Mbps bandwidth expansion, add 1 public IP quota simultaneously.

What Is an Asset Annotated As the "Other" Type?

The Internet edge firewall performs asset identification on users' public IPs. If there is a public IP that is not bound to an asset, it will be recognized as "other". The rules associated with this IP will come into effect after the asset is bound.

Why Can an IP Still Be Accessed after I Turn on the Internet Firewall Switch?

After turning on the internet edge firewall for an IP, please visit access control and Internet boundary rules to check whether the rule policy type of this IP is block or observe. It will be blocked only if the policy is block. Details of the IP rule policy type are as follows:

- Release: Allows traffic that hits a rule, logs the number of hits but does not log access control, and logs traffic.
- Observe: Allows traffic that hits a rule, logs the number of hits, access control, and traffic.
- Block: Blocks traffic hitting the rule, records the hit count and access control logs, and logs one request packet information in traffic logs.

NAT Boundary Firewall

Last updated: 2025-05-28 10:51:02

Does the Data From the NAT Boundary Firewall Pass through the Firewall Twice?

If the public IP of the NAT firewall is enabled in the Internet boundary switch, the outbound traffic will first pass through the NAT firewall and then through the Internet edge firewall.

What Are the Differences between the New Mode and Access Mode of the NAT Boundary Firewall?

- New mode: If there is no NAT Gateway in the current region, the new mode can use the NAT feature built into the NAT boundary firewall to enable specified instances to access the Internet through the firewall.
- Access mode: If there is already a NAT Gateway in the current region, or if you want to keep the egress IP for public network external access unchanged, the access mode can smoothly integrate the NAT boundary firewall between the NAT Gateway and CVM instances.

Can I Use a NAT Boundary Firewall to Replace the Original NAT Gateway?

The NAT firewall can serve as a substitution for the original NAT Gateway.

Can a NAT Boundary Firewall Be Enabled for a Specific Subnet Only?

One firewall switch corresponds to one subnet. You can choose to enable the firewalls of all subnets associated with the current subnet's route table simultaneously, or only enable the firewall for the current subnet.

Binding EIP on NAT Boundary Firewall Toggle, Will the Network Experience a Brief Interruption?

Binding will not cause a flash cut.

Toggle NAT Boundary Firewall Switch for a VPC, Will the Network Experience a Brief Interruption?

- Enable: Due to routing changes, there may be a 1–2 second network interruption. If the user only chooses to enable a certain subnet, the system will automatically create a new routing table for the current subnet, copy all existing routing policies, add a new routing

policy with the next hop pointing to the NAT boundary firewall in the new routing table, and disable the original routing policy for accessing the public network. Therefore, the internet traffic of this subnet will transit through the NAT boundary firewall.

- Disable: Due to routing changes, there may be a 1–2 second network interruption. If the user only chooses to disable a certain subnet, the system will automatically create a new routing table for the current subnet, copy all existing routing policies, and disable the routing policy with the next hop pointing to the NAT boundary firewall. The subnet will be disconnected from the Internet.

Can I Configure Consecutive Ports for DNAT on the NAT Boundary Firewall Toggle?

Port forwarding does not support configuring multiple ports under the same rule. Each DNAT port requires one rule.

Can NAT Boundary Firewall Be Configured with SNAT? How to Configure It?

1. Log in to the Cloud Firewall Console, click to select the **firewall toggle** > **NAT Boundary Switch**, and enter the NAT Boundary Switch page.
2. In the right operation column of the NAT Boundary Switch page, click **Instance Configuration** > **Egress Binding** > **Create New Rule**.
3. Select the external IP of the corresponding subnet or private network, then click **OK**.

How to Confirm That All Subnets Have Firewalls Enabled?

1. Log in to the Cloud Firewall Console, click to select the **firewall toggle** > **NAT Boundary Switch**, and enter the NAT Boundary Switch page.
2. In the NAT Boundary Switch menu, click the **Firewall Switch** page to view all enabled and not enabled subnet information.

Configure Instance Settings in NAT Boundary Firewall Toggle – Will the Server Need to Restart after Enabling DNS Traffic through NAT Firewall Switch? Will It Take Effect Without Any Operation?

No need to restart the server. Restarting the server only speeds up configuration activation. This is the same as the effective time for configuring DNS on the VPC console. To refresh network configurations, use the following command:

- Linux: dhclient
- windows: ipconfig /flushdns

Period for Automatic Synchronization of Assets in NAT Boundary Firewall Toggle

10 minutes.

Configure How Many Rules for NAT Boundary Firewall Rate Limiting

100 entries.

Number of NAT Gateways That Can Be Connected Simultaneously in NAT Boundary Firewall Access Mode

By default, it can integrate 5 simultaneously. Exceeding this, recommend using a new NAT Boundary Firewall Instance for integration.

What Causes the NAT Boundary Firewall Subnet Switch to Be Closed?

1. Default setting factor: The NAT firewall switch is closed by default during initial configuration and needs to be manually enabled.
2. Factors associated with private network and routing table: In a VPC environment, when the highly available VIP toggle of the cloud firewall in the routing table is in a specific status, such as traffic overload, maintenance, or upgrade status, it may trigger system logic, causing the NAT firewall toggle to be closed.

What Causes the NAT Boundary Firewall Subnet Switch to Fail to Enable?

Possible asset scale changes may occur within the backend polling interval but haven't been synchronized, causing the issue. You can log in to the CFW console, click the **firewall toggle** > **Internet boundary switch** > **synchronize assets**, proactively invoke backend interfaces to re-read and synchronize subnet asset information, then try to enable it again.

How to Change the VPC for a NAT Boundary Firewall?

On the NAT firewall instance page, select the modified firewall, click **More**, choose access configuration, and you can reselect the access VPC.

How Many VPCs Can NAT Boundary Firewall Bind?

There are no limitations currently.

Why Is the Allocated Elastic IP Not Accessible after Enabling the NAT Boundary Firewall?

The newly allocated EIP needs to be bound before it can be accessed.

Whether There Is a Number Limit on the Count of NAT Boundary Firewall Instances?

The number of NAT firewall instances is limited; subject to general quota limits by edition, the advanced edition, enterprise edition, and flagship edition have 1, 2, and 3 instances respectively.

Switching a Certain Subnet From NAT Boundary Firewall (New Mode) to NAT Gateway, Can It Be Achieved Without Affecting the Network?

1. Purchase a NAT Gateway for each VPC.
2. Modify the routing table, and point the next to a NAT gateway.
3. Disable the firewall feature and terminate the firewall instance.

These operations ensure that private network resources can access the public network. Since some of the user's applications require whitelist operations on the egress IP, it is best to contact related personnel to add the NAT gateway's EIP to the allowlist; otherwise, it may cause some applications to be inaccessible.

How to Verify Data after NAT Boundary Firewall Blocking?

On the session perspective of connection count in NAT boundary firewall status monitoring, after performing a blocking operation, refresh the interface. If the original data still exists, you can perform the following operations:

1. After performing a "blocking operation," the status of this interface will not be updated immediately; this is normal. Therefore, it is not recommended to execute this operation consecutively.
2. You can check the enterprise security group to confirm whether the rules have been issued. When the automatic distribution button switch of the enterprise security group is in the open status, the rules will be automatically distributed; if it is not open, manual distribution is required.

Inbound Blocklist/Allowlist Capacity of NAT Boundary Firewall, Does It Align with Serial Mode or Bypass Mode?

Capacity consistency, ban upper limit consistency.

How to Count the Number of Rules in NAT Boundary Firewall and VPC Firewall Instances?

Number of rules issued = number of source addresses × number of destination addresses × number of ports × number of protocols.

- Number of access source and destination addresses: Each IP/IP range and asset type counts as 1. Asset groups, asset tags, and templates are counted based on the number of addresses after splitting.
- Number of destination ports: Counted as separate entries if separated by commas; counted as 1 if no commas are present.
- Number of protocols: Layer-4 ANY counts as 3, layer-7 ANY counts as 6. HTTP/HTTPS or SMTP/SMTPS count as 2, a single protocol counts as 1.

Added DNAT Rules on NAT Gateway Automatically Sync to NAT Boundary Firewall?

Before creating a NAT boundary firewall instance, rules added on the NAT gateway will automatically synchronize DNAT rules to the firewall after enabling the firewall switch. However, rules added on the NAT after creating the firewall will not take effect after synchronization. Therefore, users are advised to manually add them on the CFW console.

After Shutting Down or Terminating the NAT Boundary Firewall, Will the DNAT Rules Be Automatically Synced to the NAT Gateway?

After the NAT firewall is destroyed, the DNAT rules added by users on the CFW console will be synchronized to the NAT Gateway by the firewall. If the NAT Gateway is reconnected to the NAT firewall, the DNAT rules previously created on the firewall will not be automatically synchronized back to the NAT firewall.

Will NAT Boundary Firewall/VPC Firewall Engine Updates Notify Users?

If the engine is updated, a prompt window will pop up in the console; each engine version will be prompted only once.
Users can go to the Firewall Switch > **NAT Boundary Switch** page, click **Engine Update** under the firewall instance tab to check whether the engine is to the latest version.

What Impact There Will Be If NAT Boundary Firewall Bandwidth Exceeds the Limit?

Bandwidth overage will trigger traffic throttling. The result of throttling may increase network delay. Access timeout after connection may cause packet loss. It is advisable to scale out bandwidth in time.

If VPC1, VPC2, and VPC3 Each Exclusively Use IPs and All IPs Are Exhausted, Which IP Will the Unbound VPC Use?

If there is only one non-exclusive IP left, the exclusive IP feature cannot be used, and the remaining IP is not allowed to be selected as exclusive.

NAT Boundary Firewall Configured a Full Blocking Rule Last with No Access Rules Before, curl and ping Tests Were Normally Intercepted, Why Can telnet Test Pass?

Access control rules include configuration of layer-7 rules that will be allowed, because layer-7 rules need to be detected. All traffic must first pass through TCP three-way handshake, so telnet can work here.

Inter-VPC Firewall

Last updated: 2025-05-20 14:43:05

Why Can'T the Firewall Switches between Some VPCs Be Turned On?

Due to routing and IP range conflicts and other reasons, CFW restricts the switches that cause conflicts. You can eliminate the conflicts according to the switch error prompts before trying to enable the inter-VPC firewall.

What Is the Automatically Created Firewall Subnet in VPC and the Firewall Route in the Route Table?

After the inter-VPC firewall switch is enabled, the firewall subnet and firewall route required for traffic redirection will be automatically created. Do not attempt to manually delete them to avoid affecting the use of CFW. If you wish to change the firewall subnet segment, you can submit a ticket to contact us.

Which Subnets' Traffic between VPCs Is the Inter-VPC Firewall Responsible for Diverting?

The traffic diversion range of the inter-VPC firewall depends on your routing configuration between VPCs. CFW only performs traffic diversion operations on subnets with correctly configured inter-VPC routes.

What Impact There Will Be When the Bandwidth of the Inter-VPC Firewall Reaches the Specification Limit and How to Handle It?

In the current version, since the inter-VPC firewall adopts a deployment mode of using exclusive resources for users, elastic scale-out is not currently supported.
Therefore, when the bandwidth of the inter-VPC firewall exceeds the capacity specification, the firewall will drop the part of data packets that exceed the bandwidth, which may lead to network delay, congestion or blockage. For the normal business operation of your service, it is recommended that you reasonably estimate the bandwidth specification and expand the firewall bandwidth in advance.

Can the Inter-VPC Firewall Protect Against Traffic From External VPC Visits?

Protection can be carried out through the CCN mode of the inter-VPC firewall.

What'S the Maximum Bandwidth Supported by the Inter-VPC Firewall?

20G.

Does the Inter-VPC Firewall Support Blocking UDP?

The VPC firewall is serial in the user network, actually changing the customer routing, and can block all UDP traffic.

Can the Inter-VPC Firewall Cover the Protection between VPN and Dedicated Lines?

Supported. Need to pass through purchasing CCN to get a connection.

Why Split Inter-VPC Firewall Instances?

A firewall is essentially composed of multiple firewall instances. In previous versions, the concept of instances was weakened, making it difficult to monitor and analyze the status of each firewall instance. Therefore, in the latest version, we have strengthened the concept of firewall instances, aligning their information hierarchy with that of the NAT firewall, making the interface structure clearer.

What Problems Does Intra-Region Multi-Instance Solve?

In previous versions, we would deploy a firewall instance in each region to achieve network access. However, due to routing strategy limitations, effective protection cannot be achieved when there are too many VPCs.
Currently, the inter-VPC firewall supports deploying multiple firewall instances (Virtual Private Cloud mode) in the same region, thereby achieving protection for more VPCs.

What Pain Points Does the Configuration of Routing Mode Solve?

Due to different network structures of different users, the quantity of switches becomes complex and difficult to maintain when the quantity of VPCs is excessive. Through flexible selection of single-point mode, multi-point mode, fullmesh mode, and custom routing mode, users can choose appropriate traffic diversion schemes according to the network topology, thereby simplifying switch control logic.

CCN Mode Whether VPC Wall Supports Adding New Firewall Deployment Regions after Access?

Not supported. If you want to add a new deployment region, you need to terminate the instance and rebuild it.

What Is the Blocking Logic of CFW Configuration Against UDP Parse Requests on Port 53?

When an ACL interception rule is triggered, the CFW will forge a DNS response packet, that is, the CFW will send an NXDOMAIN response packet on behalf of the DNS server to block DNS requests. This is to prevent blocked DNS requests from retrying and passing through. If it is necessary to allow DNS requests, it is recommended to place the DNS bypass rules at the frontmost in the configuration. This configuration will cause the DNS server specified in `/etc/resolv.conf` not to attempt to request resolution from the next address.

Functionality
Traffic Center

Last updated: 2025-05-20 14:43:34

What Is the Specific Delay Time of the CFW Traffic Bandwidth Graph?

Generally, there is a delay of 1 minute.

How Often Does the Traffic Center Update? How Often Do Traffic Logs Update?

The traffic center list updates every 10 minutes. The traffic log updates in real time.

CFW Traffic Peak Mismatch?

- The traffic chart displays the average bandwidth. Among them, the average bandwidth refers to the average within the statistical time scale.
- The peak value is calculated based on the traffic statistics collected within 10 seconds. The average traffic of a single IP is reported every 10 seconds, and the maximum value within a certain time range is taken as the peak value.
- Alarm and billing are both based on the traffic statistics seen on the page.

Why Do Some Traffic Logs for Requests to Destination Port 443 Not Contain Domain Information?

1. TCP handshake is incomplete or fail to establish connection.
2. Failed when accessing the domain name.
3. Client request does not carry SNI.

Traffic Analytics of CFW. in Which Regions Is VPC Deployed? Whether Proximity Analysis Is Adopted?

Currently deployed only in the Guangzhou region. In fact, based on the business requirements of customers, a cluster is set up in each region for nearby processing.

What Is the Maximum Traffic Analysis Capacity of CFW NDR? What Is the Performance Limit of the Traffic Diversion Private Link?

The performance ceiling of Private Link has not reached the theoretical value. The actual limit depends on the private network bandwidth of the server.

How to Determine Whether the Traffic Is Private Network Traffic or Public Network Traffic? How to Determine the Traffic Imported From Other Clouds Via Dedicated Lines?

Make a type judgment based on the IP type of the source address. Since the customer VPC connected by the dedicated line belongs to the private network, this traffic is therefore identified as private network traffic.

If Most Traffic Is HTTPS, Are the Rules of the Intrusion Defense Engine Passed in for Traffic Analysis Still Valid?

Intrusion prevention rules also include rules effective against HTTPS, especially those for vulnerability type traffic, which can match features through regular expression matching. Therefore, some alerts can be detected even for encrypted traffic.

What Is the Log Size of Traffic Analysis Records?

The maximum record of a single session is 1000 bytes. In fact, the data is compressed, and not all transmitted packets are recorded.

Access Control

Last updated: 2026-03-12 10:55:44

What Is the Default Rule of CFW When No Rules Are Configured, to Allow or Block?

CFW releases all traffic by default. When you turn on the CFW switch, CFW will start logging traffic and generate intrusion prevention alarms, but since no rules are configured, no traffic will be blocked at this time.

How to Configure CFW to Allow Access Only to Released Ports?

1. After enabling the Internet Firewall, click to select Access Control > **Internet Boundary Rules** > **Inbound Rules** to enter the inbound rules page.
2. On the inbound rules page, click **Add Rule** to allow the ports you need. Then, add a rule to block all ports.

> **Note:**
> Internet Firewall allows all traffic by default when no rules are configured.

How Long Does It Take for Access Control Rules to Take Effect after Configuration?

When you configure CFW rules, it takes about 10 seconds to 1 minute for the rules to take effect.

Does Cloud Wall Support Performing Access Control through a Domain Name?

Both Internet Firewall and NAT firewall support using domain names in outbound rules. The inter-VPC firewall also supports domain name access control rules.

Can CFW Support Configuration Limits through a Domain Name?

Currently, assets in Chinese mainland and Hong Kong (China) support configuring restriction policies through domain names.

Does CFW Have a Regional Blocking Feature?

Premium Edition and above have the Geo-blocking feature.

What Are the Causes for Being Unable to Select Part of the Address Templates When Adding Inbound Rules in CFW?

Neither inbound access sources nor access destinations can choose a domain name template. Outbound access sources cannot choose a domain name template, but access destinations can. This is because inbound sources cannot be domain names.

Differences between Access Control of CFW and Features of Security Groups in VPC

The security group functionality of VPC is limited and usually used for setting up allowlists for specific services of servers. It is recommended to use the enterprise security group of CFW, which supports intelligent algorithms to unify deployment strategies.

Does Cloud Firewall Support Protection for the UDP Protocol?

The NAT boundary firewall, enterprise security group, and inter-VPC firewall support UDP protection. The bypass wall of the Internet boundary does not support it.

How Many Entries Can NAT Firewall Rules Be Expanded To?

It can be expanded to 20,000 entries.

Why Does the Alert Center Still Generate Rule Entries for Observation after the Internet Edge Firewall Is Configured to Forbid Access From Overseas Regions?

1. If no corresponding block request is found in the ACL log, it is required to check if there are other bypass rules with higher priority.
2. If the corresponding block request is recorded in the ACL logs, this is likely due to the bypass preemption mechanism. If you are concerned about this issue, you can manually ban all attack alerts from outside Chinese mainland in the Alarm Center.

Why Do Some Requests Still Show in the Alarm Center and Are Not Blocked after Configuring Access Control Rules?

- It might be that the access control rule is not effective yet.
- Under the condition that the access control rule is in effect, it may be caused by the bypass packet loss phenomenon of the Internet edge firewall. The bypass firewall analyzes the mirrored network traffic. Some of the traffic may be matched by the intrusion prevention system and generate an alarm, but in fact these access requests have already been intercepted.

Does the Access Control of CFW Support Configuration of a Specific Effective Time Period?

It is recommended to select **Automation Tool** on the Common Tools Page to configure the effective time of rules, and configure the enablement and deactivation time of rules according to specific scenarios. For details, please refer to Add Automation Task.

What Are the Usage Limitations of Enabling Persistent Connection Access Control for the NAT Firewall?

1. Keep the engine up-to-date. It is recommended to perform an update. For details, see Firewall Engine Upgrade.
2. The maximum number of connections is limited by the bandwidth specification. For details, see Firewall Common Issues.

What Should Be Done If the IP Resolved by the Obtained Domain Name Conflicts with the Existing IP Rules?

Rules with relatively high processing priority.

Can an Attacker Bypass by Changing the host after the Cloud Firewall Domain Name Limiting Rule Is Issued to an IP?

CFW intercepts based on IP rules generated by authoritative DNS resolution. The modification of local host by attackers does not affect the rule effectiveness. Therefore, it cannot be bypassed.

Zero Trust Operations and Maintenance

Last updated: 2025-05-20 14:44:06

Relationship between iOA and CFW?

- Billing relationship: The CFW zero trust operations and maintenance package is sold in a federated sales mode and comes with iOA SaaS version, including all features of iOA basic package. You can go to iOA console to view and use it.
- Functional relationship: By deploying iOA in the user's office network, an identity-based zero trust security system can be built. The firewall can perform authentication and access control based on the office network identity authentication system by obtaining iOA's identity, bringing a more coherent and convenient Ops experience. Perform asset access in the CFW console. There is no need to go to the iOA console to perform operations such as deploying connectors, accessing assets, and allocating permissions, saving your time for manual deployment and improving deployment efficiency.

Role of Regional Primary and Secondary EIPs?

- Function of EIP: In the zero trust security system based on iOA, a public network EIP is needed to communicate with the iOA security gateway when operating and maintaining private network assets. CFW integrates the iOA connector. Without manual deployment, you only need to select EIP binding.
- Primary and secondary EIPs: A region supports binding up to two EIPs, and two connectors can be built to implement a primary/secondary disaster recovery configuration.

Does Integration Have an Impact on the Network?

CFW asset access will only connect the data link between assets and the office network. Regarding office network access to authorized resources, it is equivalent to adding an identity verification gateway, which has no impact on the network. The access operation will create a subnet with a 29 IP range in your corresponding VPC for traffic diversion.

What Are the Identity Perspective and Rule Perspective?

Zero trust operations and maintenance use the allowlist form at the underlying layer, that is, configure an access control allowlist based on identity and assets. Presented in the form of rules, it is the rule perspective.
The identity perspective is aggregated based on allowlist rules and the resource permissions corresponding to the identity. Query or configure the owned resource permissions from the

identity perspective to facilitate your configuration.

Which IPs' Ports Will Be Forbidden after Enabling the "Disable Port" Functionality in WeChat Remote Ops?

Once enabled, Internet Boundary Access Control Rules and Enterprise Security Group Rules will be automatically distributed to block all Internet access from public IPs to asset login protocol ports. This instruction only takes effect on public IPs with the Internet boundary switch turned on.

> **Note:**
> If the login protocol port of the asset is modified after the "block ports" feature is enabled, you need to re-enable the "block ports" feature once.

Will the Login Protocol Port of an Asset Be Banned If the Internet Boundary Switch of the Asset Is Disabled?

Will not be banned.

Why Is There No Prompt to Enter the Resource Password after Scanning the Code for Authorization When Secure Access Control Is Configured?

Please check whether the default port of your resource machine has been modified. If it is not port 22 or port 3389, go to Access Control > **Identity Access Rules** > **Instance Management** to modify it.

Support Weixin Authorization for Remote Desktop of Windows?

It is supported.

Garbled Characters When Using cmd for Remote Ops in Windows?

Execute the chcp 65001 instruction or scan the QR code provided at the bottom of cmd to log in.

Intrusion Prevention Basic Defense

Last updated: 2025-05-20 14:51:34

What Traffic Will Be Checked by the Intrusion Defense Module?

The current version of the Internet edge firewall, NAT boundary firewall, and inter-VPC firewall all support intrusion prevention. Whether intrusion prevention is supported is subject to whether the intrusion prevention switch is on in advanced settings.

Which Events Will Be Intercepted When the Protection Mode of Intrusion Defense Is in Interception Mode?

In interception mode, the firewall will intercept traffic based on the following features.

- Threat intelligence: Automatically intercept high-confidence network attacks/malicious access, and support automatic interception of outbound malicious access.
- Basic defense: Automatically intercept some rules with high confidence, and still generate a security event alarm for other rules.
- Virtual patching: Automatically intercept all traffic detected as vulnerability exploits.

How to Manually Block the Risks in the Alarm List? Can You Add Block IPs by Yourself?

For risks with a high number of alarms or high danger level in the alarm list, users can manually perform interception. Meanwhile, users can import the IP information to be intercepted into the blocklist of intrusion prevention by themselves. When this IP accesses, it will be directly blocked by CFW.

Interception Mode: in What Situations Will Interception Be Automatic? Why Are There Still Warnings When the Interception Mode Is Enabled?

- In interception mode, CFW will automatically intercept high-confidence risks and IPs in the blocklist.
- Trigger an alarm for risks with low confidence, not automatically intercept. Users can manually intercept the alerted IPs in the Alarm Center.

How Is the Interception of Malicious IPs Performed in Strict Mode?

In strict mode, threat intelligence, basic defense, and virtual patching are all in global interception mode, and any IP that generates an alarm will be intercepted. IPs with high-

confidence risks and those in the blocklist will be intercepted on their first visit. Other malicious IPs will be directly intercepted on their second visit after an alarm is triggered on their first visit.

Why Isn'T the Malicious IP Blocked?

The intrusion prevention feature of CFW is session-based and will only intercept access sessions with attack patterns. If the user does not add the IP to the blocklist, the normal access sessions of this IP will not be intercepted.

When to Enable Interception Mode?

Generally, switch from alarm observation mode to block mode. There is no change in the business. Observe for 1 – 2 days and then enable it continuously.

Is the Policy Accurate? What to Do If Directly Enabling Interception and Blocking Affects Business?

In the intrusion prevention module, the system can only set highly accurate rules to interception mode. Especially, there have been no false alarms for virtual patches yet. If any problem occurs after enabling blocking, you can contact us at any time for related help.

Will the Communication between Cloud Intranet Addresses Be Affected after CFW Interception Mode Is Enabled?

- If you enable the interception mode of the Internet edge firewall and NAT boundary firewall, the CFW will only protect north-south traffic. The east-west traffic associated with these switches will not pass through the firewall.
- If you enable the interception mode of the inter-VPC firewall, CFW will check and intercept east-west traffic, which may affect the communication of private network addresses within the cloud.

What to Do If an IP Is Misintercepted by Intrusion Defense?

1. Log in to the CFW console, click **Log Audit** > **Intrusion Prevention Log** to query whether there are clear interception records for the source or destination IP.
2. When encountering an emergency, you can enter Intrusion Defense, **disable "Enable Blocklist", disable the blocklist, and enter Alert Center > Blocked Interception Statistics** to view all interception statistics and troubleshoot and locate the interception source.
3. After locating and fixing the fault cause, you can toggle on the "Enable Blocklist" switch to re-enable this feature.

How to Quickly Locate and Restore Access in Case of Misinterception or Inaccessible Situation?

- If the firewall switch for the public IP is modified to disable, the traffic will not pass through CFW.
- Change IPS to observation mode and confirm that it is not caused by IPS interception.
- Policy configuration is set to any, meaning the public IP has full access. Confirm that it is not caused by CFW policy.

> **Note:**
> If the issue persists after completing the above steps, please submit a ticket.

Why Has the IP Previously in the Blocklist of Intrusion Defense Disappeared?

1. In the blocklist, when the effective time of one IP expires, the list will automatically delete the IP. At this point, subsequent traffic access of the IP will not be intercepted by the firewall.
2. To avoid the blocklist automatically removing IPs that pose security risks, you can click **Edit** in the operation column on the right side of the list to modify the expiration time and date of the IP to be operated.

Will IPs in the Ignore List of Intrusion Defense Still Be Intercepted?

IP addresses in the ignore list will bypass the IDPS feature directly.

How to Configure to Ignore a Certain Designated Detection Rule Against a Certain IP?

Ignore operation for detecting a specific rule is not supported currently.

When Will the Traffic for Resolving Domain Names Not Transit through CFW?

- Tencent Cloud CVM may use Tencent's self-built DNS resolving service. Generated DNS messages will not pass through the Internet boundary, therefore causing missing alarms and logs for that part of the domain name access.
- If you want a CVM to have normal usage of CFW's domain name detection and alarm features, you can manually change the resolution address in the /etc/resolv.conf file to 8.8.8.8.

Relationship between Intrusion Defense and Access Control?

- CFW determination order: **Blocklist** > **Access Control Rule** > **Allowlist** > **Intrusion Prevention Rules**.
- The intrusion prevention feature only takes effect on assets with the firewall switch enabled. Traffic of assets with protection not enabled will not be processed by the firewall.

Defense Strategies

Last updated: 2025-05-28 10:56:15

Which Types of Traffic Can Be Automatically Intercepted in the Interception Mode of Threat Intelligence?

Enable the threat intelligence interception mode. The NAT boundary firewall will automatically intercept Threat Intelligence Alarms in the outbound direction, while the Internet edge firewall and inbound direction remain in alarm observation mode.

Virtual Patch Interception Mode Supports Automatic Interception of Which Types of Traffic?

Enable the Virtual Patch Interception Mode. The Internet edge firewall will automatically identify vulnerability exploits and vulnerability attacks in all internet boundary traffic and automatically intercept connections for alarms.

What Are the Differences between the IPS Virtual Patch of Cloud Firewall and the Patch of Cloud Workload Protection Platform?

- Patches on the host are generally released by the official. The official's patch release time is relatively lengthy, often taking several weeks or even months to fix, and some require restarting the CVM.
- The IPS virtual patch on the Cloud Firewall is a defense rule updated in real time in the Cloud Firewall IPS system based on the exploit characteristics of vulnerabilities. It can achieve hourly-level updates without requiring any modification to the business or restarting the business system.
- The IPS virtual patch of the Cloud Firewall, combined with the cloud workload protection platform (such as CWPP), achieves stereoscopic defense at both the network and host levels. This is an effective combination for host security protection.

Do I Still Need to Apply Host Patches with Virtual Patches?

Yes, it is still necessary. The virtual patch can provide frontline protection for you, but the fundamental vulnerability still needs to be thoroughly resolved to achieve the safest outcome.

How Is the Danger Level of Corresponding Rules for Intrusion Protection Defined?

- The danger levels of basic defense and virtual patching are defined based on the potential damage that this attack may cause.

- The danger level of threat intelligence is defined based on the attack threat level that this IP or domain name has generated in our historical big data.

How Is the Review Mechanism for Updating Intelligence Packages Based on Threat Situations of CFW?

Intelligence is divided into high-precision intelligence packages and prioritized protection packages, with the following features:

- High-precision intelligence packages have a complete false positive reduction process.
- Prioritized protection packages target critical protection scenarios, mainly for non-real IPs, and are only used in strict mode. Interception/observation modes are not enabled by default.

Intrusion Defense Virtual Patching, Can It Identify Shiro Vulnerability Traffic?

It can detect, but may not cover all scenarios, because some are encrypted traffic.

CFW Supports Protection Against Which Vulnerabilities?

For details, go to **Intrusion Prevention** > **Intelligence Center** to search and view.

How Does a Firewall Judge a Web Attack?

External hackers bring attack patterns when scanning and sniffing. For example, with the weblogic vulnerability, the firewall will identify an attempted attack when detecting the attack pattern.

Authentication Protection Against Brute-Force Attacks, Which Protocols Are Supported?

Support the following protocols: MySQL, Oracle, SSH, Redis, MongoDB, IMAP, POP3, FTP, SMTP, SQL Server, and RDP.

Handling Existing Mining Attacks

- No CWPP purchased, reinstalling the machine is not necessarily required, manual virus killing is sufficient, mining indicates an infected state.
- If CWPP has been purchased, it can be used directly to eliminate threats.

Alert Center

Last updated: 2025-05-20 14:52:31

Has the Alarm Information of the Security Baseline Disappeared?

The number after the alarm type indicates the number of unprocessed alarms in the current list (the total number of alarms will be shown for BOT attacks). If the corresponding security baseline alarm switch is not enabled, the console will not show the security baseline options.

Why Ban after Interception?

Intrusion prevention testing for network attacks is session-based. Only when an IP is blocked (added to the blocklist), all its access operations will be intercepted.

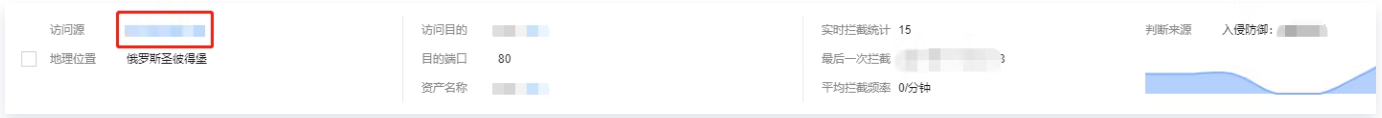
What to Do If You Want to Modify after Performing Operations on an Event?

Log in to the CFW console, enter the Intrusion Defense module, and you can remove items from the "Blocklist" or "Ignore List".

How to View the Threat Profile of an IP?

- In security event alarms, you can refer to viewing the threat profile in security event alert - event details.

- In block interception statistics, you can directly click IP to navigate.



Red Exclamation Mark Appearing on the Right of the IP Address?

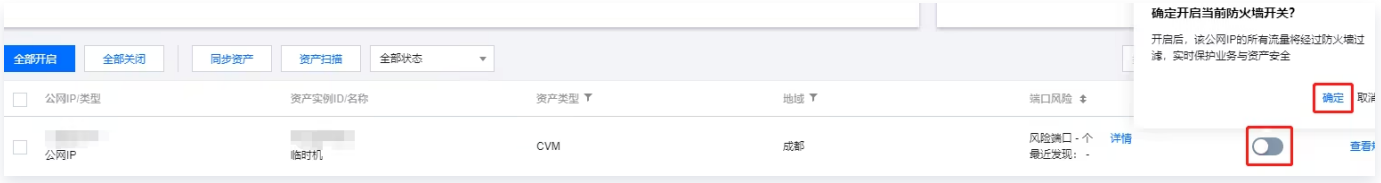
This IP might be a Tencent Cloud CDN address. We do not recommend that you manually block or ban it. If you have enabled the intrusion prevention interception mode, CFW will automatically intercept attack traffic originating from this address. We will allow normal traffic. Please rest assured.

How Often Is the Alert Center Data Updated?

The alert center data is updated every 10 minutes.

What Operations Are Required after Purchasing CFW for the Alert Center to Have a Traffic Trend Chart?

1. On the Firewall Switch page, select the corresponding instance and click **Firewall Switch** > **Confirm** to enable the firewall switch.



2. After the firewall switch is enabled, the access control of CFW defaults to full connection mode, and the intrusion defense defaults to observation mode. Therefore, it has no impact on the business system.

Why Can'T You See Data in the Blocking Statistics in the Alarm Center?

1. Please confirm whether you have enabled the corresponding firewall switch and set the blocking or interception mode.
2. Select all policies under Blocking Statistics and check if the corresponding event is visible.
3. If you are still unable to view the corresponding event, please contact us for further verification. Thank you for your understanding and support.

Can I Still Receive Bandwidth Alarms When Not Selecting the Root Account and Sub-Account in the Alarm Object Settings in the Alert Center?

If the root account and sub-account that receive alerts are not selected, you will not receive SMS, Message Center notifications, or WeChat notifications from the alert center, but the console will still display the alerts.

Why Cannot the Threat Intelligence Alarm Generated by the Alert Center in Firewall Interception Mode Perform the Ban Operation (Displayed As Gray)?

The current Internet Bypass Firewall does not support the blocking feature for UDP protocol. Please verify whether it is UDP protocol.

Firewall Has Set Up an Alarm, but Inbound Attack Behavior Based on TI Did Not Trigger an SMS Alarm. Is This Normal?

Normally, only outbound attack behavior will trigger Threat Intelligence Alarms. Alerts against inbound direction from threat intelligence are generally of low severity, so they will not trigger features such as alarms and regions.

Why Are Events of Automatic Blocking Also Displayed in the Firewall Alert Center?

The processing process is to report alarms and then handle them. When an attack is first detected, the system will report alarms and automatically dispose of it, that is, add it to the blocklist. When an attack is detected for the second time, the event will be intercepted and recorded in the interception statistics.

What Are the Causes for Alarm Events in the Firewall Alert Center Not Being Displayed in Real Time?

The Alert Center is mainly used for report statistics and log aggregation. There is usually a delay of 15–20 minutes.

In the Attack Alert Summary, What Are the Alarm Events Tracked and Summarized Based On?

For alarms on the same day, when the source and destination IPs and matched rules are the same, the Alert Center will aggregate events of up to 50 ports with inconsistent ports into one alarm event. It should be noted that: inbound alarms from threat intelligence will aggregate the assets of the destination IP together (as shown in the figure below).

How to Change the Number of Compromised Hosts From 1 to 0 after Handling Alarm Events Related to Compromised Hosts in the Alarm Central?

Ignore warning events so that the count can be adjusted to 0. If necessary, block attack IPs by adding ACL rules in Intrusion Prevention – Blocklist.

If you add the IP to the blocklist again after ignoring it, the count of compromised hosts will become 1 again.

Why Is There No Data When Viewing Line Charts of Attack Alerts Other Than Those in the Last 7 Days in the Attack Alert Statistics in the Alarm Center?

The statistical curve of attack alerts in the Alert Center only counts the data of the last 7 days.

Security Baseline

Last updated: 2025-05-20 14:52:56

What Is the Security Baseline of CFW?

The security baseline refers to a preliminary IP address or domain name access list that the CFW forms by observing the traffic access status within a certain time range. Users can maintain the baseline list by adding or deleting IP addresses or domain names based on the security score, associated security events, and network access status, thereby forming the final security baseline.
After the security baseline is set, any newly-added IP address or domain name access outside the baseline will trigger a security alarm. Users can handle IP addresses or domain names in the alarm list. The security baseline is applicable to traffic baseline protection during the critical maintenance period.

Why Is the Baseline Inspection Time Grayed Out and Unable to Select?

You can check the status of tasks for the above baseline score. The baseline check time is not selectable when the baseline is in learning status.

- Baseline learning time: Statistical data added within the baseline time to the baseline end time.
- Baseline check time: Statistical data added from the baseline time to within the current time range.

Log-Related

Last updated: 2025-05-20 14:53:15

How Long Is the Default Storage Time for CFW Logs? What Is the Maximum Storage Capacity?

- CFW provides free default storage for logs within 7 days, with a maximum storage capacity of 50 GB.
- After enabling the log analysis service, CFW will provide default storage for the logs within 6 months. The storage capacity starts from 1,000 GB, and the maximum expandable capacity is 300 TB.

What Is the Relationship between Log Audit and Analytics and CLS?

Currently, log audit is built-in for CFW and irrelevant to CLS. Firewall logs can be delivered to CLS through Ckafka, convenient for users to analyze on their own.

What Traffic Does Access Control Log, Intrusion Prevention Log, and Traffic Log Record Separately?

- Access control logging hits the traffic of access control rules.
- Intrusion prevention log records the traffic that hits intrusion prevention rules.
- Traffic logs record the released traffic as well as a piece of request data of the intercepted traffic.

Can Firewall Logs Be Taken Out for Archiving?

Yes. Logs support export and log delivery function, sending to the customer's kafka.

How to Download Logs?

- You can use the log delivery feature to forward logs for analysis (premise is purchasing Tencent Cloud message queue Ckafka instance). For configuration reference, see Log Analytics.
- Or log in to the CFW console, click on the left operation bar **Log Audit** > **Traffic Log** to enter the Traffic Log page, click in the upper right corner , and you can download the log.

> **Note:**
> Export based on current retrieval conditions. Support exporting up to 1 million logs. Enjoy a certain export limit per month.

How Long Does It Take for Log Delivery to Be Successful?

It takes about 1 minute to deliver logs. Therefore, related logs will be updated with a slight delay.

Do the Delivered Logs Have Tags to Mark the Log Type?

There are no tags in the logs to identify the log type. It is recommended that you select different topics when delivering logs to distinguish different logs.

Interception Mode Is Enabled. Why Do Observation Types Still Appear in Logs?

Virtual patching is automated interception. If there is a vulnerability attack in an intrusion and it hits the virtual patch, it will be automatically intercepted. Basic rules support automatic interception of high-confidence basic rules. If basic rules are not high-confidence, they will not be intercepted.

Will Traffic Logs Record the IP Traffic Logs Intercepted by Access Control Rules or Intrusion Prevention?

Traffic logs record the released traffic as well as the request packet information of the IP traffic intercepted by access control rules or intrusion prevention.

Will the Intercepted Attacks Generate Logs?

- Access Control Rule: Intercepts access data in blocking mode, logs the number of rule hits, and simultaneously logs access control.
- Intrusion Detection: Generates intrusion detection events when hitting an intrusion detection policy. Confirm the specific interception logs by log analysis.

How to Check Whether the Accessed/Attacked Delivered in Logs Is Blocked or Allowed?

The strategy field identifier in logs indicates whether the access is blocked or monitored.

> **Note:**
> The traffic log has no field value of strategy.

Account-Related

Last updated: 2025-05-20 14:53:35

Can CFW Be Used by Other Tencent Cloud Accounts?

CFW cannot be used under another account. CFW can only protect cloud assets under the current Tencent Cloud Main Account.

Does Role Creation Authorization Impact Business Proceeding Normally?

No. Creating role authorization allows the CFW backend system to read your cloud resources, Virtual Private Cloud (VPC), subnets and other data through user authorization. It is used to present the data required for building the page and performing operations, and no automated operations that affect business will be performed.

Alert Center Setting Alarm Objects Without Selecting Root Account and Sub-Account, Can Bandwidth Alarm Be Received?

If the root account and sub-account that receive the alarm are not selected, Short Message Service (SMS), Message Center and WeChat notifications from the alert center will not be received, but the console will still display the alarms.

How to Authorize Cloud Wall Permission to a Sub-Account?

You need to create a CFW role in the CAM role first, and then add the following 6 permissions in the sub-account.

- QcloudCFWFullAccess
- QcloudSSAFullAccess
- QcloudVSSFullAccess
- QcloudCWPFullAccess
- QcloudAccessForCFWRole
- QcloudCamSubaccountsAuthorizeRoleFullAccess

CVM Overview Page Cannot Be Opened, Prompting you Do not Have Permission to perform This operation, Failure Information Description: you are not authorized to perform operation (cfw:DescribeCfwUserStatus)?

This detailed permission has not been added to CAM yet. Temporarily configure the following permissions for this sub-account:

- QcloudCFWFullAccess

- QcloudCFWReadOnlyAccess

Billing

Last updated: 2025-05-20 14:53:55

Does CFW Support Configuration Modification?

CFW can enhance the purchased configuration through scale-out. Temporarily, it does not support autonomously reducing the purchased version configuration.

Can CFW Be Renewed Upon Expiration? Will the Resource Be Reclaimed Upon Expiration?

The usage period of CFW can only be selected when purchased. After expiration, the service will automatically suspend. If you need to continue usage, you can repurchase it, which will not impact your business.

- You can restore the configuration information if you renew the product within 14 days upon expiration.
- Upon expiration for 14 days, the system will reclaim all CFW resources and they cannot be restored. You can only purchase again and reconfigure.

How Many CFWs Can an Account Purchase?

An account can purchase a CFW. Currently, CFW provides three paid versions, which are advanced edition, enterprise edition and flagship edition, respectively.

Is It Possible to Get a Refund for CFW?

The cloud firewall product complies with Tencent Cloud Instruction on Refunds for Cloud Services. If you are not satisfied with the cloud firewall after purchase, we support unconditional refund within five days. If you need a refund, please submit a ticket to contact us. No refund is supported if the product has been used for more than five days.

Others

Last updated: 2025-05-20 14:54:13

Will Public Network Assets Be Auto-Identified on the Overview Page? How to Achieve It?

It will auto-identify. It is actually through Tencent Cloud api and CAM authorization to get these; all assets under this account are enumerated by Cloud api.

How to Set to Enable Observation Mode and Temporarily Not Block after Turning on the Firewall?

Just turn on the public network IP firewall switch. After enabling the firewall switch, it is in alarm observation mode by default. It is unnecessary to configure the access control list (ACL). Access control is default to all-allow.

Where Do I Need to Confirm If the IP Is Blocked by CFW?

- Log in to the CFW console, and click on **Log Audit** > **Intrusion Prevention Log** and **Access Control Log** modules to check if the IP has been blocked by CFW.
- In addition, on the Alert Center > **Attack Interception Statistics** page, you can query the interception work performed by CFW in the intrusion prevention module.

How to Check the CFW Version?

You can view the package version and expiration date of the current account in the upper left corner of the Overview Page.

Can CFW Limit Based on MAC Address?

CFW does not impose restrictions based on MAC addresses. The cloud network isolates Layer 2, and IP addressing is the only option. CVMs communicate not via ARP but through IP addressing.

Can I Adjust or Disable the Cloud Firewall Bandwidth Alarm Threshold?

Bandwidth alarm is an important indicator of CFW. Exceeding the bandwidth will make it unable to protect the traffic of the exceeded portion. You can adjust the first and second-level alarm thresholds in the console. It is not supported to disable them.

Will the Switch, Scale-Out, Adding CAM Authorization, and Intrusion Defense Switch of CFW Affect Business?

- Turning on the Internet edge firewall will not have an impact on the business; turning on the NAT firewall and VPC firewall will cause a 1–2s momentary disconnection to the Cloud Connect Network (CCN). It is recommended that you perform this operation during the non-peak period of the business.
- Scaling of the Internet edge firewall will not have an impact on the business; scaling of the NAT firewall may incur a 1–2s momentary disconnection. Please submit a ticket for consultation.
- Scaling of CFW, switching on/off of intrusion defense, and addition of CAM authorization will not affect business.

Configured Recipients in the Message Center but the Configuration Has Not Taken Effect?

- If you have configured recipients in the message center but still haven't received message pushes or there is content inconsistency with the configuration, it may be because Notification Settings > Message Center Subscription Settings is not enabled.
- CFW will, by default, push non-subscribed messages, based on the recipients and content in Notification Settings. If you need to enable message center configuration, please turn on Notification Settings > Message Center Subscription Settings.