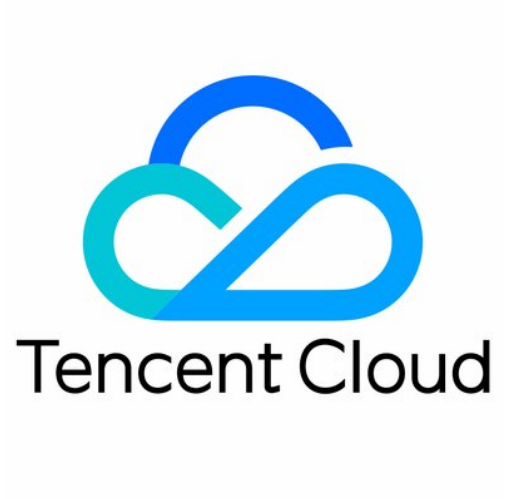
Tencent Cloud Firewall

FAQs

Product Documentation



Contents

FAQs
Basic Introduction

Last updated：2023-12-11 16:57:31

What is Cloud Firewall?

Tencent Cloud Firewall (CFW) is a SaaS firewall based on the public cloud environment that provides network perimeter protection and addresses security and management needs for unified access control and log audit. In addition to the features of traditional firewalls, CFW supports multi-tenancy and elastic scaling and is an essential network security infrastructure for cloud migration.

Can CFW protect assets not running on Tencent Cloud?

No. CFW only protects IP assets under Tencent Cloud accounts.

What's the difference between CFW and security group?

Cloud Firewall and Security Group are standalone systems. When the Internet service is enabled for a public EIP, traffic is allowed only when it is allowed by the policies of both systems.
Control scope of the two systems is different. Edge firewall controls the access traffic of public IP addresses, while security group controls all traffic of CVM NIC.
Application scope of the two systems is different. Security group is applied to instances, while CFW is applied to public IPS, NAT edge protection, and peer connections or CCN between VPCs.
Security group ACL is the most fundamental feature of CFW, and its more important capabilities are log audit of full traffic and real-time interception of Intrusion Protection System (IPS).

What's the difference between CFW and WAF?

Web Application Firewall (WAF) only protects web services and prevents attacks from outside to inside. It does not monitor or prevent malicious outgoing access of services.
CFW protects all services. It not only provides basic prevention from web vulnerabilities, but also supports detection of outgoing access from inside to outside. In addition, CFW will automatically intercept compromised servers and malicious outgoing access.

Can CFW protect CDN or COS?

No. CFW does not protect SaaS services such as CDN, COS, high defense IP, SaaS-WAF, and CDB, except for database services.

Does traffic go through CFW before other products? Does CFW protect CDN traffic?

IP addresses of CDN nodes belong to corresponding CDN carriers, which are beyond the protection scope of CFW. Only CDN traffic that goes back to CLB or CVM will be detected by CFW. High defense IP that goes back to CLB will also go through CFW, with back-to-source addresses of these IP nodes displayed.
For the current version, only the BGP IP address type is supported. The IP addresses of China Mobile, China Unicom, and China Telecom are not supported currently. CFW will automatically ignore the IP addresses of China Mobile, China Unicom, and China Telecom during identification of user assets.

Does CFW have QPS limitations?

CFW is a SaaS service without limitations on concurrency, creation, and QPS of traditional firewalls. Actual throughput is the only one performance indication of CFW.

Does external inbound traffic go through CFW or WAF first?

For inbound traffic

SaaS-WAF and CFW work together as the overall perimeter protection layer for cloud security. WAF offers protection for encrypted HTTPS traffic, while Cloud Firewall integrates Intrusion Prevention System (IPS), and virtual patching to protect unencrypted traffic.
SaaS-WAF and CFW work in parallel. After the traffic passes through the SaaS WAF, it does not go through CFW. For serial deployment, CLB-WAF is required. In this case, traffic goes through CFW and then CLB-WAF.
Note
Traffic that goes back to CLB or CVM will not go through CFW as well. Outgoing access of source CVM nodes can be identified and detected by using the NAT firewall.

For outbound traffic

The NAT firewall can help control outgoing requests based on CVM and control access based on domain name. With Tencent Threat Intelligence, it can automatically block any malicious IP addresses or domain names for outgoing requests.
If the NAT firewall is not enabled, access control for outbound traffic is only available with the edge firewall after the traffic goes through the NAT gateway. From the perspective of Cloud Firewall, the traffic comes from a public IP address.

Bandwidth

Last updated：2024-01-24 16:23:01

What is bandwidth? How can I select appropriate bandwidth configuration?

CFW bandwidth is independent from bandwidth of other network products. Therefore, you need to purchase CFW bandwidth separately.
NAT and CFW are independent from but connected with each other. Therefore, you need to ensure that the CFW bandwidth purchased is the same as or higher than that of NAT, so that both systems meet users' needs for bandwidth or throughput.

What is peak bandwidth? Does it refer to uplink or downlink bandwidth?

Peak bandwidth refers to the maximum bandwidth in both uplink and downlink directions. For example, if you purchase bandwidth of 100 Mbps, CFW can process traffic of 100 Mbps in both uplink and downlink directions at the same time.

Does it affect my business when the peak bandwidth is exceeded?

The edge firewall is deployed in a bypass mode, so exceeding the peak bandwidth **will not cause a packet loss or affect the traffic speed of your service**; NAT firewall is deployed in a serial mode, so exceeding the peak bandwidth will cause a packet loss. If the public network traffic is higher than the purchased CFW bandwidth, CFW **does not promise to protect the traffic beyond peak bandwidth**. Such traffic will be directly allowed to pass. Please keep your eye on CFW bandwidth alerts. In case of high bandwidth, disable the firewall toggle for some networks or expand the bandwidth to ensure normal service running.

Will the CFW edge firewall bandwidth limit the traffic?

No. CFW does not limit the traffic.

How is inbound/outbound bandwidth calculated? Will rule matching of inbound traffic be affected when the outbound bandwidth exceeds the purchased configuration?

Inbound bandwidth and outbound bandwidth are calculated respectively.
CFW does not promise to protect the traffic beyond the purchased bandwidth configuration. If only the outbound traffic exceeds the upper limit, rule matching of inbound traffic will not be affected.

Is the bandwidth of edge firewall and NAT edge firewall calculated respectively?

Yes. The bandwidth for them is calculated respectively.

Note

The bandwidth of NAT edge firewall is the same as that of edge firewall. You can expand the bandwidth of NAT edge firewall by expanding that of edge firewall.

Can I scale up or down the CFW bandwidth?

Bandwidth can only be scaled up.

Does the CFW bandwidth limit depends on the bandwidth of accessed CVM?

No. The CFW bandwidth limit is configured based on actually used bandwidth to ensure that traffic bandwidth consumed at a time does not exceed the bandwidth configuration of CFW.

Firewall
Cloud Firewall

Last updated：2024-01-24 16:23:02

What protocols does Cloud Firewall support?

Edge firewall supports TCP, HTTP, and HTTPS currently.

NAT edge firewall supports TCP, UDP, ICMP, HTTP, HTTPS, SMTP, SMTPS, and FTP.

Inter-VPC firewall supports TCP, UDP, and ICMP.

How does CFW protect UDP?

Edge firewall does not protect UDP currently. You are advised to enable both the edge firewall and the NAT firewall.

NAT Firewall

Last updated：2024-01-24 16:23:01

Will traffic coming out from a NAT firewall pass through the firewall for twice?

Yes, one for intranet IP address and the other for public IP address.

What is the difference between Create New mode and Use Existing mode of a NAT firewall?

Create New mode: If no NAT gateway is available in the current region, you can specify an instance to pass the firewall for accessing Internet by using the built-in NAT feature of the NAT firewall in Create New mode.
Use Existing mode: If a NAT gateway is available in the current region, or you want a public outbound IP address to remain unchanged, you can use the Use Existing mode to smoothly access the NAT edge firewall between the NAT gateway and CVM instance.

Can I use a NAT edge firewall to replace the existing NAT gateway?

Yes. You can use a NAT edge firewall to replace the existing NAT gateway.

Can a NAT edge firewall be enabled for a specified subnet only?

Yes. You can choose to enable the firewall toggle for the current subnet, or for all subnets in the route table associated with the current subnet.

Will the network be interrupted when a NAT edge firewall is bound with an EIP?

No. Binding will not cause a network interruption.

Will the network be interrupted when the NAT firewall toggle is turned on/off?

Enable: If you enable the NAT edge firewall feature for a specified subnet only, the system will automatically add a routing policy with the next hop being the NAT edge firewall in the current route table and disable the original routing policies. In this case, Internet traffic of the current subnet will go through the NAT edge firewall.
Disable: If you disable the NAT edge firewall feature for a specified subnet only, the system will automatically disable the routing policy with the next hop being the NAT edge firewall. In this case, this subnet will be disconnected from the Internet.

Can I configure continuous ports for DNAT?

No. It is not allowed to configure multiple ports under the same rule. Each DNAT port uses one rule.

Can I configure SNAT for a NAT edge firewall? You can perform the following operations to configure SNAT.

1. Log in to the Cloud Firewall console, and select **Firewall toggle** -> **NAT edge firewall** to enter the NAT edge firewall page.
2. Select **Instance configuration** -> **Bound egress** -> **Create rule** in the Action column on the left.
3. Select the external IP address of the specified subnet or private network, and then click **OK**.

How can I query subnets enabled with the firewall feature?

1. Log in to the Cloud Firewall console, and select **Firewall toggle** -> **NAT edge firewall** to enter the NAT edge firewall page.
2. Enter the **Firewall toggle** page to view all subnets enabled or disabled with the firewall feature.

Do I need to restart my server after enabling the DNS feature in instance configuration? Will the feature take effect without a restart?

You do not need to restart your server. Restarting your server will only validate the configuration sooner. This is similar to configuring DNS effective time on the VPC console. You can run the following commands to update your network configuration:
Linux: dhclient
Windows: ipconfig/flushdns

How frequently will assets be automatically synchronized?

Every 10 minutes.

Why can't I enable the NAT firewall feature for a subnet?

This situation may be caused by asynchronization of a changed asset scale. You can log in to the Cloud Firewall console, go to **Firewall toggle** -> **Edge firewall** -> **Sync assets** to manually synchronize the subnet asset information, and then try to enable the firewall feature again.

How can I change the VPC for a NAT firewall?

Click the Settings button in the upper right corner, and then access another VPC.

How many VPCs can be bound to a NAT firewall?

There are no limitations currently.

What if I failed to create a NAT edge firewall?

If your VPC has private line or peer connections, at least one 24/subnet must be reserved for firewall access.

Why can't I access an allocated EIP after the NAT firewall feature is enabled?

A newly allocated EIP can be accessed only after being bound.

Inter-VPC Firewall

Last updated：2024-01-24 16:23:02

Why can't an inter-VPC firewall be enabled?

Due to issues such as route and network segment conflicts, CFW limits any firewall generating conflicts. You can fix the conflicts as instructed, and then try to enable the inter-VPC firewall again.

What are firewall subnet and firewall route in the route table automatically created in a VPC?

After the inter-VPC firewall toggle is enabled, the firewall subnet and firewall route required for traffic introduction control will be automatically created. Please do not manually delete them to avoid effects on CFW. If you want to change the firewall subnet segment, submit a ticket to contact us.

What subnets among VPCs will inter-VPC firewall introduce traffic for?

It depends on your inter-VPC routing configuration. CFW only introduces traffic for subnets correctly configured with inter-VPC routing.

What if the bandwidth of inter-VPC firewall reaches the upper limit?

The current version does not support elastic scaling because the inter-VPC firewall is deployed with exclusive resources.
When the bandwidth of inter-VPC firewall reaches the upper limit, the firewall escape will be enabled and the firewall will be switched to the bypass mode in critical conditions, with 50% buffer bandwidth reserved to avoid effects on normal services.

Note

In bypass mode, CFW does not process any traffic, and all traffic is allowed to pass.
Please keep your eye on CFW bandwidth alerts. In case of high bandwidth, disable the firewall feature for some networks.

Feature
Traffic Monitoring

Last updated：2024-01-24 16:27:16

How often will the CFW traffic bandwidth diagram be updated to the latest version?

Generally every 1 minute.

How frequently is the Traffic Monitoring updated? How frequently are traffic logs updated?

Traffic Monitoring is updated every 10 minutes, while traffic logs are updated in real time.

Why does the CFW peak traffic value not match the actual value?

The traffic diagram displays the average bandwidth value, which means the average value within the statistical period. The peak value is calculated based on the traffic statistics collected every 10 seconds. The average traffic of an IP address is reported every 10 seconds, and the largest value among a specific period of time is regarded as the peak value.
Alert and billing are both based on the traffic statistics displayed on the page.

Access Control

Last updated：2024-01-24 16:27:16

Does CFW allow or block traffic by default when no rules are configured?

By default, CFW allows all traffic. Once enabled, CFW will record traffic logs and generate intrusion defense alerts, but will not block any traffic because no rules are configured.

How can CFW allow a specific port?

1. After enabling the edge firewall, select **Access Control** -> **Edge Rules** -> **Inbound Rules** to enter the inbound rule page.
2. Click **Add Rule** to allow a specific port, and then add a rule to block all ports.

Note

If no rule is configured, all traffic is allowed by default.

When will configured access control rules take effect?

CFW rules will take effect after 10 seconds to 1 minute upon configuration.

Does CFW support access control by domain name?

Both edge firewall and NAT firewall can set outbound rules by domain name.

Can CFW configure limitation policies by domain name?

Currently, limitation policies can be configured by domain name for assets in Chinese mainland and Hong Kong.

Does CFW support blocking by region?

Enterprise Edition and above support blocking by region.

Why can't I select the automatic both-way enterprise security group?

Automatic both-way access is supported only when the source address is an instance, subnet, or private network address. In this case, a same outbound rule (with the earliest execution order) will be allocated, which is applicable to scenarios that allow both-way internal-to-internal access.

Will the login protocol port be blocked if the edge firewall feature is not enabled for an asset?

No.

Intrusion Defense
Basic Protection

Last updated：2024-01-24 16:27:16

What kind of traffic will be checked by the Intrusion Prevention System (IPS)?

Traffic going through the edge firewall and NAT firewall will be checked by the Intrusion Prevention System.

What will be blocked in the Block mode?

In the Block mode, CFW will perform blocking in the following conditions:
Threat intelligence: Network attacks or malicious access with high confidence, as well as malicious outbound access can be automatically blocked.
Basic protection: Malicious behaviors that hit high-confidence rules are automatically blocked, and security event alerts are generated when other rules are hit.
Virtual patching: Virtual patching support automatic blocking of all traffic detected as vulnerability exploits.

How to manually block risks in the alert list? Can I manually add IP addresses for blocking?

For risks with frequent alerts or high risk levels, you can perform manual blocking. Besides, you can import IP addresses to be blocked to the blocklist of IPS. In case of access with any of these IP addresses, it will be directly blocked by CFW.
###What requests are blocked automatically in Block mode? Why do alerts still appear when Block mode is enabled?
In the Block mode, CFW will automatically block risks with high confidence and IP addresses in the blocklist.
Alerts will be generated for risks with low confidence. You can manually block the alert IP addresses in Alert Management.

How are malicious IP addresses blocked in Strict mode?

In the Strict mode, threat intelligence, base protection, and virtual patching are all in Global Block mode. All IP addresses that generate alerts will be blocked. For risks with high confidence and IP addresses in the blocklist, blocking will be triggered upon initial access. For other malicious IP addresses, an alert will be generated upon initial access, and blocking will be triggered upon access for twice.

Why are malicious IP addresses not blocked?

Intrusion defense of CFW is performed on sessions. Only sessions with attack characteristics will be blocked. If an IP address is not added to the blocklist, its sessions will not be blocked.

When will the Block mode be enabled?

Generally, if services remain unchanged after switching from Observe mode to Block mode for 1 to 2 days, the Block mode will be enabled.

Will the Block mode affect services after it is enabled? Are the blocking policies precise?

IPS only set rules with high precision to the Block mode. False positives are never found for virtual patching. If any problem occurs after the Block mode is enabled, feel free to contact us for help.

Will the communication between cloud intranet addresses be affected after the CFW Block mode is enabled?

No. After the Block mode is enabled, only Internet traffic of cloud services will be affected, and communication between cloud intranet addresses will not be affected.

What should I do if an IP address is incorrectly blocked by IPS?

1. Log in to the Cloud Firewall console, select **Log auditing** -> **Intrusion defense logs**, and then you can check the blocking history of the source or destination IP address.
2. In case of emergency, enter the **IPS** menu to turn off "Enable blocklist", and then go to **Alert management** -> **Blocked statistics** to view all blocking statistics and locate the blocking source.
3. After the fault is located and fixed, you can turn on "Enable blocklist" to enable it again.

What can I do in case of incorrect interception or access failure?

Check whether the firewall for the public IP address is disabled. In this case, traffic does not go through CFW.
Modify the IPS to Observe mode.
Configure the CFW policy to "Any", which means that the public IP address is allowed to pass.

Note

If none of the above works, please submit a ticket to contact us.

Why is an IP address missing in the configured blocklist?

1. An IP address whose effective period expires will be automatically removed from the blocklist, and the access of this IP address will not be blocked by the firewall anymore.
2. 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.

Will IP addresses in the ignored list be blocked?

IP addresses in the ignored list will directly bypass the IDPS.

How can I make specified detection rules ignored for an IP address?

Currently, it is not supported to make specified detection rules ignored.

In what case will DNS traffic bypass CFW?

Tencent Cloud CVM may use the DNS service developed by Tencent, and generated DNS messages will not go across the edge. In this case, alerts and logs will be generated for such domain names.
To enable a specified CVM to normally use domain name detection and alert features of CFW, you can manually modify the resolution address under /etc/resolv.conf to 8.8.8.8.

What is the relationship between Intrusion Protection System and access control?

CFW judgment order: **Blocklist** -> **Access control** -> **Ignored list** -> **Intrusion Protection System**
Intrusion Protection System takes effect only for assets with firewall enabled. For assets without protection enabled, their traffic will not go through CFW.

Defense Policy

Last updated：2024-01-24 16:27:16

What kind of traffic will be automatically blocked in Block mode of threat intelligence?

After the Block mode of threat intelligence is enabled, the NAT edge firewall will automatically block outbound threat intelligence alerts, and edge firewall and inbound traffic will be observed.

What kind of traffic will be automatically blocked in Block mode of virtual patching?

After the Block mode of virtual patching is enabled, the edge firewall will automatically identify vulnerability exploits and attacks of all network perimeter traffic. Connections that generate alerts will be automatically blocked.

What is the difference between IPS virtual patching and patches of other host security products?

Patches on a host are generally officially released, which may take several weeks or months. Some patches also require a CVM restart.
IPS virtual patching of CFW takes only few hours to update without the need to change or restart services. This is implemented by updating prevention rules of IPS in real time based on vulnerability exploit characteristics.
CFW IPS virtual patching and host security products such as CWPP, an optimal combination for host security protection, work together to systematically protect networks and hosts.

Do I still need to make a fix on my host after virtual patching is used?

Yes. Virtual patching protects the forefront of your network, and you still need to thoroughly fix vulnerabilities for most secure protection.

How are threat levels of intrusion defense rules defined?

The threat levels for basic defense and virtual patching are defined based on the threats they may cause.
The threat levels for threat intelligence are defined based on the threat level of historical attacks initiated by a specific IP address or domain name.

How does the CFW threat intelligence package update mechanism work?

There are two kinds of threat intelligence packages: high-precision package and prioritized protection package. Their features are as follows:
For high-precision packages, a complete false positive removal process is available.
Prioritized protection packages are only used in Strict mode for non-real IP addresses, and are disabled in Block or Observe mode by default.

Can shiro vulnerabilities be identify for intrusion defense virtual patching?

Yes, but not all scenarios can be covered, since some traffic is encrypted.

What vulnerabilities can be prevented by CFW?

For vulnerabilities that can be prevented by CFW, go to **Intrusion defense** -> **Intelligence center**.

How CFW determine a web attack?

Attack characteristics will be introduced during scanning and sniffing of external hackers. For example, once CFW detects the attack characteristics of the weblogic vulnerability, it will regard it as an attempted attack.

What protocol types are supported for brute force prevention?

The following protocol types are supported: MySQL, Oracle, SSH, Redis, MongoDB, IMAP, POP3, FTP, SMTP, SQLServer, and RDP.

How to deal with existing mining attacks?

If you have not purchased Tencent CWPP, you can manually kill the virus without the need of reinstallation. The server is infected if mining works.
If you have purchased Tencent CWPP, you can directly clear the threat.

Alert Management

Last updated：2024-01-24 16:27:16

Why do security baseline alerts disappear?

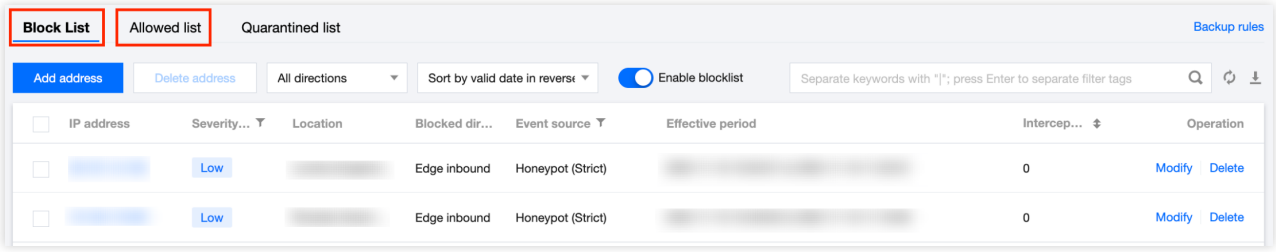
The number following an alert type indicates the number of alerts not processed. (BOT Attack displays the number of all alerts.) If the security baseline alert feature is not enabled, the console will not display the security baseline option.

Why is an IP address banned after interception?

Intrusion defense detects network attacks for sessions. Only when an IP is banned (added to the blocklist), all its access operations will be blocked.

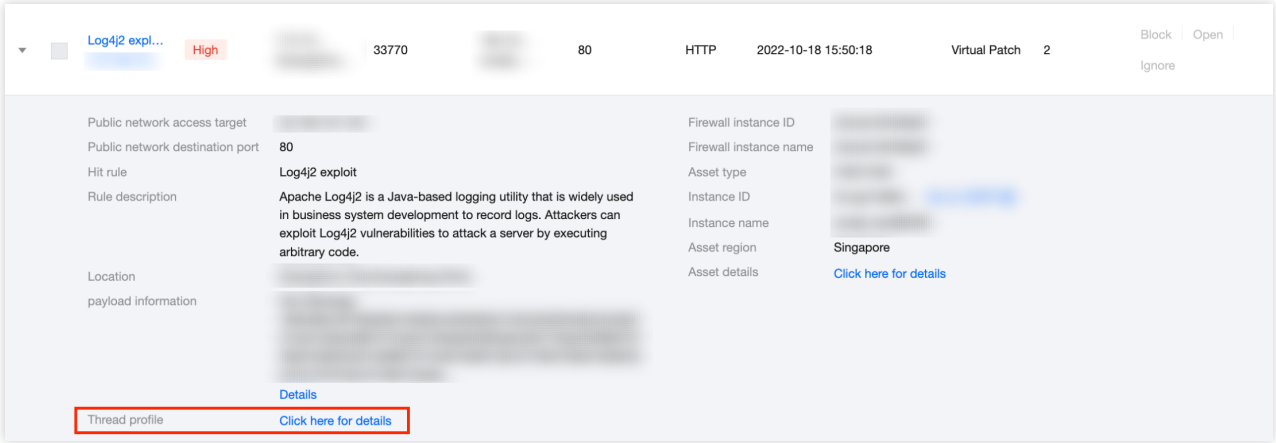
How can I modify a blocked or ignored event?

Log in to the Cloud Firewall console, enter the Intrusion Protection System module, and then you can remove an event from the "Blocklist" or "Ignored list".

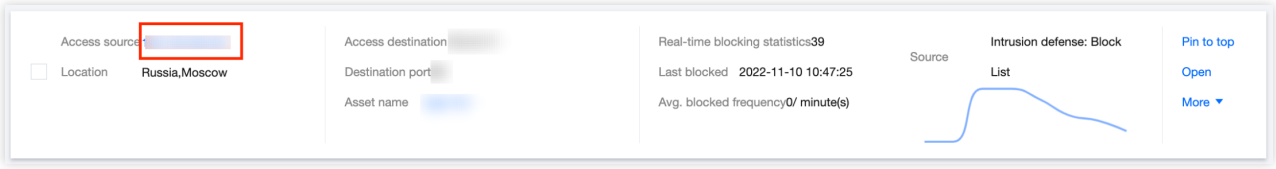


How can I view the threat profile of a specified IP address?

For a security event alert, you can view the threat profile in Security event alert - Event details.



In "Blocked statistics", you can directly click the **IP address** to redirect to details.



Why is an IP address following a red exclamation mark?

It means that this IP address may be a Tencent Cloud CDN address, which is not advised to be manually blocked or banned. If you have enabled the Block mode of IPS, CFW will automatically block attacks from this address. Normal traffic will not be affected.

How frequently will data in Alert Management be updated?

Data in Alert Management will be updated every 10 minutes.

What should I do to display the traffic trend chart in Alert Management?

1. On the Firewall toggle page, select an instance, click **Firewall toggle** -> **OK** to enable the firewall toggle.
2. After the firewall toggle is enabled, CFW ACL is in "All-pass" mode and intrusion defense is "Observe" mode by default. There is no impact on your service system.

Why is there no blocking data in Alert Management?

1. Check whether you have enabled the firewall toggle and set it to block or interception mode.
2. Select all policies for blocking data, and then check whether you can view corresponding events.
3. If you still fail to view corresponding events, contact us for help.

Can I receive bandwidth alerts if primary account and sub-account are not configured as alert objects in Alert Management?

If no primary account or sub-account is selected for receiving alerts, you will not be notified via SMS from Alert Management, or Message Center. However, alerts will still be displayed on the console.

Security Baseline

Last updated：2024-01-24 16:27:16

What is the security baseline of CFW?

By observing the traffic access statistics within a specific period of time, CFW generates a basic IP address or domain name access list. You can add or delete IP addresses or domain names based on the security scores, associated security events, and network access statistics, and finally form a security baseline.
After the security baseline is configured, security alerts will be triggered every time an IP address or domain name beyond the baseline is added. You can process IP addresses or domain names in the alert list. The security baseline feature is applicable to traffic baseline protection during prioritized protection.

Why can't baseline check time be configured?

You can check the task status of the security baseline score. In baseline learning status, the baseline check time cannot be configured.
Baseline learning time: statistics between the time added to baseline and baseline end time
Baseline check time: statistics between the time added to baseline and current time

Log

Last updated：2024-01-24 16:27:16

How long are CFW logs stored by default? What is the maximum storage capacity?

By default, CFW stores logs within 7 days for free, with the maximum storage capacity being 50 GB.
After the log analysis service is enabled, CFW will store logs within 6 months by default, with the available storage capacity being 1000 GB at least and 300 TB at most.

What if the log storage duration or capacity exceeds the quota specified in the package?

For default log storage with a capacity of 50 GB, logs preserved for over 7 days or beyond 50 GB will be automatically overwritten.
After the log analysis service is enabled, logs preserved for over 6 months will be overwritten.
After the log analysis service is enabled, if the log storage capacity reaches the upper limit, the earliest logs will be automatically overwritten in a rolling way to store the latest logs. If the total capacity of logs preserved in a rolling way is 9 times as large as the purchased capacity, the system will not store new logs any more.
Note
For example, if you purchase 1000 GB for log storage, once the log storage capacity reaches 10000 GB, no new logs will be recorded.
For better log analysis and query, you are advised to expand log storage capacity or use the log shipping feature.

What is the relationship among log auditing, log analysis, and CLS?

Currently, log auditing is a built-in feature of CFW, which is unrelated to CLS. CFW logs can be shipped so that users can analyze logs themselves.

What do access control logs, intrusion defense logs, and traffic logs record respectively?

Access control logs record traffic that hits the access control rules.
Intrusion defense logs record traffic that hits the intrusion prevention rules.
Traffic logs record traffic allowed to pass.

Can I archive logs in CFW?

Yes. You can export and ship logs to the Kafka instances of customers.

How can I download logs?

You can use the log shipping feature to export logs for analysis (ensure that you have purchased a Tencent Cloud Kafka instance). For details about the configuration method, refer to Log Analysis.
Alternatively, log in to the Cloud Firewall console, select **Log auditing** -> **Traffic logs** in the left navigation pane to enter the traffic log page, and then click

in the upper right corner to download logs.

Note

A maximum of 60,000 log records can be exported based on specified search criteria.

How long does it take to ship logs successfully?

It takes about 1 minute to ship logs, so related log updates may not be included.

Do shipped logs have any tag to identify the log type?

No. No tags are available to identify the log type. You are advised to select different topics during log shipping to distinguish your logs.

Why are "Observe" logs still found when the Block mode is enabled?

If any intrusion contains vulnerability attacks and hits virtual patching, the virtual patching will perform blocking automatically, but automatic blocking is not yet supported in basic protection rules currently. Therefore, only the Observe mode is available in basic protection rules. In future versions, automatic blocking with high confidence and permanent blocking will be supported.

Do traffic logs record IP traffic blocked by ACL or IPS?

No. Traffic logs do not record IP traffic blocked by ACL or IPS. Only allowed traffic is recorded.

Will logs be generated for blocked attacks?

ACL: Access data will be blocked in block mode, rule hitting times, and ACL logs will be recorded, but traffic logs will not be recorded.
Intrusion detection system (IDS): An intrusion detection event will be generated for any intrusion that hits intrusion detection policies. You can view blocking logs by using the log analysis feature.

How can I figure out whether access or attack is blocked or allowed in shipped logs?

The strategy field in logs indicates whether access is blocked or observed.

Note

The strategy field is unavailable for traffic logs.

Why can't I select a purchased CKafka instance in Supported environment in log shipping?

You need to add an access method to the CKafka instance first. Currently, the public domain access method is available, while supported environment is unavailable yet. For details, go to the Cloud Kafka console.

Account

Last updated：2024-01-24 16:27:16

Can I use CFW under another Tencent Cloud account?

No. CFW cannot be used across accounts. It can only protect cloud assets under the current Tencent Cloud primary account.

Will my service be affected when I add role authorization?

No. By adding role authorization, you allow the Cloud Firewall console to read your VPCs, subnets, and other cloud resources, so that related data can be displayed on the page. This will not affect any automatic operation of your service.

Can I receive bandwidth alerts if primary account and sub-account are not configured as alert objects in Alert Management?

If no primary account or sub-account is selected for receiving alerts, you will not be notified via SMS from Alert Management, Message Center, or WeChat. However, alerts will still be displayed on the console.

How can I grant CFW permissions to sub-accounts?

You need to create a CFW role in CAM, and then add the following permissions to your sub-accounts:
QcloudCFWReadOnlyAccess
QcloudAccessForCFWRole
QcloudAccessForCFWRoleInUploadLog
QcloudAccessForCFWRoleInVPCFireWall
QcloudCFWFullAccess
QcloudCamSubaccountsAuthorizeRoleFullAccess"

What if I failed to open the CVM overview page with a warning message displayed: you are not authorized to perform operation(cfw:DescribeCfwUserStatus)?

In this case, grant the following permissions to the current sub-account:
QcloudCFWFullAccess
QcloudCFWReadOnlyAccess"

Billing

Last updated：2023-12-11 16:55:00

Can I modify the configurations for Cloud Firewall?

CFW supports scaling up of purchased configuration, but scaling down is not supported currently.

Can I renew my Cloud Firewall subscription when it expires? Will I lose all my resources when my subscription expires?

The usage duration of CFW can only be configured when you purchase the service. Upon expiration, the service will be automatically stopped. You can purchase it again without affecting your business.
Your configuration can be recovered if you renew the service within 14 days upon expiration.
After 14 days upon expiration, all your CFW resources will be recycled and cannot be recovered. In this case, you can purchase the service and configure it again.

How many firewalls can be purchased for an account?

An account can purchase one firewall. Paid editions of Tencent Cloud Firewall include Premium Edition, Enterprise Edition, and Ultimate Edition.

Others

Last updated：2024-01-24 16:27:16

Will public network assets be automatically identified on the overview page? How is it implemented?

Yes. Public network assets are automatically identified via Tencent Cloud APIs and CAM authorization. All assets of an account are enumerated through cloud APIs.

After enabling the firewall feature, I want to enable "Observe" mode without interception. What should I do?

Enabling the firewall feature for a public IP address is OK. The "Observe" mode is used by default after the firewall feature is enabled. You do not need to configure the ACL, with the default ACL policy being "All-pass".

How can I determine whether an IP address is blocked by CFW?

Log in to the Cloud Firewall console, select **Log auditing** -> **Intrusion defense logs** and **Access control logs**, and then you can check whether an IP address is blocked by CFW.
Alternatively, enter **Alert management** -> **Blocked attacks**, and then you can check the block statistics in the intrusion defense module.

How can I check the Cloud Firewall version?

It is not supported to check the version currently. You can check the package and expiration date of the current account on the right of the Overview page.

Can Cloud Firewall limit traffic by MAC address?

No. Cloud Firewall cannot limit traffic by MAC address. The second layer is shielded on cloud networks, so addressing can be performed only via IP. For example, addressing is performed via IP instead of ARP among CVMs.

Can I adjust or disable Cloud Firewall bandwidth alert thresholds?

Bandwidth alert is an important indicator for Cloud Firewall, and traffic beyond the bandwidth limit will not be protected. You can adjust the first-level and second-level alert thresholds on the console. Disabling thresholds is not supported.

Is my business affected when I enable or disable Cloud Firewall, scale up, add CAM authorization, and enable or disable intrusion defense?

Enabling the edge firewall will not affect your business; enabling the NAT firewall or VPC firewall will cause an interruption of CCN for 1 to 2 seconds. In this case, you are advised to operate during non-peak hours.

Scale-up of the edge firewall will not affect your business; scale-up of the NAT firewall may cause an interruption for 1 to 2 seconds. For any question, submit a ticket.
Scaling up Cloud Firewall, enabling/disabling intrusion defense, or adding CAM authorization will not affect your business.