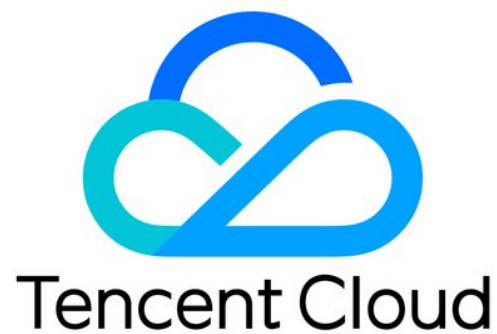


Web Application Firewall

FAQS

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

FAQS

- Product Consultation

- Connection

 - Real Server

 - Port Support

 - Domain Name

 - CNAME

 - Associated Product

- Usage

FAQS

Product Consultation

Last updated : 2023-12-29 14:55:56

Can I use, migrate, and share WAF instances across accounts?

No, you cannot use, migrate, or share WAF instances across accounts.

Is WAF available to servers outside Tencent Cloud?

WAF can be connected with servers in data centers outside Tencent Cloud. WAF protects servers in any public networks, including but not limited to Tencent Cloud, and clouds and IDCs from other vendors.

Note:

Domain names connected in the Chinese mainland must be ICP filed as required by the Ministry of Industry and Information Technology of China.

Does WAF support HTTPS protection?

WAF fully supports HTTPS services. You just need to upload the SSL certificate and private key as instructed or select the Tencent Cloud-hosted certificate to use WAF for HTTPS traffic protection.

Does the WAF QPS limit apply to the entire instance, or to a single domain name?

The QPS limit in WAF is for the entire instance. For example, if three domain names are protected, the total QPS of the three domain names cannot exceed the limit. If the QPS limit of the purchased instance is exceeded, speed will be limited and packets will be lost.

Can Anti-DDoS Pro instances be used for WAF?

Yes. You can empower WAF with high DDoS protection capabilities simply by selecting IPs specified in a WAF instance on the configuration page in the Anti-DDoS Pro console. For more information, see [Combination of Anti-DDoS Pro and Web Application Firewall](#).

Are there any risks in uploading an SSL certificate's private key?

An SSL certificate's private key hosted on Tencent Cloud will enjoy extremely high security, in terms of:

Uploading stage

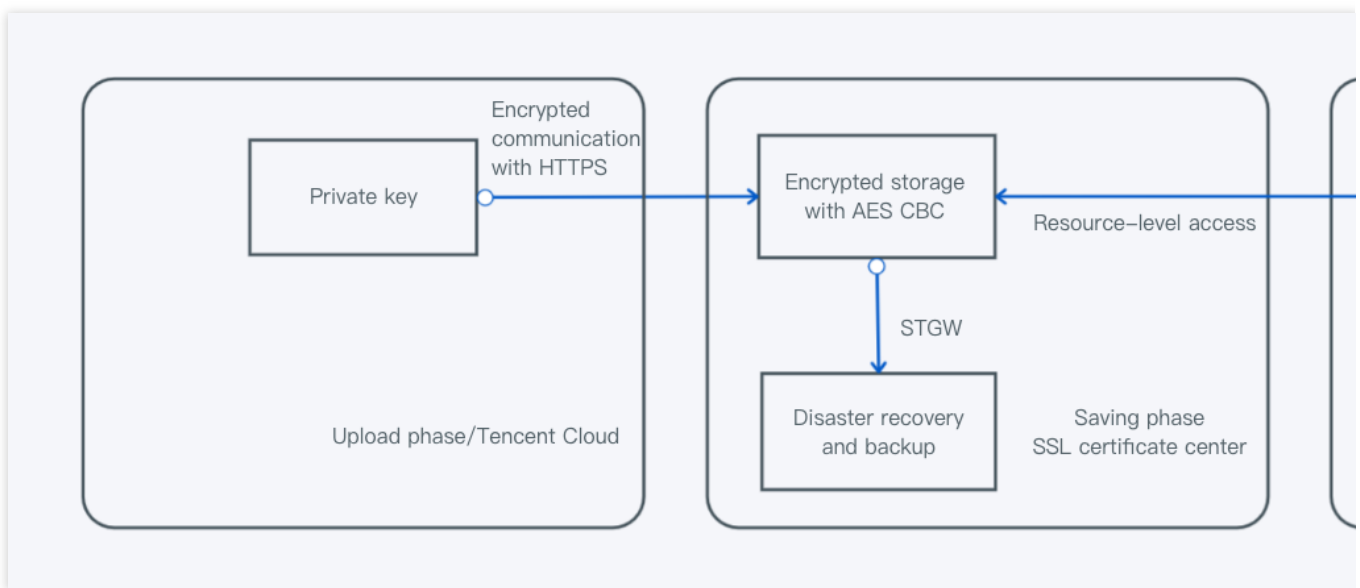
The process from uploading the private key to configuring the certificate on the Tencent Cloud certificate hosting platform is protected with HTTPS, an encrypted communication, and enterprise SSL certificates, ensuring the safety of communication data.

Saving stage

1. After uploading, the certificate is stored in the database. The certificate's private key will be encrypted using the AES CBC mode, which effectively prevents the private key from brute force attacks.
2. The certificate database will be backed up for disaster recovery. For high availability and high security of the certificate data, no external APIs will be used and the data will be protected by STGW.
3. There are multiple backend servers for SSL certificates, which are accessed via a load balancer to ensure API stability.

Managing and reading certificates

1. Integrating resource-level Cloud Access Management (CAM), SSL Certificate Service is backed by a well-established access management system that allows you to grant different permissions to your sub-accounts on different certificates to prevent malicious revocation and deletion.
2. The certificate pulling in WAF is protected by STGW. The business pulls the certificate on demand while identifying and authenticating the source of the request to avoid illegal and unnecessary access.



Is the SSL mutual authentication supported by both the SaaS WAF and CLB WAF?

It is supported by CLB WAF but not by SaaS WAF.

What are the differences between WAF and CFW?

The differences are as follows:

Type	Tencent Cloud WAF		Tencent Cloud CFW
	SaaS WAF	CLB WAF	
Protected	Websites and	Websites and API services.	Businesses completely exposed on

Target	API services.		the internet
Application Scenarios	It is applicable to those who require multi-level protection or cybersecurity assurance service, particularly for webs, APIs, application layers and anti-cheating behavior.	It is applicable to those who require multi-level protection or cybersecurity assurance service, particularly for webs, APIs, application layers and anti-cheating behavior, and who have used or plan to use layer-7 CLB instances on Tencent Cloud.	It is applicable to those who require multi-level protection or cybersecurity assurance service, or who require protection for CVMs and network.
Core Protection Capability	Web vulnerability and unknown threat prevention, and self-service false negative and false positive handling. CC attack protection. API security and business security. Leakage and tamper protection.	Web vulnerability and unknown threat prevention, and self-service false negative and false positive handling. CC attack protection. API security and business security. Protected IPv6 access to websites.	IPS virtual patching (which covers OWASP TOP 10 web vulnerabilities) eliminates the need for CVM to install physical patches or reboots. Discovers the overwhelmed CVM and blocks the CVM from malicious external connections automatically. Supports controlling external connections proactively based on domain name.
Core Strength	It is applicable to Tencent Cloud and non-Tencent Cloud users.	Cloud-native access ensures the safety, stability and reliability of Tencent Cloud users' website business with separation between forwarding and security protection via one-click bypass, which is implemented without changing the existing network architecture. Besides, multi-region access is also supported.	The cloud-native firewall can be enabled with one click, without affecting your business. It integrates security capabilities, such as IPS, threat intelligence, and omission scanning, necessary for multi-level protection and cybersecurity assurance scenarios, which is only available to Tencent Cloud users.
How to Choose	SaaS WAF is recommended for those who	CLB WAF is recommended for those who have used or plan to use layer-7 CLB instances.	CFW is recommended for those who have concerns over the security of CVM (whether it will be

require protection for websites and APIs on cloud and in local IDC.

overwhelmed), and businesses exposed on the internet that expose public network businesses in addition to web businesses.

How does WAF prioritize hit rules?

WAF rules follow the following hit priorities: precise allowlist > IP allowlist > IP blocklist, regional blocking, access control, CC rules > bot protection > web protection (rule engine), AI engine, tamper protection, leakage protection.

Connection Real Server

Last updated : 2023-12-29 14:56:07

Can the real server IP added to WAF be the private IP of a Tencent Cloud CVM instance?

When adding a domain name to WAF, the real server address must be a domain name or a public IP, such as CVM public IP, CLB public IP, or Egress IP of other local IDCs, while a CVM private IP is not supported.

What is a forwarding IP used for?

A forwarding IP is automatically assigned after the protected domain name is configured in SaaS WAF. When forwarding traffic to the client's real server, WAF will use the forwarding IP as source address. To achieve better protection, you need to add the forwarding IP to a trusted list on the server. It is recommended allowing only access traffic from the WAF forwarding IP to the real server.

How many real server IPs can be set for one protected domain name in WAF?

Up to 20 real server IPs can be set for one protected domain name in WAF.

How does the traffic balancing work when multiple real servers are configured in WAF?

If multiple forwarding IPs are configured, WAF achieves load balancing for access requests by polling.

Does WAF automatically add a forwarding IP range to a security group?

WAF does not automatically add a forwarding IP range to a security group. To do so, see [Getting Started](#).

Port Support

Last updated : 2023-12-29 14:56:18

Which ports does WAF support?

You can view and configure the ports supported by WAF in the console.

1. Log in to the [WAF console](#) and select **Web security protection** > **Protection settings** on the left sidebar.
2. On the **Protection settings** page, click **Add domain name**.
3. In **Server configuration** on the **Add domain name** page, select the target protocol to view and configure the port.

You can configure up to five ports for one domain name.

By default, WAF Premium supports HTTP (80/8080) and HTTPS (443/8443) standard ports but not non-standard ports.

WAF Enterprise and Ultimate support non-standard ports in addition to the default HTTP (80/8080) and HTTPS (443/8443) standard ports as listed below:

Protocol	Port
HTTP	80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 800, 805, 808, 1000, 1090, 2020, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7007, 7008, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7040, 7070, 7081, 7082, 7083, 7088, 7097, 7510, 7621, 7777, 7800, 8000, 8002, 8003, 8004, 8005, 8006, 8007, 8008, 8009, 8010, 8011, 8012, 8020, 8021, 8022, 8060, 8025, 8026, 8060, 8077, 8078, 8080, 8081, 8082, 8083, 8086, 8087, 8088, 8089, 8090, 8106, 8181, 8182, 8184, 8210, 8215, 8334, 8336, 8445, 8686, 8800, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9180, 9182, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 10000, 10001, 10080, 10083, 12601, 20080, 20083, 25060, 28080, 28080, 33702, 48800, and 52301
HTTPS	443, 4443, 5100, 5200, 5443, 6443, 7443, 8084, 8085, 8091, 8442, 8443, 8553, 8663, 9443, 9550, 9553, 9663, 10803, and 18980

Note:

If you use Ultimate Edition and need to protect ports not included in the HTTP or HTTPS list, WAF offers the non-standard port customization service (for ports 1-65535). You can customize up to five non-standard ports for all domain names in your plan. If you need this service, [submit a ticket](#) to contact WAF_hepler for assistance.

Ports already in the HTTP or HTTPS list cannot be customized for other protocols.

If you need HTTP and HTTPS non-standard ports, [submit a ticket](#) to have them added to the allowlist by WAF_hepler.

Domain Name

Last updated : 2023-12-29 14:56:31

How do I connect a domain name with WAF?

You can connect domain names to WAF in the [WAF Console](#) as instructed in [Add a Domain Name](#).

Does WAF support wildcard domain names?

Yes. You can add a wildcard domain name in the [WAF console](#).

Note:

When a wildcard domain is added to WAF, other Tencent Cloud users can still add subdomain names that match the wildcard domain name to WAF.

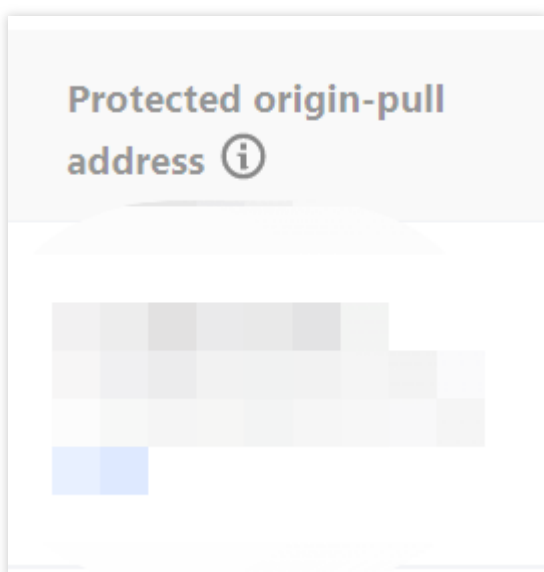
If you add both a wildcard and a precise domain name (e.g. `*.test.com` and `a.test.com`), policies of the precise domain name prevail.

How long does it take to update the DNS resolution (protection) status of my domain name?

After you add the CNAME record at your DNS provider, status of the domain name on WAF is updated in 10 to 20 minutes. If you don't see the update in 30 minutes, please check the CNAME configuration or [submit a ticket](#).

Will the intermediate IP change?

The intermediate IP is subject to be changed by WAF. You will be notified by an SMS message, an email, or a message in Message Center if your intermediate IP address changes. You can check the effective intermediate IP on the [Domain Name List](#) page of the WAF console.



Will the SaaS WAF-connected VIP address change?

Yes. VIP address may change when WAF is maintaining and upgrading its in/cross-region disaster recovery capabilities. To ensure the service availability, WAF only supports configuring VIP addresses by adding the CNAME.

Can I modify the SaaS WAF-connected VIP address?

No. A SaaS WAF-connected VIP address cannot be modified. If the associated domain name fails due to DDoS attacks, you can [submit a ticket](#) for assistance.

What are the requirements for connecting a domain name to WAF?

If the domain name points to a real server in the Chinese mainland, an ICP filing number is required.

If the domain name is not

If you have obtained an ICP filing for the domain name through another service provider, you must add Tencent Cloud as a service provider to the ICP filing.

Note:

If the instance to which you add the domain name is a SaaS WAF instance, you also need to add a CNAME record at the DNS service provider of the domain name. Set the record value to the CNAME allocated by WAF.

What options does WAF offer for domain name origin-pull?

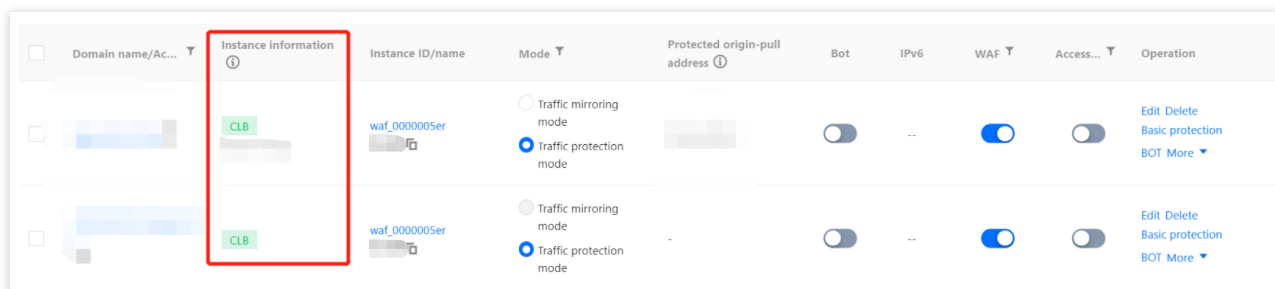
WAF performs origin-pull based on domain name or IP. You can choose which option to configure as you need. For more information, see [Add a Domain Name](#).

How do I bind a CNAME to my domain name connected to WAF?

See [Step 3. Modify DNS Resolution](#).

If I remove a domain name and add it back to WAF, does the CNAME change?

Yes. You can check the CNAME in the [Domain Name List page in the WAF console](#).



Domain name/Access...	Instance information	Instance ID/name	Mode	Protected origin-pull address	Bot	IPv6	WAF	Access...	Operation
	CLB	waf_0000005er	<input type="radio"/> Traffic mirroring mode <input checked="" type="radio"/> Traffic protection mode		<input type="checkbox"/>	--	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete Basic protection BOT More
	CLB	waf_0000005er	<input type="radio"/> Traffic mirroring mode <input checked="" type="radio"/> Traffic protection mode		<input type="checkbox"/>	--	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete Basic protection BOT More

What is the forwarding domain name?

When you add a domain name to WAF, you must specify a forwarding domain name. It can be the CNAME of proxy or another domain name. The protocol type (HTTP or HTTPS) is not required.

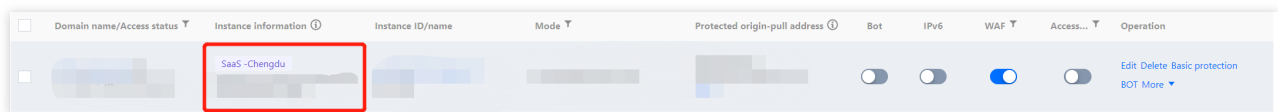
CNAME

Last updated : 2023-12-29 14:56:41

How do I configure CNAME?

You cannot access the CNAME domain name directly. You need to complete the CNAME configuration at your domain name service provider. WAF will protect your domain name after the configuration takes effect. For more information, see [CNAME Configuration](#).

If you have completed CNAME configuration, after you connect your domain name to WAF, the system will automatically assign a CNAME domain name suffixed with `.qcloudxxxx.com` (for example, `.qcloudcjpj.com` and `qcloudwzgj.com`), which is displayed in **Instance information** on the [domain name list page in the WAF console](#).



Domain name/Access status	Instance Information	Instance ID/name	Mode	Protected origin-pull address	Bot	IPv6	WAF	Access...	Operation
	SaaS-Chengdu				<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete Basic protection BOT More

Associated Product

Last updated : 2023-12-29 14:56:53

How do I use WAF together with CDN or Anti-DDoS Pro services?

You can use WAF with Anti-DDoS Pro directly, or use it with CDN by setting the CDN origin server IP as the IP of a WAF instance. Recommended deployment architecture: Client > CDN > WAF + Anti-DDoS Pro > CLB > Real server. If you need the CDN and Anti-DDoS capabilities, simply set the CNAME provided after the connection to WAF as the CDN origin server, and associate Anti-DDoS Pro with the WAF instance. In this way, the user traffic, after going through CDN, is forwarded to WAF, which has the capability of cleansing high-traffic DDoS attacks, and finally reaches the real server for full protection.

How do I connect a CDN domain name to WAF?

To connect a CDN domain name, simply use the CNAME address that WAF assigned for your domain name as the CDN real server. The content is pulled from the origin as traffic flows in the order "user > CDN > WAF > CLB > real server". Meanwhile, you can log in to the WAF console, and select **Yes** for **Use proxy** on the [Add domain name](#) page. Then, WAF obtains the real IP of your client for protection based on the XFF field in HTTP headers.



The screenshot shows the 'Add domain name' configuration page in the WAF console. The 'Instance' section has 'SaaS' selected. The 'Domain name' field is empty with a placeholder 'Please enter the domain name'. Under 'Server configuration', 'HTTP' is checked with a port of '80', and 'HTTPS' is unchecked. The 'Use proxy' section is highlighted with a red box, showing 'No' selected and 'Yes' unselected. A note below the radio buttons reads: 'Choose Yes if you are using proxies (Dayu, CDN or any other acceleration service)'.

Usage

Last updated : 2023-12-29 14:58:03

How do I download access logs of the last 180 days?

When Access Logs is enabled, WAF stores the logs for at least 180 days. You can query and download access logs of the last 30 days. To download logs of the last 180 days, please [submit a ticket](#).

Does WAF support health check?

SaaS WAF supports a four-layer health check mechanism, which can be enabled for Enterprise Edition and above versions when the domain is accessed. After enabling, it actively detects the health status of all source IP addresses every 3 seconds. For more information, please [submit a ticket](#).

Does WAF support session persistence?

Yes. WAF supports session persistence. You can [submit a ticket](#) to activate this feature.

Will logging still be available once WAF is disabled for the domain name list?

No. Once WAF is disabled, all its protection features are unavailable, and only the traffic forwarding mode starts to run instead, with no logs recorded.

When will a configuration change take effect?

In general, a configuration change takes effect within 10 seconds.

Note

It applies to connection configurations (including setting the real server, link mode, and whether to enable HTTP2.0).

The VIP of WAF-protected domain name is blocked due to DDoS attacks. What should I do?

WAF VIP addresses come with 2-GB Anti-DDoS Basic protection bandwidth. When you need to recover your business immediately after the VIP is blocked, purchase an [Anti-DDoS Pro](#) instance and bind it to the VIP address.

If the uploaded files are blocked, will they still be blocked with HTTPS or SFTP?

If WAF is disabled, the file will not be blocked. If WAF is enabled and the blocking mode is set, WAF will block malicious files uploaded over HTTP or HTTPS, but will not block files uploaded over SFTP. SFTP is a non-HTTP or non-HTTPS protocol beyond the protection of WAF.

Will the persistent connection be disconnected when the WAF certificate is changed?

No. Updating the certificate will reload nginx, and the thread will not be recycled until the end of the old request session, so it will not be disconnected.

What cipher suite does the SaaS WAF or CLB WAF support?

SaaS WAF does not support SSL cipher suites.

CLB WAF supports:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:AES:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK

WAF supports the following TLS versions:

TLSv1, TLSv1.1, and TLSv1.2.

Cipher suites:

EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:RSA+3DES:!MD5.

Note

SaaS WAF supports ECDHE cipher suites by default (such as TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA). Customization for TLS protocol and cipher suite is available in the Exclusive edition.

How do I query the module hit by a block page?

1. When a malicious request is detected, WAF blocks the request and returns a block page with a UUID.



Sorry, the request you submitted may pose a threat to the website. The request has been blocked by 1

This page is [Tencent T-Sec Web Application Firewall\(WAF\)](#)This is default block page, if you have any questions, please contact the wel

2. You can copy the UUID and search for it on the [Attack Logs page](#).

Note

Specify the query period.

Check information of the hit rule in the log fields: `attack_type` , `rule_id` , and `attack_content` .

Attack Logs All domain names

All attack types All actions All risk levels Last 4 hours 2022-06-16 15:43:36 ~ 2022-06-16 19:43:36 Auto refresh

1 uui

Number of attacks 1times Number of logs 1rules

1

2022-06-16 15:40 2022-06-16 16:10 2022-06-16 16:40 2022-06-16 17:10 2022-06-16 17:40 2022-06-16 18:10

Raw data

Search

- host
- uri
- attack_ip
- attack_type

Logging time ↓	attack_ip	status	method	uri	domain
2022-		Block	GET	/	

Total items: 1