Web Application Firewall

FAQS

Product Documentation

Contents

FAQS

Product Consultation

Last updated：2022-06-23 10:11:31

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

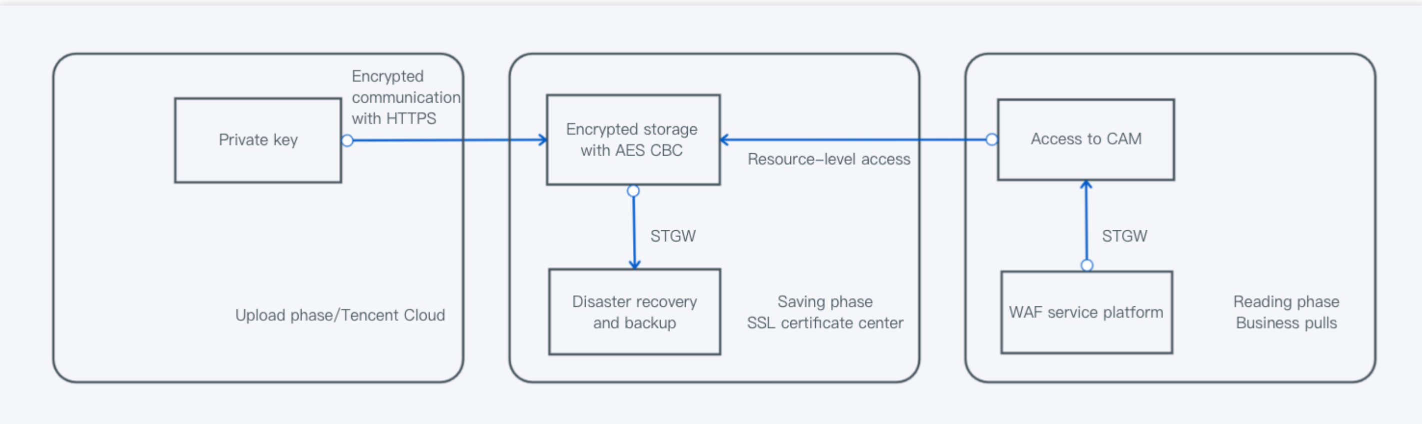
The process from uploading the private key to configuring the certificate on the Tencent Cloud certificate hosting platform is protected with HTTPS, an encrypted communication, and enterprise SSL certificates, ensuring the safety of communication data.

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:

Product / Item	Tencent Cloud WAF		Tencent Cloud CFW
	SaaS WAF	CLB WAF	

<table>
<tr><th rowspan="2">Product
Item</th><th colspan="2">Tencent Cloud WAF</th><th rowspan="2">Tencent Cloud CFW</th></tr>
<tr><th>SaaS WAF</th><th>CLB WAF</th></tr>
<tr><td>Protected Target</td><td>Websites and API services.</td><td>Websites and API services.</td><td>Businesses completely exposed on the internet</td></tr>
<tr><td>Application Scenarios</td><td>It is applicable to those who require multi-level protection or cybersecurity assurance service, particularly for webs, APIs, application layers and anti-cheating behavior.</td><td>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.</td><td>It is applicable to those who require multi-level protection or cybersecurity assurance service, or who require protection for CVMs and network.</td></tr>
<tr><td>Core Protection Capability</td><td>• 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.</td><td>• 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.</td><td>• 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.</td></tr>
</table>

Item \ Product	Tencent Cloud WAF		Tencent Cloud CFW
	SaaS WAF	CLB WAF	
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 require protection for websites and APIs on cloud and in local IDC.	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 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：2022-06-23 10:11:31

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：2022-06-23 10:11:31

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：2022-06-23 17:03:54

How do I connect a domain name?

You can connect a domain name in the WAF console. For more information, see Step 1. Add a Domain Name.

Does WAF support connecting wildcard domain names?

Yes. You can connect a wildcard domain name in the WAF console.

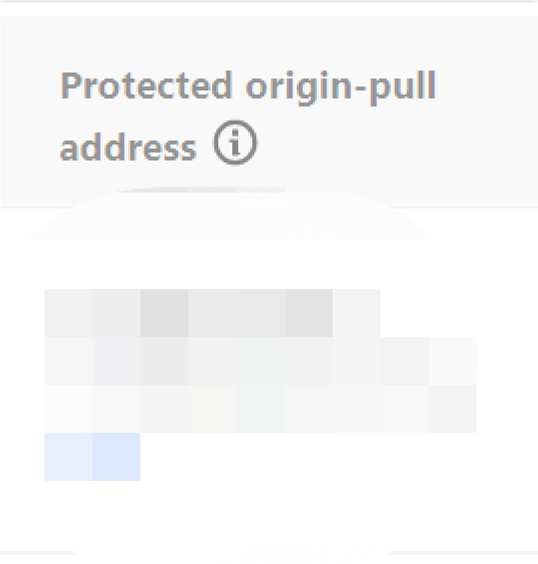
> Note：
>
> - If a wildcard domain name, such as `*.test.com`, is already connected to Tencent Cloud, then any of its sub-domain names cannot be connected to another account.
> - If the wildcard domain name `*.test.com` is already connected to your account, then wildcard domain names in formats such as `*.a.test.com` cannot be connected to this account.
> - If you add both a wildcard and a precise domain name (e.g. `*.test.com` and `a.test.com`), WAF first uses the protection policies configured for the precise domain name.

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

Verify that CNAME configuration for your website domain name is correct. Once you add a CNAME record in DNS, wait 10-20 minutes for the protection status to be updated. If you have waited over 30 minutes, and the protection status has not been updated yet, you can contact us for help by submitting a ticket.

Will WAF notify me when the intermediate IP address of my domain name is changed?

In principle, the intermediate IP address of your domain name is not changed. If it happens, we will notify you by SMS, email or Message Center. You can view your intermediate IP address in the Domain Name List of the console.



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

The business content on your real server must be legal, and you can modify the DNS resolution properly. Otherwise, you will not be able to connect your domain name to WAF.

After obtained the ICP filing from the MIIT, you need to file your domain name with Tencent Cloud.

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

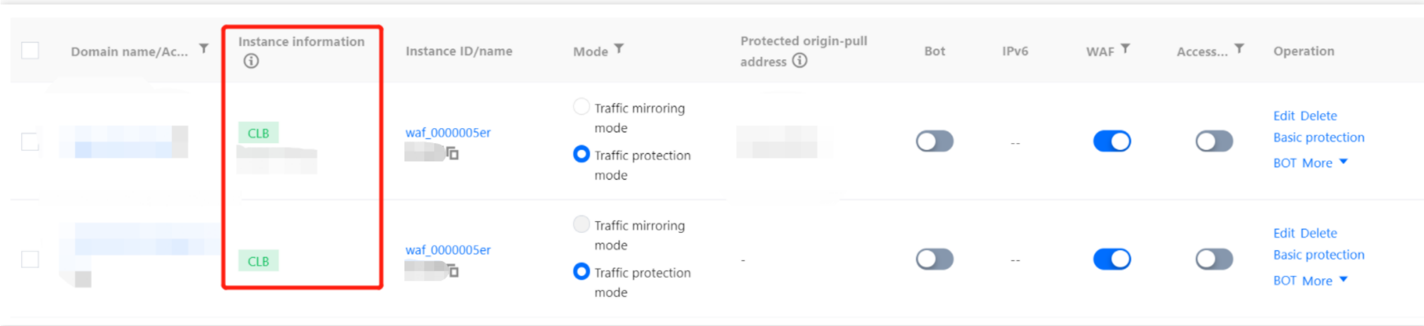
WAF performs origin-pull based on domain name or IP. You can choose which option to configure as you need. For more information, see Add a Domain Name.

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

See CNAME Configuration for how to bind CNAME with your DNS service provider.

Will the CNAME change if my domain name is deleted and added again?

After you delete a domain name from an instance, if you add it to the same instance, the CNAME record won't change; if you add it to another instance, the CNAME record will change. You can view the specific value in the instance information in the domain name list in the WAF console.



Can I change the VIP address of my domain name?

No, you can't change it, in principle. However, if an exception occurs to your WAF service, you may contact us quickly by submitting a ticket so that we can switch it to another working VIP address for you.

How do I enter a forwarding domain name when adding a domain name to WAF?

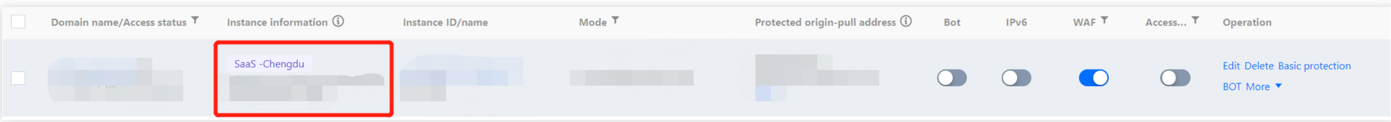
You can enter a CNAME address from other proxies or any other domain name as forwarding domain name. The domain name you entered and the one you added to WAF cannot be identical, and the protocol type (HTTP or HTTPS) can be left empty.

CNAME

Last updated：2022-06-23 10:11:31

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 `.qcloudxxx.com` (for example, `.qlcoudcjpj.com` and `qcloudwzgj.com`), which is displayed in **Instance information** on the domain name list page in the WAF console.



Associated Product

Last updated：2022-06-23 10:11:32

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.

Usage

Last updated：2022-06-23 10:11:32

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

Access logging is used to record access logs of domain names protected by WAF. It allows you to query and download access logs generated in the last 30 days and retain them for no fewer than 180 days. If you need logs of the last 180 days, submit a ticket for assistance. After enabling this feature, you can query and download access logs as needed to meet your security compliance and Ops requirements.

Does WAF support health check?

Health check is enabled for WAF by default. WAF checks the connection status of all real server IPs. For the real server IP that does not respond, WAF will not forward requests to this IP until its connection status becomes normal.

Does WAF support session persistence?

Session persistence is supported and enabled by default in WAF.

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

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), instead of protection configurations.

What should I do if the VIP address of my WAF-protected domain name is blocked due to DDoS?

By default, WAF VIP addresses come with Anti-DDoS Basic capabilities (2 Gbps). If blocking occurs in the basic protection and you need to recover your business urgently, purchase an Anti-DDoS Pro instance and bind it to the VIP address of the WAF instance.

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 for changing the WAF certificate?

No. Renewing 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.

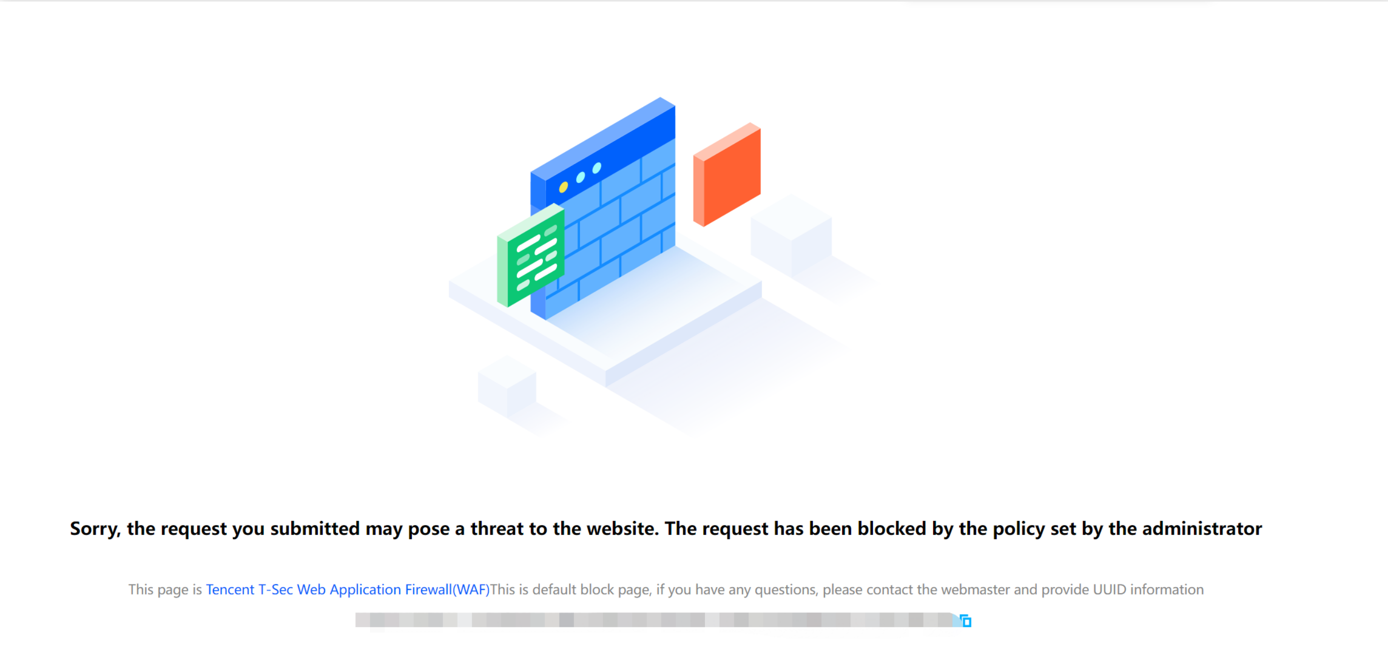
What cipher suite does the SaaS WAF or CLB WAF support?

- SaaS WAF does not support setting 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 suite:
    EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:RSA+3DES:!MD5.

> Note：
> Customization for TLS protocol and cipher suite is available in Exclusive Edition.

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

1. When malicious users access a protected domain name illegally, WAF will block the request and redirect them to the block page that will return a UUID.



2. Copy the UUID and search for it on the Attack Logs page to view the block packet information.

> Note：
>
> - Check the time period before searching.
> - A packet mainly contains the following fields: `attack_type` , `rule_id` , and `attack_content` , from which you can query the hit rules for subsequent operations.