



Web Application Firewall

Product Documentation





Contents

Web Application Firewall 3

- Product Introduction 3
 - WAF Overview 3
 - Product Category 6
 - Strengths 9
 - Scenarios 11
 - Basic Concepts 12
- Purchase Guide 14
 - Billing Overview 14
 - Purchase Guide 15
 - Payment Overdue 16
- Getting Started 18
- Operation Guide 20
 - Overview 20
 - Best Practices 24
 - Building a CLB WAF Test Environment 24
 - Building a SaaS WAF Origin Server 27
 - CLB WAF Connection 36
 - Comparison of Access Methods 36
 - Precise Domain Access 38
 - Layer 7 Load Balancing CLB Integration 38
 - Step 1: Confirm CLB Configuration 38
 - Step 2: Bind Domain Name to CLB Instance 39
 - Step 3: Verify the configuration 40
 - Asset Center 41
 - Instance Management 41
 - Access Management 44
 - Basic Security Configurations 45
 - Match Mode Field Description 45
 - Rule Engine 46
 - IP Blocking 50
 - Access Control 51
 - CC Protection Rule Settings 53
 - API Security Management 57
 - API Traffic Analysis 57
 - Blocklist/Allowlist Protection Settings 59
 - Features 59
 - IP Blocklist 60
 - IP Allowlist 62
 - Precise Allowlist Management 64
 - Rule Allowlist 65
 - Statistics and Logs 66
 - Attack Logs 66
 - Access Logs 70
 - Log Shipping 77
 - IP Query 79
 - Rule Engine 80
 - Custom Policy 85
 - Webpage Anti-Tampering 88
 - Information Leakage Prevention 90
 - Regional Blocking 92
 - Attack Log 94
- Glossary 100



Product Introduction

WAF Overview

Web Application Firewall (WAF) is a one-stop, AI-based risk prevention solution for web business operations. It identifies malicious traffic using AI and rule engines to protect websites, enhancing overall security and reliability. By leveraging bot behavior analysis, it defends against malicious access requests and safeguards critical website services and data.

Converge Cloud provides an on-cloud WAF called CLB WAF, which offers robust protection through seamless integration with the Converge Cloud CLB cluster.

- CLB WAF works by mirroring HTTP/HTTPS traffic from CLB instances to the WAF cluster. The WAF performs real-time threat detection and cleansing, then synchronizes trusted request statuses back to the CLB cluster. This ensures that malicious traffic is blocked while legitimate requests are allowed, providing continuous and reliable website protection.

Converge Cloud WAF effectively prevents SQL injection, cross-site scripting (XSS), trojan uploads, unauthorized access, and other OWASP security risks. It also offers comprehensive protection against CC attacks, provides zero-day vulnerability patching, and helps prevent webpage tampering.

Feature	Description
AI + WAF	Web attack recognition is based on AI + rules, offering anti-bypass capability with low false negative and false positive rates. It effectively defends against common web attacks, including the OWASP Top 10 threats such as SQL injection, unauthorized access, cross-site scripting (XSS), cross-site request forgery (CSRF), and web shell trojan uploads.
Virtual zero-day vulnerability patching	The 24×7 Converge Cloud Security Team proactively identifies and responds to vulnerabilities. Within 24 hours, it issues virtual patches for zero-day and high-risk web vulnerabilities. Protected users receive instant and automatic protection, significantly reducing vulnerability response time.
Web tampering protection	Core web content can be cached to the cloud and published as substitute pages, preventing negative consequences from web page tampering.
Data leakage protection	Backend data is safeguarded through a three-phase defense strategy — pre-event server and application concealment, mid-event attack prevention, and post-event sensitive data replacement and concealment.



Feature	Description
CC attack protection	Smart CC protection automatically generates defense policies based on real server anomalies (e.g., timeouts, delays) and behavioral big data analysis. It supports multi-dimensional access control, intelligent filtering of malicious requests, and defense measures such as CAPTCHA and frequency control.
Crawler and bot traffic management	The AI + rules-based bot management system prevents risks from malicious bots such as data scraping, content infringement, price comparison, inventory crawling, malicious SEO, and strategy leakage.
30 BGP lines for access protection	With 30 dedicated BGP lines across protective nodes, WAF enables smart node scheduling to reduce access latency and ensure fast, stable connections — delivering strong cloud-based security without sacrificing performance.

Why WAF

Web Application Firewall (WAF) can effectively protect enterprise websites and business systems in the following use cases:

- **Data leakage (leakage of core information assets)**
A website is the entry to enterprise information assets and may be hacked for asset theft, causing incalculable losses to enterprises.
- **Malicious access and data crawling (unavailability and data utilized by competitors)**
Hackers control botnets to launch CC attacks on a website, which will consume all its resources and makes it unavailable. Malicious users scrape core content of websites (blog, recruitment, forum, and e-commerce websites) by using web crawlers.
For example, e-commerce offering details are crawled by competitors for analysis, and low-price offering information is crawled or promotion intelligence is obtained before sales campaigns by bargain hunters for their benefits.
- **Network trojans and tampering (affecting credibility and image)**
After obtaining website or server permissions, attackers can inject malicious code to make users execute malicious programs, drive traffic, steal accounts, and show off. They may also implant links to pornographic, gambling, and illegal information or tamper with the images and texts on the website, adversely affecting website operations, undermining the credibility, and damaging the image.
- **Framework vulnerability (attacks during patching)**
Many web systems are based on common open-source frameworks such as Struts 2, Spring, and



WordPress, which are prone to security vulnerabilities. A lot of attacks will emerge just one day after the vulnerabilities are discovered, making patching extremely hard.

- Business interruption due to high-traffic DDoS attacks

DDoS attacks have become a cost-effective and easy way to interrupt the business of competitors or make their key portals inaccessible. These attacks have severe impact on business continuity and brand image. More often than not, companies are very passive when attacked.



Product Category

Converge Cloud provides two types of cloud WAF, namely, SaaS WAF and CLB WAF. They have basically the same security protection capabilities but different connection methods and use cases. You can select an appropriate WAF type based on your actual deployment.

CLB WAF

Connect Method Overview

Connect Type	Connect Steps
CLB Domain Onboarding	Configure the domain and Layer-7 Load Balancer (CLB) resources (listeners) in the WAF console. This allows bypass threat detection and cleansing of HTTP/HTTPS traffic passing through the load balancer listener, achieving separation of business forwarding and security protection.
CLB Instance Object Onboarding	Enable Layer-7 Load Balancer (CLB) instance connect to WAF in the WAF console. This allows bypass threat detection and cleansing of HTTP/HTTPS traffic passing through the load balancer instance, achieving separation of business forwarding and security protection.
API Gateway and Serverless Cloud Function Domain Onboarding	Enable WAF protection through the API Gateway console (refer to API Gateway product documentation) and SCF console, then configure the domain in the WAF console. This allows bypass threat detection and cleansing of HTTP/HTTPS traffic passing through the API Gateway and SCF, achieving separation of business forwarding and security protection.
API Gateway Instance Object Onboarding	Enable WAF protection in the API Gateway console (refer to API Gateway product documentation) and in the WAF console, then enable API Gateway (instance) connect to WAF. This allows bypass threat detection and cleansing of HTTP/HTTPS traffic passing through the API Gateway instance, achieving separation of business forwarding and security protection.

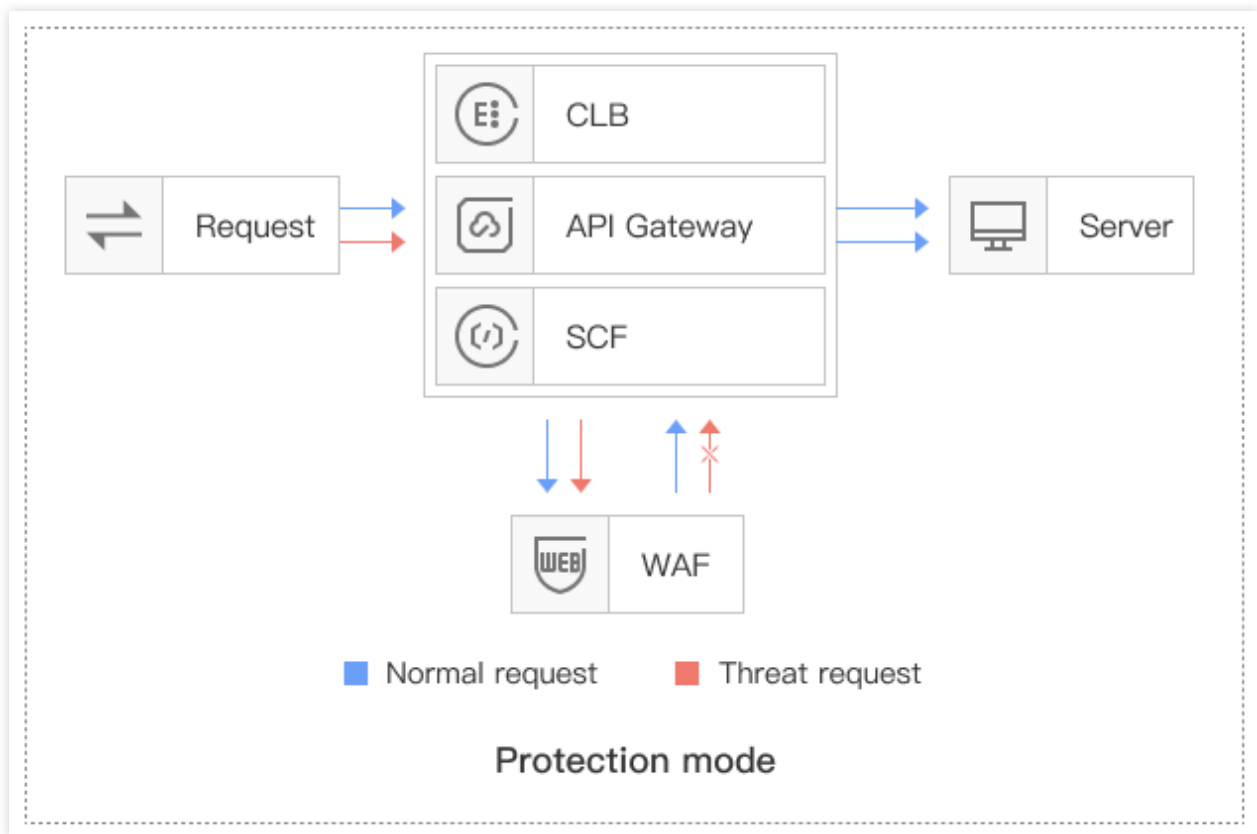
Traffic Processing Mode

CLB WAF provides two traffic processing modes:

- Protection mode

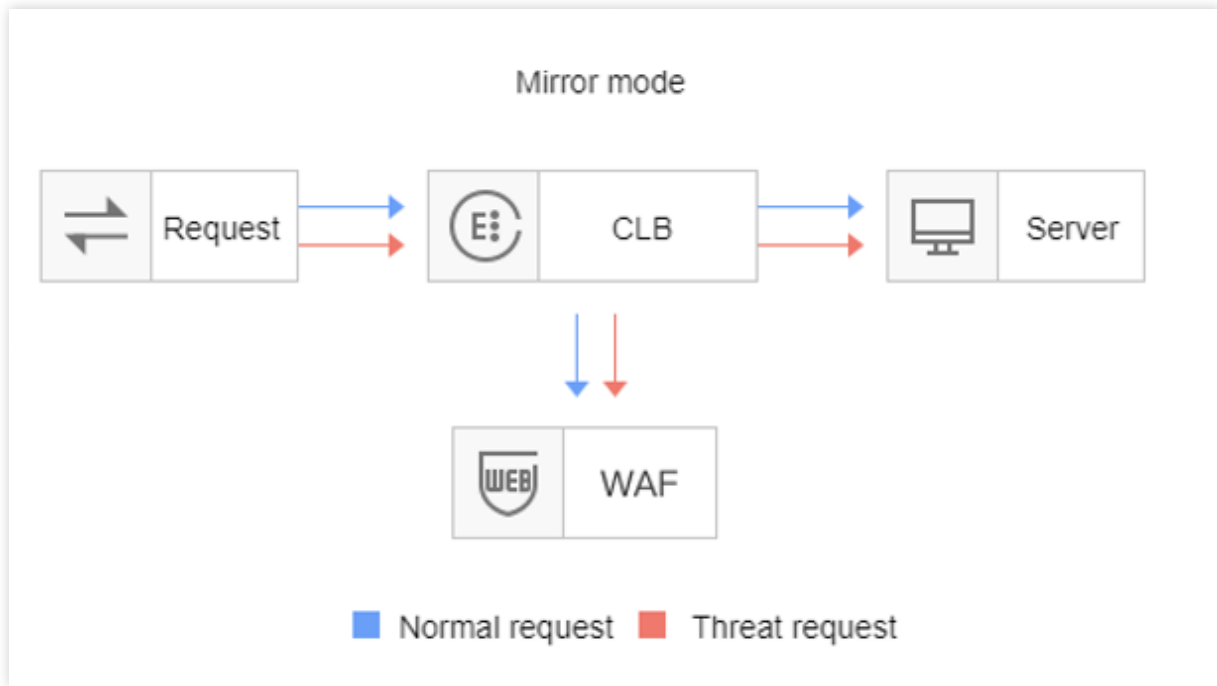
By associating through the domain, CLB, API Gateway, and SCF forward business traffic to the WAF cluster, where WAF performs bypass detection and alerts, synchronizes the request's trusted status,

and the gateway cluster intercepts or allows the request based on the status.



- Mirror mode

By associating through the domain, CLB mirrors traffic to the WAF cluster, where WAF performs bypass detection and alerts, without returning the request's trusted status



Strengths

Multiple Access Methods

- Supports quick access to WAF services without any application adjustment, and provides quick binding to Converge Cloud CLB to perform bypass detection and traffic cleansing with the quick bypass feature, which can separate business request forwarding from security protection.
- Supports access to WAF services through CNAME, hiding your real server and forwarding trusted traffic to the real server for Converge Cloud and non-Converge Cloud users.
- Supports cross-region deployment of cluster protection resources, dynamic scaling, and on-demand usage to avoid redundancy and single points of failure.

Protection from AI Engine and Rule Engine

- The security rule engine protects your business against the OWASP Top 10 attacks, including SQL injection, unauthorized access, cross-site scripting (XSS), cross-site request forgery (CSRF), and command line injection. WAF is also powered with AI defense capabilities to enable continuous learning through cross-validation and accurately and effectively capture common web attacks, zero-day attacks, and other new unknown attacks.
- WAF continuously learns the characteristics of massive business data to generate business-oriented personalized protection policies and avoid false positives. You can use the AI engine to handle false positives and false negatives to improve operation efficiency.
- Converge Cloud Security Laboratory provides outstanding security protection capabilities for Converge Cloud. WAF's protection systems are continuously upgraded by the dedicated protection team 24/7, building up cutting-edge protection systems for your website.

Bot Traffic Management

- With the AI-based behavior analysis engine, this feature realizes real-time session tracking, and efficient detection of malicious bots based on the matching of behavior models and behavior labels by using traffic profile.
- Provides more than 1,000 known bot types to quickly set up protection policies.
- Provides crawler and IP intelligence features to quickly identify bot behaviors.
- Provides features of protocols and over 50 sessions to define protection policies for various scenarios.
- Provides detailed reports and statistics of known, unknown, and custom bot types to quickly locate malicious bots and defend your website against them.



Intelligent Protection Against CC Attacks

- Intelligently generates and applies protection policies to defeat attacks and blocks high-frequency access requests in real time to block attacker IPs based on the real server's abnormal response such as timeout and response latency, and historical data of website access.
- Supports custom sessions to defend against CC attacks at the session level, realizing more accurate protection against CC attacks and fewer false positives.
- Allows you to view IP addresses that are blocked due to CC protection in real time to quickly adjust protection policies as needed.
- Supports quick access to 100 Gbps of Anti-DDoS capability to defend against traffic-intensive DDoS attacks, helping you easily cope with sudden attacks.

Scenarios

Government Website Protection

WAF allows you to quickly connect to the protection service. Then, you can simply configure parameters to hide your real server and protect your website content from tampering, thereby ensuring the availability of government services and smooth user access.

Ecommerce Website Protection

WAF provides continuous optimization of protection rules, precise blocking of Web attacks, and all-round protection against OWASP Top 10 Web application risks. In case of highly concurrent purchases, it can intelligently filter malicious attacks and junk access to ensure smooth access to businesses.

Finance Website Protection

WAF can be accessed with one click, and integrates with the large-traffic Converge Cloud DDoS defense, and also provides web security protection. WAF can effectively detect abnormal access like account credential enumeration attack to avoid user information leakage. With cloud resources and automatic scaling capability, WAF can easily deal with sudden business growth and large-traffic CC attacks.

Data Leakage Protection

WAF can avoid website core data leakage caused by hacker injection and intrusion attacks. CC attack protection: Protection against malicious CC (HTTPFlood) attacks. WAF can ensure website availability by blocking massive malicious requests on layer 4 and layer 7.

Basic Concepts

SSL Certificate

Secure Sockets Layer (SSL) is a security protocol designed to ensure the security and data integrity of internet communication. Based on the SSL protocol, an SSL certificate can be installed on a server to achieve encrypted data transmission.

Domain Name Resolution

Servers on the internet communicate with each other through IP addresses. However, most people are used to remembering a domain name that can be mapped to multiple IP addresses. The conversion between a domain name and an IP address is called domain name resolution.

The following are common domain name resolution types:

- A record resolution: It specifies the IPv4 address of the domain name.
 - Select "A" as the record type.
 - Enter the server IP address provided by Converge Cloud as the record value.
 - MX priority does not need to be configured.
 - Set TTL to 600 by default.
- CNAME record resolution: It is used to point a domain name to another one which will be used to provide the IP address.
 - Select "CNAME" as the record type.
 - Enter the CNAME record generated after the protected domain name is added to WAF as the record value.
 - MX priority does not need to be configured.
 - Set TTL to 600 by default.

Security Group

A security group is a virtual firewall that features stateful data packet filtering. It is used to configure the network access control of CVM instances. You can add CVM instances with the same network security isolation requirements in the same region to the same security group to filter their inbound and outbound traffic through the network policies of the security group.

QPS

Queries per second (QPS) is a metric measuring how much traffic is processed by a particular query server within the specified time period. On the internet, the performance of DNS servers is often measured with QPS, which corresponds to fetches/sec (responded requests per second, i.e., the maximum throughput).



Intermediate IP Address

After you add a domain name, WAF will automatically allocate multiple intermediate IP addresses to it accordingly, which can be used as the egress IPs of WAF to forward filtered normal traffic to your real server.

CC Attack Protection

Challenge Collapsar (CC) attack protection refers to a protection service against CC attacks where attackers use certain tools to simulate multiple users in order to continuously send connection requests to your website and make your business unavailable. You can add CC protection rules to defend against CC attacks for webpage requests.

Tamper Protection

Tamper protection refers to a mechanism where core webpages can be cached to the cloud and those in the cache can be published instead to realize the effect of webpage substitution. When the core webpages receive requests, content stored in cloud will be returned.

Leakage Protection

Leakage protection refers to a mechanism where the responding webpages are checked for sensitive information such as ID and phone numbers and any sensitive information detected will be observed or replaced with asterisks (*) according to the preset match behaviors, which helps avoid leakage of sensitive information.

Region Blocking

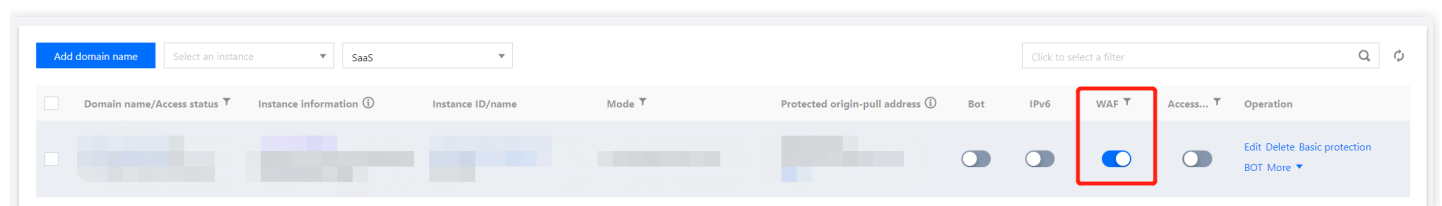
Region blocking refers to a mechanism that determines the region of an attacking IP and blocks access requests from all IPs in the specific region in order to quickly block attacks.

Quick Bypass

Quick bypass refers to a feature that can quickly switch to pure forwarding. On the domain name



management page, you can select the target domain name and click to enable this feature and quickly allow all blocked traffic for a swift business recovery.



Purchase Guide

Billing Overview

Currently, WAF is available as CLB WAF instances with different plans. You can select a WAF instance and plan according to your business needs.

WAF supports only the monthly subscription (prepaid) billing mode and does not support pay-as-you-go.

Billing Mode

WAF adopts a billing structure consisting of a basic plan plus extra packs or value-added capabilities:

- **Basic Plan (Required):**
You can purchase it under the prepaid billing mode. (*Pricing details are omitted.*)
For more information on plans and extra packs, see the pricing on the purchase page.
- **Extra Packs (Optional):**
After purchasing the basic plan, you can add extra domain packs and business packs (extra QPS packs) to upgrade the instance specifications.
- **Value-Added Capabilities (Optional):**
After purchasing the basic plan, you can opt to add security log packs and bot traffic management for enhanced protection.

Note:

For more information on the expiration of prepaid WAF instances, see [Prepaid Billing](#).



Purchase Guide

Currently, WAF is available as CLB WAF instances. For more information, see [Basic Plan Specification Description](#).

You can select a WAF instance and plan according to your business needs.

WAF supports only the monthly subscription (prepaid) billing mode and does not support pay-as-you-go.

Purchase Process

1. Log in to the Converge Cloud console.
2. Go to the WAF purchase page.
3. On the purchase page, select the desired instance type, region, extra domain pack, extra QPS pack, security log pack, and validity period, then click Buy Now.
For more information, see [Billing Overview](#).
4. Complete the payment.

Subsequent Operations

After purchasing a CLB WAF instance, you can manage and configure it as instructed in [Getting Started](#).

Payment Overdue

If you are a customer of a Converge Cloud partner, the rules regarding resources when there are overdue payments are subject to the agreement between you and the partner.

This document describes the payment overdue policy and data repossession mechanism of WAF, a monthly subscribed product.

Expiration Alert

From seven days before the expiration of your WAF resource until it is released, the system will send an alert to your Converge Cloud account creator, global resource collaborators, and financial collaborators via email, SMS, and Message Center as configured in the message subscription in the Message Center.

For more information on the alert mechanism from seven days before the expiration of your resource until it is released, see Prepaid Billing.

Note:

If your account balance is sufficient and you previously enabled auto-renewal, the system will perform renewal automatically on the expiration date.

If your account balance is insufficient for automatic renewal, the system will dispatch a notification stating, "Auto-renewal cannot proceed due to insufficient balance, an account charge is required." This notification will be communicated via email, SMS, and in-platform messages, and is scheduled to be sent every day. Additionally, a voice call alert will be triggered a day before expiration (the actual mode of communication depends on your subscription settings in the Message Center).

Overdue Payment Reminder

On and after the day of expiration of your WAF instance resource, the system will send alerts for resource isolation to your Converge Cloud account creator and all collaborators via email, SMS, and Message Center as configured in the message subscription in the Message Center.

Repossession

- The system will send renewal reminder notices to users seven days prior to the expiration of the Web Application Firewall resource.
- Within seven days of the Web Application Firewall expiration, you can still use the service. Renewal should be carried out promptly; a reminder of the expiration will be sent by the system.
- Once eight days since the Web Application Firewall's expiration have passed, service will be terminated. Neither forwarding nor protection features will be available, and the system will reclaim the resource; associated configuration data will be abolished and cannot be recovered.

Warning:



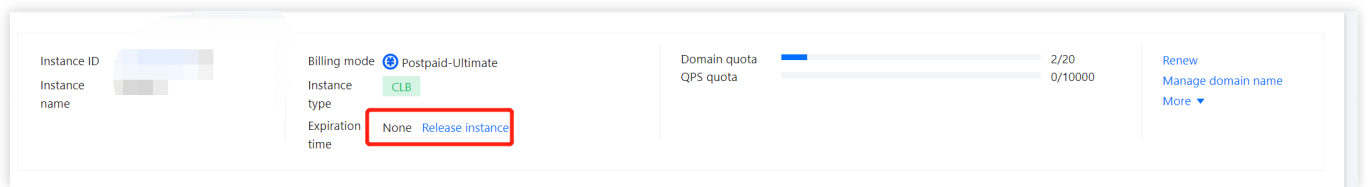
If you are certain that you no longer require the services of the Web Application Firewall, please ensure domain-related configurations have been transferred prior to discontinuation to avert any potential disruption to your services:

- DNS resolution will not be adjusted automatically. If you have decided that you will not be using the Web Application Firewall, please redirect your domain's DNS resolution to the original server. Failure to do so may lead to inaccessibility of web services.
- Automatic unbinding of the domain and the Cloud Load Balancer Listener will not happen. Please ensure this action takes place promptly before resource reclamation.

Releasing Instance Resource

After your WAF resources expire, you can release them in the console.

1. Log in to the WAF console and select Instance Management on the left sidebar.
2. On the Instance Management page, select the target instance and click Release Instance.



3. After the instance is released, the backend will clear all its configurations. If you still want to use it, cancel the operation and renew the instance as soon as possible.

Getting Started

Quick Deployment and Use of WAF Instance

This document describes how to quickly deploy and use a WAF instance. Specifically, purchase a WAF instance, organize the website domain name information, perform domain name connection and protection configuration, and get an overview of the business and security through the reports and stay on top of security status. You can view traffic processing details in attack logs and then adjust the protection configuration accordingly to meet special business needs. You can also use CM to configure different types of custom alarms and notification channels for more efficient Ops.

Step 1. Purchase an instance

You can purchase multiple WAF instances. Multi-instance management better suits your business division and management requirements and allows you to achieve nearby access and protection of multi-region active-active instances in a unified manner.

For more information on instance purchase, see [Purchase Guide](#).

For more information on instance management and renewal, see [Instance Management](#).

Step 2. Connect your website

Domain name connection guide for CLB WAF

CLB WAF associates with Converge Cloud Layer-7 CLB (listener) cluster by your domain name, and detects and purges HTTP or HTTPS traffic that goes through the CLB instance for side-channel threats. In this way, it can provide protection without interrupting your traffic forwarding. To achieve the above, you need to follow the steps below:

- Step 1. Confirm CLB configuration
- Step 2. Bind a domain name to the CLB instance
- Step 3. Verify the configuration

Step 3. Configure the protection

WAF will protect the traffic to the connected website. It has multiple detection and protection modules to help your website tackle different types of security threats. The rule engine is enabled by default and used to defend against common web application attacks such as SQL injection, XSS, and web shell upload. Other modules can be enabled and configured with protection rules manually as needed.

Step 4. Analyze logs

By default, WAF logs attacks only. After purchasing and activating the log service, you can have all access

requests logged by domain name.

Attack log

An attack log records the time, source IP, type, and details of an attack to facilitate real-time threat check and analysis as well as protection policy adjustment, fully meeting the needs of routine security Ops and business.

Currently, attacks are displayed in an aggregated manner; that is, logs of the same type from the same request source IP within a specific period are displayed as one log to reduce your Ops workload and improve the efficiency. Additionally, you can query attack logs with full-text search, fuzzy search, and search by filter. For more information, see [Attack Logs](#).

Access log

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 at least 180 days. For more information, see [Access Log](#).

Step 5. Generate a security report

After your website is connected to WAF for protection, you can go to the WAF overview page to query the current total number of domain names, connected website conditions, instance conditions, website business and attack traffic analysis data in the last 30 days, and rule updates. In this way, you can have a better picture of the overall security of your website business. For more information, see [Access Log](#).

Step 6. Configure alarms in CM

After your website is connected to WAF protection, you can configure alarms in CM. Then, WAF will send you alarm notifications when exceptions are detected in the website request traffic and business traffic, so you can stay informed of your business security changes. In this way, you can quickly respond to exceptions and adjust WAF policies to ensure business stability and security.

You can configure the same domain name into instances of the same type in different regions to separate the connection configurations of forwarding and protecting resources while using the same protection policy.

Operation Guide

Overview

The Overview page allows you to get an overall picture of the security status of your domain name.

Security Overview

1. Log in to the Converge Cloud WAF console and select Overview on the left sidebar. Then open the Security Overview tab.
2. Select a domain name to view data that measures the security status of the domain name.

Instance Overview

To view expired instances under your account, select a domain name and click Include x instances. # Overview Page

The Overview page allows you to get an overall picture of the security status of your domain name.

Security Overview

1. Log in to the Converge Cloud WAF console and select Overview on the left sidebar. Then open the Security Overview tab.
2. Select a domain name to view data that measures the security status of the domain name.

Instance Overview

To view expired instances under your account, select a domain name and click Include x instances.

Rule Updates

By clicking See more in the rule updates section, you can view WAF supported rules in detail.

Attacks Overview

All domain names

1. When "All domain names" is selected, all attack data are displayed. You can also set a time range to display data you want to see.
2. At the lower part of the page, you can view the following information including top 5 domain names by web attacks, top 5 attacker IPs, and top 5 domain names by CC attacks.

Field description:

- Top 5 domain names by web attacks: It displays five domain names that suffer web attacks most frequently.

- Top 5 attacker IPs: It displays five IPs that initiate attacks most frequently.
- Top 5 domain names by CC attacks: It displays five domain names that suffer CC attacks most frequently.
- Top 5 requester IPs: It displays five IPs that send access requests most frequently.
- Distribution of attacker IPs: It displays how the attacker IPs distribute across regions.
- Types of attacks (%): It displays the distribution of the attack types.
- Types of browsers (%): It displays the distribution of the browser types.

Single domain name

1. When a specific domain name is selected, the corresponding attack data is displayed. You can also set a time range to display data you want to see.
2. At the lower part of the page, you can view the following information including top 5 attacker IPs, top 5 requester IPs, and distribution of attacker IPs.

Field description:

- Top 5 attacker IPs: It displays five IPs that initiate attacks most frequently.
- Top 5 requester IPs: It displays five IPs that send access requests most frequently.
- Distribution of attacker IPs: It displays how the attacker IPs distribute across regions.
- Types of attacks (%): It displays the distribution of the attack types.
- Types of browsers (%): It displays the distribution of the browser types.

Overview of Security Analysis

- Basic security analysis: It displays the number of web attacks on the selected domain name during the specified period.
- Application operation analysis: It displays the QPS and bandwidth of the selected domain name on the left, and top 5 slowest pages and top 5 most visited pages on the right.
- If the actual business QPS peak exceeds the user instance specification value or 80% of the specification value, the QPS trend analysis page will display the corresponding WAF instance specification value.
 - If All Resources is selected, the trend graphs of the most recent 3 instances exceeding the limit will be displayed by default, along with their QPS specification values.
 - If a single WAF instance resource is selected, the instance specification value and corresponding over-limit alert events will be displayed by default. For the detailed calculation method of the WAF instance QPS rule value, please refer to Sandbox Isolation Status.
- Application security analysis: It displays the bot information of the selected domain name during the specified period. To view more details, you can click View bot traffic analysis.

Rule Updates



By clicking See more in the rule updates section, you can view WAF supported rules in detail.

Attacks Overview

All domain names

1. When "All domain names" is selected, all attack data are displayed. You can also set a time range to display data you want to see.
2. At the lower part of the page, you can view the following information including top 5 domain names by web attacks, top 5 attacker IPs, and top 5 domain names by CC attacks.

Field description:

- Top 5 domain names by web attacks: It displays five domain names that suffer web attacks most frequently.
- Top 5 attacker IPs: It displays five IPs that initiate attacks most frequently.
- Top 5 domain names by CC attacks: It displays five domain names that suffer CC attacks most frequently.
- Top 5 requester IPs: It displays five IPs that send access requests most frequently.
- Distribution of attacker IPs: It displays how the attacker IPs distribute across regions.
- Types of attacks (%): It displays the distribution of the attack types.
- Types of browsers (%): It displays the distribution of the browser types.

Single domain name

1. When a specific domain name is selected, the corresponding attack data is displayed. You can also set a time range to display data you want to see.
2. At the lower part of the page, you can view the following information including top 5 attacker IPs, top 5 requester IPs, and distribution of attacker IPs.

Field description:

- Top 5 attacker IPs: It displays five IPs that initiate attacks most frequently.
- Top 5 requester IPs: It displays five IPs that send access requests most frequently.
- Distribution of attacker IPs: It displays how the attacker IPs distribute across regions.
- Types of attacks (%): It displays the distribution of the attack types.
- Types of browsers (%): It displays the distribution of the browser types.

Overview of Security Analysis

- Basic security analysis: It displays the number of web attacks on the selected domain name during the specified period.
- Application operation analysis: It displays the QPS and bandwidth of the selected domain name on

the left, and top 5 slowest pages and top 5 most visited pages on the right.

- If the actual business QPS peak exceeds the user instance specification value or 80% of the specification value, the QPS trend analysis page will display the corresponding WAF instance specification value.
 - * If All Resources is selected, the trend graphs of the most recent 3 instances exceeding the limit will be displayed by default, along with their QPS specification values.
 - * If a single WAF instance resource is selected, the instance specification value and corresponding over-limit alert events will be displayed by default. For the detailed calculation method of the WAF instance QPS rule value, please refer to Sandbox Isolation Status.
- Application security analysis: It displays the bot information of the selected domain name during the specified period. To view more details, you can click View bot traffic analysis.

Best Practices

Building a CLB WAF Test Environment

Creating a CVM

1. Log in to the tenant side, enter the CVM page, select the corresponding region, and click Create.
2. Select the network consistent with the CLB network, select other options according to the actual situation, and click Next: Select Image.
3. After selecting the image according to the actual situation, click Next: Select Storage and Bandwidth.
4. After selecting the storage and bandwidth according to the actual situation, click Next: Set Security Group and Host.
5. After selecting the security group and host according to the actual situation, enter the host password and click Next: Confirm Configuration Information.
6. Check the information you just selected. After confirming that everything is correct, click Enable.

Applying for an EIP and Binding It to the CVM

1. Under the CVM menu, click Elastic IP, select the same region as the CVM region, and click Apply. Then select options according to the actual situation.
2. Click Confirm to return to the Elastic IP List page, and you can see that the created elastic IP address is displayed as Unbound.
3. Click the Operation column on the Elastic IP page, click More, and select Bind.
4. Select the CVM you want to bind and click Confirm.
5. Check the information that needs to be confirmed. After confirming that everything is correct, click Confirm.
6. Go to the Elastic IP List page. You can see that the created EIP address is displayed as Bound.

Installing Nginx and Enabling Port 80

1. Click the CVM ID. On the CVM parameter page, copy the server ID of the CVM.
2. Enter CVM on the operation side, choose VM Management > Tenant-Side Resources, select UUID in the search box, and then paste the server ID you just copied to find the private IP address of the host.
3. Log in to the private IP address of the host and enter the command: `ssh host private IP address` . The

password is the one entered when you activated CVM.

4. Enter the `virsh console UUID --force` command. For example, enter the `virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force` command to enter CVM.

```
[root@kvm-3_12 ~]# virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force
Connected to domain 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11
Escape character is ^]

[root@VM_0_12_centos ~]#
```

5. After entering CVM, enter the following command to perform an installation:

Install: `<1>yum install -y nginx`

Start the Nginx service: `service nginx start` .

Check whether port 80 is enabled: `netstat -nap|grep 80` .

```
[root@VM_0_12_centos ~]# netstat -nap|grep 80
tcp        0      0 0.0.0.0:80          0.0.0.0:*          LISTEN     20928/nginx: master
tcp6       0      0 :::80             :::*                LISTEN     20928/nginx: master
udp6       0      0 fe80::5054:ff:febc::123 :::*                6695/ntpd
```

Forwarding Ports Using NAT Gateway (If Required)

1. Under the VPC menu, select NAT Gateway. After selecting the corresponding region, click Create to create a NAT gateway.
2. Enter information according to the actual situation and click Create to return to the NAT Gateway List page.
3. In the created NAT gateway, click the gateway ID.
4. Click Port Forwarding.
5. Click Create.
6. Add a port to be forwarded.
7. Under VPC, select Route Table. Under the corresponding region, click Create to create a route table.
8. Enter information and click Create. Select the policy as the added NAT gateway.
9. A prompt indicates that you need to associate a subnet. After selecting the associated subnet, click OK to return to the Route Table List page.

Visiting `http:// Public IP Address:788/` to Verify Whether the Website Is Normal

Adding a CLB Instance and Listener

1. Click CLB. On the LB Instance List page, click Create.
2. Enter information according to the actual situation. The CLB should be consistent with that of the CVM network. Then click Confirm Activation.
3. On the Purchase Confirmation page, click Confirm.
4. Click Finish.
5. On the LB Instance List page, view the instance you just created and click the instance ID.
6. Click Listener Management.
7. Click Create or Start Creation to create a listener.
8. Enter the name, protocol, and port number. Enter the port number forwarded through the NAT gateway, such as 788. Then click OK.
9. Click Start Creation under the listener and enter the domain name to be configured. For subsequent steps, see "Binding HTTP Listeners in CLB Instance" in the "Functional Test Case (CLB) Tenant Side" documentation.

Adding Engine Nodes for CLB WAF

1. Log in to the operation side. In Virtual Machine Management > Operation-side Resource in the CVM, allocate engine node IP addresses after submitting a request to the environment administrator.
2. Log in to the WAF operation side and click Add in Cluster Management.
3. Enter the engine IP addresses, use ";" to separate them, and click Confirm.
4. The IP addresses are added successfully.

Building a SaaS WAF Origin Server

When you create a SaaS WAF domain name, you need to enter the origin server address. The origin server address only needs to be connected to the SaaS WAF engine. The origin server IP address can be either a private IP address or a public IP address. Next, an origin server of the private IP address type and an origin server of the public IP address type will be created, respectively.

1. Origin Server with a Private IP Address

1. Log in to the operation side, select CVM to create a CVM. Click Operation-side Resource and click Create.
2. After configuring all information on the Create CVM page, view the newly added CVM.
3. Enter the newly-added CVM.

![] (When you create a SaaS WAF domain name, you need to enter the origin server address. The origin server address only needs to be connected to the SaaS WAF engine. The origin server IP address can be either a private IP address or a public IP address. Next, an origin server of the private IP address type and an origin server of the public IP address type will be created, respectively.

1. Origin Server with a Private IP Address

1. Log in to the operation side, select CVM to create a CVM. Click Operation-side Resource and click Create.
2. After configuring all information on the Create CVM page, view the newly added CVM.
3. Enter the newly-added CVM.

```
[root@tcs-10-27-0-6 ~/v_yurenzhou]# cat 154.87.sh
#!/bin/sh

sshpas -p 20070 ssh root@.154.87 -p 22
```

```
[root@tcs-10-27-0-6 ~/v_yurenzhou]# . 154.87.sh
Warning: Permanently added '154.87' (ECDSA) to the list of known hosts.
[root@VM_154_87_linux ~]# ll
total 4
-rw-r--r-- 1 root root 90 1 6 23:01 test
[root@VM_154_87_linux ~]# find / -name nginx
```

4. Install Nginx in the CVM and enter the `<1>yum install -y nginx`

```
[root@VM_154_87_linux ~]# yum -y install nginx
fastestmirror, langpacks
epel | 4.7 kB 00:00:00
extras | 2.9 kB 00:00:00
os | 3.6 kB 00:00:00
updates | 2.9 kB 00:00:00
(1/7): epel/7/x86_64/group_gz | 95 kB 00:00:00
(2/7): extras/7/x86_64/primary_db | 206 kB 00:00:00
(3/7): os/7/x86_64/group_gz | 153 kB 00:00:00
(4/7): epel/7/x86_64/updateinfo | 1.0 MB 00:00:00
(5/7): os/7/x86_64/primary_db | 6.1 MB 00:00:00
(6/7): updates/7/x86_64/primary_db | 3.8 MB 00:00:00
(7/7): epel/7/x86_64/primary_db | 6.9 MB 00:00:00
Determining fastest mirrors
```

Start the Nginx service: `service nginx start` .

Check whether port 80 is enabled: `netstat -nap|grep nginx` .

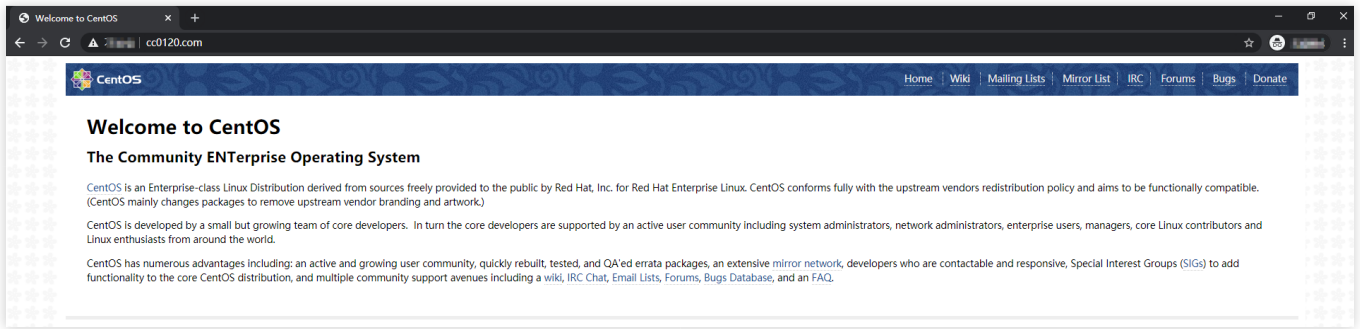
```
[root@VM_154_87_linux ~]# service nginx start
Redirecting to /bin/systemctl start nginx.service
[root@VM_154_87_linux ~]# netstat -nap |grep nginx
tcp        0      0 0.0.0.0:80          0.0.0.0:*          LISTEN      27979/nginx: master
tcp6       0      0 :::80              :::*                LISTEN      27979/nginx: master
unix  3      [ ]          STREAM  CONNECTED  103293  27979/nginx: master
unix  3      [ ]          STREAM  CONNECTED  103296  27979/nginx: master
unix  3      [ ]          STREAM  CONNECTED  103295  27979/nginx: master
unix  3      [ ]          STREAM  CONNECTED  103294  27979/nginx: master
```

5. In the SaaS engine, use the ping or telnet command to test whether the IP address and port of the CVM are connected.

```
[root@VM_12_7_centos ~]# ping 10.10.154.87
PING 10.10.154.87 (10.10.154.87) 56(84) bytes of data.
64 bytes from 10.10.154.87: icmp_seq=1 ttl=53 time=0.823 ms
64 bytes from 10.10.154.87: icmp_seq=2 ttl=53 time=0.832 ms
^C
--- 10.10.154.87 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.823/0.827/0.832/0.029 ms
```

```
[root@VM_12_7_centos ~]# telnet 10.10.154.87 80
Trying 10.10.154.87...
Connected to 10.10.154.87.
Escape character is '^]'.
^]
telnet>
```

6. Add a domain name in SaaS WAF. For the origin server IP address, enter the CVM IP address you applied for.
7. Configure a host and access the newly added domain name. You can access the origin server of the private IP address type.



2. Origin Server with a Public IP Address

1. Log in to the tenant side, go to the CVM page, select the corresponding region, and click Create.
2. Select the network consistent with the CLB network, select other options according to the actual situation, and click Next: Select Image.
3. After selecting the image according to the actual situation, click Next: Select Storage and Bandwidth.
4. After selecting the storage and bandwidth according to the actual situation, click Next: Set Security Group and Host.
5. After selecting the security group and host according to the actual situation, enter the host password and click Next: Confirm Configuration Information.
6. Check the information you just selected. After confirming that everything is correct, click Enable.
7. Apply for an elastic IP address and bind it to the CVM. Under the CVM menu, click Elastic IP, select the same region as the CVM region, and click Apply. Then select options according to the actual situation.
8. Click Confirm to return to the Elastic IP List page, and you can see that the created elastic IP address is displayed as Unbound.
9. Click the Operation column on the Elastic IP page, click More, and select Bind.
10. Select the CVM you want to bind and click Confirm.
11. Check the information that needs to be confirmed. After confirming that everything is correct, click Confirm.
12. Go to the Elastic IP List page. You can see that the created EIP address is displayed as Bound.

13. Install Nginx, enable port 80, and then click the CVM ID. On the CVM parameter page that appears, copy the server ID of the CVM.
14. Enter CVM on the operation side, choose VM Management > Tenant-Side Resources, select UUID in the search box, and then paste the server ID you just copied to find the private IP address of the host.
15. Log in to the private IP address of the host and enter the command: `ssh host private IP address` . The password is the one entered when you activated CVM.

```
WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Fri Sep 11 10:40:09 2020 from 10.10.240.32
[root@vm_17_41-centos ~]# ssh 3.12
root@3.12's password:
Last login: Fri Sep 11 10:54:47 2020 from .19.77
Welcome to tlinux 2.2 64bit
Version 2.2 20200119
[root@kvm_3_12 ~]#
```

16. Enter the `virsh console UUID --force` command. For example, enter the `virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force` command to enter CVM.

```
[root@kvm_3_12 ~]# virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force
Connected to domain 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11
Escape character is ^]

[root@VM_0_12-centos ~]#
```

17. After entering CVM, enter the following command to perform an installation:

Install: `<1>yum install -y nginx`

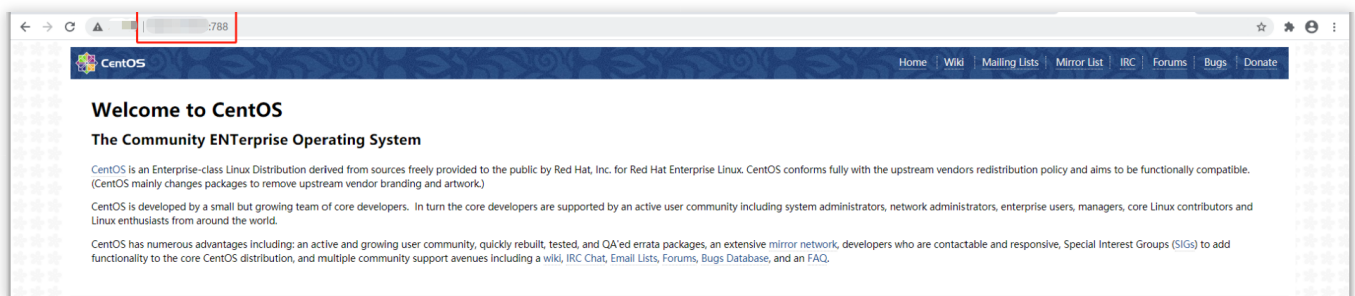
Start the Nginx service: `service nginx start` .

Check whether port 80 is enabled: `netstat -nap|grep 80` .

```
[root@VM_0_12-centos ~]# netstat -nap|grep 80
tcp        0      0 0.0.0.0:80          0.0.0.0:*          LISTEN     20928/nginx: master
tcp6       0      0 :::80              :::*                LISTEN     20928/nginx: master
udp6       0      0 fe80::5054:ff:feb::123 :::*                6695/ntpd
```

18. Since some customers prohibit external access to ports 80 and 443 on their public IP addresses, you need to forward port 80 of the CVM to another port (for example, port 788) through a NATGW, and associate this gateway in the route table (ignore steps 2.18 to 2.26 if it is not involved). Under the VPC menu, select NAT Gateway. After selecting the corresponding region, click Create to create a NAT gateway.
19. Enter information according to the actual situation and click Create to return to the NAT Gateway List page.

20. In the created NAT gateway, click the gateway ID.
21. Click Port Forwarding.
22. Click Create.
23. Add a port to be forwarded.
24. Under VPC, select Route Table. Under the corresponding region, click Create to create a route table.
25. Enter information and click Create. Select the policy as the added NAT gateway.
26. A prompt indicates that you need to associate a subnet. After selecting the associated subnet, click OK to return to the Route Table List page.
27. Visiting `http://Public IP Address:788/` to Verify Whether the Website Is Normal



28. Add a domain name in SaaS WAF. For the origin server IP address, enter the elastic IP address.
)

```
[root@tcs-10-27-0-6 ~/v_yurenzhou]# . 154.87.sh
Warning: Permanently added '[redacted] 154.87' (ECDSA) to the list of known hosts.
[root@VM_154_87_linux ~]# ll
total 4
-rw-r--r-- 1 root root 90 1 6 23:01 test
[root@VM_154_87_linux ~]# find / -name nginx
```

29. Install Nginx in the CVM and enter the `<1>yum install -y nginx`

```
[root@VM_154_87_linux ~]# yum -y install nginx
fastestmirror, langpacks
epel | 4.7 kB 00:00:00
extras | 2.9 kB 00:00:00
os | 3.6 kB 00:00:00
updates | 2.9 kB 00:00:00
(1/7): epel/7/x86_64/group_gz | 95 kB 00:00:00
(2/7): extras/7/x86_64/primary_db | 206 kB 00:00:00
(3/7): os/7/x86_64/group_gz | 153 kB 00:00:00
(4/7): epel/7/x86_64/updateinfo | 1.0 MB 00:00:00
(5/7): os/7/x86_64/primary_db | 6.1 MB 00:00:00
(6/7): updates/7/x86_64/primary_db | 3.8 MB 00:00:00
(7/7): epel/7/x86_64/primary_db | 6.9 MB 00:00:00
Determining fastest mirrors
```

Start the Nginx service: `service nginx start` .

Check whether port 80 is enabled: `netstat -nap|grep nginx` .

```
[root@VM_154_87_linux ~]# service nginx start
Redirecting to /bin/systemctl start nginx.service
[root@VM_154_87_linux ~]# netstat -nap |grep nginx
tcp        0      0 0.0.0.0:80          0.0.0.0:*        LISTEN      27979/nginx: master
tcp6       0      0 :::80              :::*              LISTEN      27979/nginx: master
unix  3      [ ]          STREAM  CONNECTED  103293  27979/nginx: master
unix  3      [ ]          STREAM  CONNECTED  103296  27979/nginx: master
unix  3      [ ]          STREAM  CONNECTED  103295  27979/nginx: master
unix  3      [ ]          STREAM  CONNECTED  103294  27979/nginx: master
```

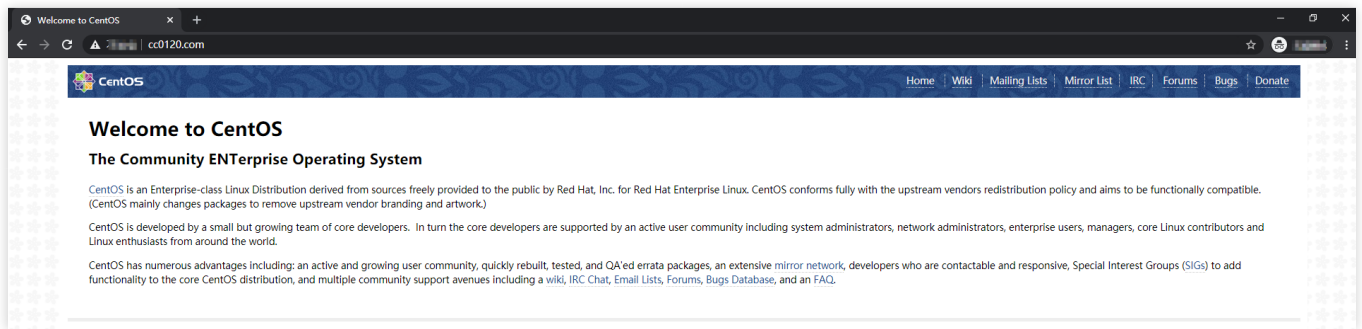
30. In the SaaS engine, use the ping or telnet command to test whether the IP address and port of the CVM are connected.

```
[root@VM_12_7_centos ~]# ping 10.10.154.87
PING 10.10.154.87 (10.10.154.87) 56(84) bytes of data.
64 bytes from 10.10.154.87: icmp_seq=1 ttl=53 time=0.823 ms
64 bytes from 10.10.154.87: icmp_seq=2 ttl=53 time=0.832 ms
^C
--- 10.10.154.87 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.823/0.827/0.832/0.029 ms
```

```
[root@VM_12_7_centos ~]# telnet 10.10.154.87 80
Trying 10.10.154.87...
Connected to 10.10.154.87.
Escape character is '^]'.
^]
telnet>
```

31. Add a domain name in SaaS WAF. For the origin server IP address, enter the CVM IP address you applied for.

32. Configure a host and access the newly added domain name. You can access the origin server of the private IP address type.



2. Origin Server with a Public IP Address

1. Log in to the tenant side, go to the CVM page, select the corresponding region, and click Create.
2. Select the network consistent with the CLB network, select other options according to the actual situation, and click Next: Select Image.
3. After selecting the image according to the actual situation, click Next: Select Storage and Bandwidth.
4. After selecting the storage and bandwidth according to the actual situation, click Next: Set Security Group and Host.
5. After selecting the security group and host according to the actual situation, enter the host password and click Next: Confirm Configuration Information.
6. Check the information you just selected. After confirming that everything is correct, click Enable.
7. Apply for an elastic IP address and bind it to the CVM. Under the CVM menu, click Elastic IP, select the same region as the CVM region, and click Apply. Then select options according to the actual situation.
8. Click Confirm to return to the Elastic IP List page, and you can see that the created elastic IP address is displayed as Unbound.
9. Click the Operation column on the Elastic IP page, click More, and select Bind.
10. Select the CVM you want to bind and click Confirm.
11. Check the information that needs to be confirmed. After confirming that everything is correct, click Confirm.
12. Go to the Elastic IP List page. You can see that the created EIP address is displayed as Bound.

13. Install Nginx, enable port 80, and then click the CVM ID. On the CVM parameter page that appears, copy the server ID of the CVM.
14. Enter CVM on the operation side, choose VM Management > Tenant-Side Resources, select UUID in the search box, and then paste the server ID you just copied to find the private IP address of the host.
15. Log in to the private IP address of the host and enter the command: `ssh host private IP address` . The password is the one entered when you activated CVM.

```
WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Fri Sep 11 10:40:09 2020 from 10.10.240.32
[root@vm_17_41-centos ~]# ssh 3.12
root@3.12's password:
Last login: Fri Sep 11 10:54:47 2020 from .19.77
Welcome to tlinux 2.2 64bit
Version 2.2 20200119
[root@kvm_3_12 ~]#
```

16. Enter the `virsh console UUID --force` command. For example, enter the `virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force` command to enter CVM.

```
[root@kvm_3_12 ~]# virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force
Connected to domain 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11
Escape character is ^]

[root@VM_0_12-centos ~]#
```

17. After entering CVM, enter the following command to perform an installation:

Install: `<1>yum install -y nginx`

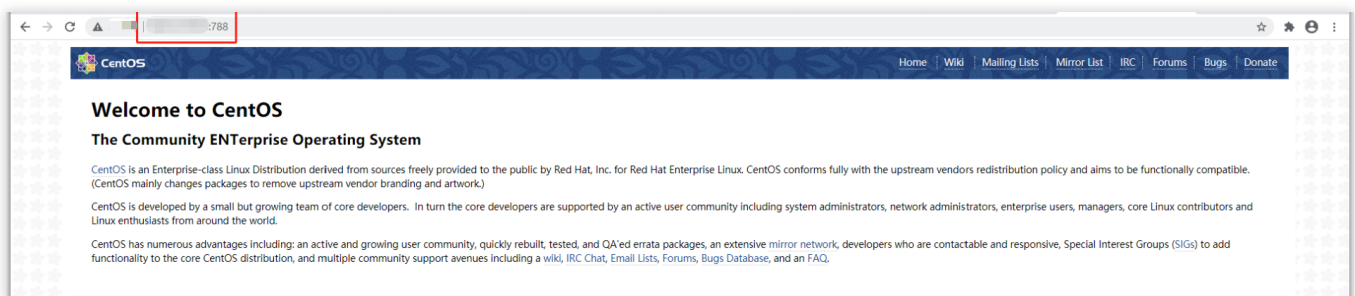
Start the Nginx service: `service nginx start` .

Check whether port 80 is enabled: `netstat -nap|grep 80` .

```
[root@VM_0_12-centos ~]# netstat -nap|grep 80
tcp        0      0 0.0.0.0:80          0.0.0.0:*          LISTEN     20928/nginx: master
tcp6       0      0 :::80             :::*               LISTEN     20928/nginx: master
udp6       0      0 fe80::5054:ff:feb::123 :::*              6695/ntpd
```

18. Since some customers prohibit external access to ports 80 and 443 on their public IP addresses, you need to forward port 80 of the CVM to another port (for example, port 788) through a NATGW, and associate this gateway in the route table (ignore steps 2.18 to 2.26 if it is not involved). Under the VPC menu, select NAT Gateway. After selecting the corresponding region, click Create to create a NAT gateway.
19. Enter information according to the actual situation and click Create to return to the NAT Gateway List page.

20. In the created NAT gateway, click the gateway ID.
21. Click Port Forwarding.
22. Click Create.
23. Add a port to be forwarded.
24. Under VPC, select Route Table. Under the corresponding region, click Create to create a route table.
25. Enter information and click Create. Select the policy as the added NAT gateway.
26. A prompt indicates that you need to associate a subnet. After selecting the associated subnet, click OK to return to the Route Table List page.
27. Visiting `http://Public IP Address:788/` to Verify Whether the Website Is Normal



28. Add a domain name in SaaS WAF. For the origin server IP address, enter the elastic IP address.



CLB WAF Connection

Comparison of Access Methods

The current CLB WAF supports five types of traffic sources: Layer-7 CLB instances (both internal and public), API Gateway, SCF, APISIX Gateway, and custom application gateways. The comparison is as follows:

Instance Type	Applicable Scenarios	Core Advantages	Access Method	Supported Regions
Cloud-Native Layer-7 CLB Instance	Suitable for users who are using or planning to use Converge Cloud public or internal Layer-7 CLB, such as high-concurrency web applications.	Supports both mirror and protection modes. No need to adjust architecture, supports one-click bypass, stable and reliable.	Connect via domain and instance object.	-
API Gateway Instance	Suitable for users of Converge Cloud API Gateways, such as microservices architecture, API open platforms, etc., needing unified management of API security.	Supports protection mode. Separation of forwarding and protection, more reliable with API Gateway controlling traffic access.	Associate WAF policies in the API Gateway configuration to achieve security protection for API traffic. It supports domain and instance object connect. Details can be found in API Gateway product documentation.	-
Cloud Function Instance	Suitable for Cloud Function (SCF) users, such as serverless web applications, event-driven business protection.	Supports protection mode. Separation of forwarding and protection, more reliable with Cloud Function controlling traffic access.	Connect via SCF trigger and WAF interaction. Flow details on the SCF side can be found in the Cloud Function product documentation.	-
APISIX Gateway Service	Suitable for APISIX Gateway users who want to combine Converge Cloud WAF for enhanced	Compatible with the open-source ecosystem. Supports SDK plugin	Connect via SDK integration, forwarding business traffic to Converge Cloud WAF cluster (custom	-



Instance Type	Applicable Scenarios	Core Advantages	Access Method	Supported Regions
	security protection.	integration, autonomous and controllable.	integration required).	
Custom Application Gateway Services	Suitable for customers in mixed-cloud WAF deployment scenarios in both cloud and on-premises environments.	Compatible with any environment. Supports SDK plugin integration, autonomous and controllable.	Connect via customer gateway integration, forwarding business traffic to Converge Cloud WAF hybrid cloud protection cluster.	Customer-defined region

Domain Connect Method Comparison

- **Layer-7 CLB Instance:**
By binding the domain and Layer-7 Load Balancer (CLB) resources (listeners) in the WAF console, HTTP/HTTPS traffic passing through the load balancer listener undergoes bypass threat detection and cleansing, achieving separation of business forwarding and security protection.
- **API Gateway and Cloud Function Instances:**
Enable WAF protection through the API Gateway console (refer to API Gateway product documentation) and the Cloud Function console. After configuring the domain in the WAF console, HTTP/HTTPS traffic passing through the API Gateway and Cloud Function Gateway undergoes bypass threat detection and cleansing, achieving separation of business forwarding and security protection.
- **APISIX Gateway Service:**
APISIX Gateway integrates SDK and forwards business traffic to the Converge Cloud WAF cluster (custom integration required).
- **Custom Application Gateway Services:**
Customer gateways integrate SDK and forward business traffic to the Converge Cloud WAF hybrid cloud protection cluster.

Precise Domain Access

Layer 7 Load Balancing CLB Integration

Step 1. Confirm CLB Configuration

This document describes how to confirm your CLB configuration prior to accessing CLB WAF.

Directions

By associating domain names with a CLB listener, CLB WAF checks and blocks HTTP or HTTPS traffic passing through the listener. Before accessing CLB WAF, make sure that your website business has been deployed on Converge Cloud and used Converge Cloud CLB (previously Application Load Balancer) over the public network.

Note:

We recommend using SaaS WAF for website business not deployed on Converge Cloud.

To ensure traffic forwarding, it is necessary to configure your CLB instance and associate your domain name with a listener. For more details, see [Configuring an HTTP Listener](#) and [Configuring an HTTPS Listener](#).

Perform the following steps to view the CLB listener configuration. `clb.technicalsupport.convergecloud` is used as an example.

1. Log in to the CLB console, and click Instance Management on the left sidebar.
2. Select a region and CLB instance. Click Configure listener on the right.
3. On the page displayed, click Listener Management to view the listener configuration details. In this example, the listener name is `waf-test`, and the domain name is `clb.technicalsupport.convergecloud` and is in "Not Enabled" status.

Subsequent Operations

After confirming your CLB configuration, you can proceed to the following steps:

- Step 2. Bind Domain Name to CLB Instance
- Step 3. Verify the Configuration



Step 2. Bind Domain Name to CLB Instance

This document describes how to bind a domain name to a CLB instance in the WAF console.

Directions

1. Log in to the WAF console and select Connection Management > Domain Onboarding on the left sidebar.
2. On the domain onboarding page, click Add domain, select CLB WAF instance, configure relevant parameters, and click OK.

Field description

- Associated instance: Select the CLB type and an instance name.
- Domain name: Enter the domain name to be protected, such as `clb.technicalsupport.convergecloud`.
- Traffic source: Select CLB.
- Use proxy: Select whether proxy services including Anti-DDoS and CDN are used based on the actual conditions.

Note:

If you select Yes, WAF will get real client IPs, which may be forged, from the XFF field as the source IPs.

- CLB listener: Select as needed.

3. Click OK to return to the domain name list, where you can view the protected domain name `clb.technicalsupport.convergecloud` and the ID, name, Action, and other information of the CLB instance.

Subsequent Operations

After the domain name is bound to a CLB instance, you can proceed to Step 3. Verify the Configuration.



Step 3: Verify the configuration

This document describes how to check whether the CLB WAF is running.

Directions

1. By binding domain names to a CLB listener, WAF can protect traffic to the domain names passing through the CLB listener. To check whether the CLB WAF is running, ensure that your local computer can access the domain names added to different CLB instances.

Note:

To check whether the access to domain names added in CLB is normal for IPv4 domain name requests, see [Getting Started with CLB](#). For IPv6 domain name requests, see [Getting Started with IPv6 CLB](#).

2. Open `http://wow.convergewaf.com/?test=alert(123)` in a browser.

Note:

`wow.convergewaf.com` is a sample domain name. Please replace it with the actual domain name that has been added.

Asset Center

Instance Management

This document guides you through the instance management module in the Web Application Firewall (WAF) asset center, where you can view instance details, purchase new instances, and renew or manage packages and scale-out packages of the instance.

Creating and Viewing Instances

1. Log in to the WAF console, select Asset Management > Instance Management in the left navigation bar.
2. On the instance management page, display all purchased instance overviews, click Create Instance, go to the purchase page, and purchase on demand. For more purchase details, please refer to Purchase Guide.
3. If the instance is associated with an Anti-DDoS EIP, the DDOS protection status will display as Anti-DDoS EIP bound under the instance type.
 - Hover the mouse here to view the Anti-DDoS EIP address. Click to view details and navigate to the EIP console.
 - After binding an Anti-DDoS EIP, the bandwidth is sustained by the EIP. Specification limits are not displayed. Business bandwidth on the VIP is counted normally in the backend, and the bandwidth range takes effect. Support disassociation on the EIP console. After disassociation, bandwidth is displayed automatically.
4. On the instance management page, click "Instance ID" and the instance detail page pops up on the right.
5. On the instance detail page (the following introduction is based on a SaaS instance as an example), you can view the basic information, plan information, extensions, add-ons, value-added capability, and attack log shipping info of the instance.



- In the Basic Info module, click  to enable/disable plan renewal and elastic protection.
- The extensions module supports redirection to purchase domain extension packages, capacity expansion packages.
- The Add-ons capability module supports enabling/disabling BOT management and API security.
- The attack log delivery shipping module supports one-click enabling/disabling of attack log shipping.

Search Existing Instance

If you purchase multiple instances and need to retrieve or search, you can use this feature. Existing instances support retrieval by region and data type, as well as keyword search.

1. Log in to the WAF console, select Asset Management > Instance Management in the left navigation bar, and go to the instance management page.
2. On the instance management page, you can filter existing instances by type and region, or search for existing instances by keyword in the search bar using "Instance ID, instance name, and billing mode".
 - Click in the upper left corner type dropdown box, filter existing instances by WAF type.
 - Click in the upper left corner of the region dropdown box to filter existing instances by region.
 - Click the search box to query existing instances by keyword such as "Instance ID, instance name, billing mode and tag".

Managing Instance Domains

You can configure domains of instance by following way.

1. On the instance management page, click Associated domains to go to the domain list page.
2. On the domain list page, you can create, edit, and delete domain names. For details, see Domain Name List.

Network Configuration

1. For instances with DDoS protection, users can configure network.
2. Click Network Configuration, a pop-up window appears where you can enable/disable native VIP instance. It is recommended to disable them.

Purchase Instance Renewal and Expansion Package

After searching for the required instance and viewing it, you can check the expiry time of your purchased product package and the remaining usage of the expansion package on the instance management page dashboard.

1. If your package is about to expire and needs renewal, click Renew. On the WAF package renewal webpage, select a renewal duration and click Renew Now to renew your current package.
2. If the dashboard displays that the domain pack or QPS specification is about to reach its limit, click More, select Extra domain package, Extra capacity package, or API Security, and you can proceed with purchasing related services.

Note: If the current instance or domain name package has expired, renew first, then repurchase.

- Purchase extra domain package: Select purchase quantity (1–500), click Buy Now to purchase the extra domain package.
- Purchase extra capacity package: Select purchase quantity (1–500), click Buy Now to purchase the



extra capacity package.

- API Security: Choose whether to activate API security and purchase extra capacity package as needed, click Buy Now to purchase related services.

Access Management

Scenarios

This document instructs you to manage your domain names in the WAF console.

Directions

Adding and viewing a domain name

1. Log in to the WAF console and select Asset Management > Access Management on the left sidebar.
2. On the page displayed, click Add domain.
3. On the pop-up page, configure the required parameters and click OK.
4. On the domain name list page, click a domain name you want to view. The basic details of the domain name will be displayed.

Toggling on protection switch



1. On the domain name list page, click the WAF switch . A window will pop up to ask you to confirm your operation.
2. In the pop-up window, click OK. After the switch is on, WAF protection will take effect based on your custom policies and defense settings.

Editing a domain name

1. On the domain name list page, select the target domain name and click Edit.
2. On the page displayed, modify the server configuration, proxy, and origin address, and click OK to save your changes.

Deleting a domain name

1. On the domain name list page, select a domain name to delete and click Delete on the right.
2. In the pop-up window, click OK to delete the domain name.



Basic Security Configurations

Match Mode Field Description

When setting allowlist rules, custom allow rules, custom access control, and CC protection rules, you need to configure the match method in the rules to define the request features to match. This article introduces the fields supported by the rule matching condition and their definitions.

Custom Rule Scenario

Module Name	Description
Set allowlist rule	Allow requests with specified characteristics to pass without testing by the rule engine.
Set custom allow rule	Allow requests with specified characteristics to pass without testing by all or specific protection modules. Note: Protection modules: Web Protection - Rules Engine, Web Protection - malicious file detection, IP blocking, Access Control - Region Blocking, Access Control - Custom Rules, CC protection, Data leakage prevention, IP Blocklist/Allowlist, Bot Protection, API security, Mini Program Traffic Risk Control, Large Model Security
Set Access Control Rule	Control access of public network users through feature matching.
Set CC protection rule	Handle statistical objects with frequency anomalies that hit the match condition.

Matching Condition

Matching condition refers to the request features that Web Application Firewall (WAF) needs to detect. When setting an allowlist rule, custom allow rule, custom access control, or CC protection rule, you define the matching condition to specify the request features to detect. If a request meets the match condition set within the rules, it hits the corresponding rule. WAF then handles the request based on the rule action set in the rules (such as observation, block, or redirect).

The matching condition consists of match field, parameters, operator, and content. On the right, you can select whether the match field is case sensitive.

Rule Engine

Note:

If your Web Rule Library supports 25 attack types, refer to this document to set protection rules.

This document introduces how to set protection rules through Web Application Firewall (WAF) to protect against web attacks.

Background

The Converge Cloud WAF rule protection engine provides expert rule sets based on Converge Cloud security Web threats and intelligence accumulation, automatically protecting against OWASP TOP10 attacks. Currently, the protection targets 25 common types of Web attacks, including SQL injection, XSS attack, command injection attack, server-side request forgery, Trojan Horse attack, etc. The newly upgraded rule engine supports more granular rule category management and finer operational capability.

Optimizations include:

- Rule engine protection latency reduced, access experience optimized;
- Rule engine categorization is more granular, leveraging refined security operation;
- Rule protection rule allowlist is more granular, supporting scheduled and periodic effect.

Operation Steps

Managing the Rules

1. Log in to the Web Application Firewall console, and at the top of the left sidebar, switch the console to the instance location.
2. Select Protection Policies > Basic Security in the left sidebar.
3. On the basic security page, select the target domain name, click Web Security, and select Regex Engine. The Web security page shows different attack type rule set conditions in an integrated way and provides a uniform configuration management feature. Details are as follows:
 - Number of enabled rules: Displays the total number of rules in the corresponding attack type rule set and the current number of enabled rules. This helps users understand the current security protection status and modify rules as needed. By default, all are enabled.
 - Action: Supports one-click selection of Observe/Block mode to improve management efficiency. Defaults to Block mode.
 - Protection level: Supports selecting different protection level rules, including loose, normal, strict, or super strict. The normal level includes loose rules, the strict level includes normal and loose rules, and the super strict level includes all rules. Defaults to strict.
 - On/Off: Supports users to configure with one click whether specific attack type rule sets take effect,



suitable for rapid security policy adjustment as needed.

4. Click in the upper right corner Batch configuration, select rule sets as needed to batch configure protection mode and protection level, then click Apply to successfully configure.
5. Click View Details to check corresponding attack type rule set info and set the status of individual rules, supporting disable, enable, or observation only.

Observation only means attack delivery to the attack log when a rule is triggered, without performing other actions. Single rule status has a higher priority than sub-type and global settings. Once set, it will be locked but can be manually unlocked. After unlocking, it synchronizes with sub-type or global setting status. All rules are enabled by default.

6. Users can enter "Rule ID, Rule description, CVE number" to search rule sets, view specific rules and perform operations. Meanwhile, click in the upper left corner Batch Switch Rule Status to alter multiple rule statuses at the same time.

Rule Allowlist

For related operations on rule allowlist, see Rule Allowlist.

Viewing Rule Categories

1. Log in to the Web Application Firewall console, and at the top of the left sidebar, switch the console to the instance location.
2. Select Service Management > System Settings > Web Rule Library in the left sidebar.

The attacks against which the WAF currently protects are classified as follows:

Attack Classification	Attack Description
XSS Attack / XSS Attack (Extended)	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.



Attack Classification	Attack Description
SQL Injection Attack / SQL Injection Attack (Extended)	A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.
Known Exploits / Known Exploits (Extended)	Known Exploits are mainly used to detect remote arbitrary code execution vulnerabilities, remote arbitrary command execution vulnerabilities, path traversal vulnerabilities, open redirect vulnerabilities, unauthorized access vulnerabilities, etc. in various applications, web servers, middleware, etc.
File Upload Attack / File Upload Attack (Extended)	The file upload attack exploits vulnerabilities in an application's inadequate validation of uploaded file types, content, or paths to upload malicious files (such as WebShells, trojans, etc.), thereby gaining control over the server.
Server-Side template injection vulnerability / Server-Side template injection vulnerability (Extended)	Prevents attackers from exploiting vulnerabilities in server access request APIs to initiate malicious requests.
Unauthorized access vulnerability / Unauthorized access vulnerability (Extended)	Some management backends and debugging pages don't verify the permissions of users sending requests. Therefore, attackers can use some system features to get sensitive information and execute code.
Trojan Horse Attack / Trojan Horse Attack (Extended)	A WebShell is a malicious script implanted on a web server to enable remote control by attackers. Attackers upload WebShell scripts (e.g., PHP, ASP files) via file upload vulnerabilities or other exploits, allowing them to execute commands, steal data, or establish persistence for further attacks.
XML Injection Attack / XML Injection Attack (Extended)	XXE (XML External Entity) attacks exploit vulnerabilities in XML parsers by crafting malicious XML documents to read local files, initiate remote requests, or cause denial of service. Attackers inject external entity definitions to access restricted resources or probe internal network information.
Non-Compliant protocol / Non-	Attackers launch attacks by crafting malformed HTTP request packets.



Attack Classification	Attack Description
Compliant protocol (Extended)	
Invalid access to core files / Invalid access to core files (Extended)	Arbitrary file read/download vulnerabilities allow attackers to bypass application restrictions by crafting specific paths or parameters to read or download arbitrary files (e.g., configuration files, database credentials). This is typically caused by insufficient validation of user-supplied file paths.
Command Injection Attack / Command Injection Attack (Extended)	The attacker crafts malicious inputs (such as system commands or code) to exploit vulnerabilities in how the target program processes user inputs. This causes the system to improperly execute the injected code or commands. Such attacks may result in data breaches, service disruptions, or even complete compromise of system control.
Server-Side request forgery	Prevents attackers from exploiting vulnerabilities in server access request APIs to initiate malicious requests.
Bad Robot	Bad Robot detection is mainly used to detect malicious tools such as web scanners and script batch acquisition tools.
LDAP Injection Attack	LDAP Injection attacks involve inserting malicious LDAP query statements into input data from the client to manipulate predefined LDAP query logic. Successful LDAP injection can lead to unauthorized access to sensitive information in directory services (e.g., user credentials, permissions) or even modification/deletion of directory data.

Note:

The expansion rule set for each attack type has a wider detection range, broader detection content, and stronger detection ability compared with the standard rule set, but it requires tolerating certain rule false positives.

IP Blocking

This document describes Web Application Firewall (WAF) attacker IP penalty, which can quickly block malicious attacker IPs and defeat attacks and threats from malicious scanners, proxies, and webs to improve defense efficiency.

Overview

Attacker IP penalty can automatically block repeated web attacks the client IP suffered in a short period of time. You can view attack logs for attack details.

Prerequisites

- You have purchased a WAF plan.
- You have added a protected domain name, and ensured the domain name is in normal protection. For detailed directions, see [Getting Started](#).
- Currently, IPs can be blocked by domain name. Domain names can have different blocking durations, which are calculated separately.

Directions

1. Log in to the WAF console and select Configuration Center > Basic Security > Web Security on the left sidebar.

2. On the web security page, select the target domain name in the top-left corner and click  next to IP blocking to enable IP blocking.

3. On the web security page, click  next to IP blocking to modify default parameters and click OK.

Field description:

- **Web attacks:** It records the number of web attacks from a malicious IP in a specified period. The attacks will trigger the rule engines against web attacks excluding AI engine, custom policies, and CC protection.
- **Detection duration:** It specifies the duration to detect the attacker IP.
- **Blocking duration:** It specifies the duration to block the attacker IP.

Access Control

Overview

Access control rules allow you to control access from public network users by matching HTTP message sections such as request path, GET parameters, POST parameters, Referer, and User-Agent. This feature enables Converge Cloud users to respond flexibly with a combination of rules to easily address various cyber attacks.

Note:

- Each rule can contain up to 5 conditions.
- Conditions in each rule are evaluated using a logical AND, that is, the rule does not take effect unless all the conditions are matched.
- Each rule supports five actions: Block, CAPTCHA, Observe, and Redirect.
 - Block: Enables WAF to block access requests that hit the specified rule.
 - CAPTCHA: Enables WAF to verify access requests that hit the specified rule.
 - Observe: Enables WAF to observe access requests that hit the specified rule.
 - Redirect: Enables WAF to redirect access requests that hit the specified rule.
 - JS validation: Enables WAF to validate JavaScript in access requests that hit the specified rule.
- Priority: The value range is 1-100. A smaller number represents higher priority.

Example

Example 1: Banning specific IP addresses from access to a designated site

To ban specific IP addresses from access to a designated site, the webmaster can perform configuration with the following steps:

1. Log in to the WAF console and click Protection Policies > Basic Security on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click Access control.
3. On the access control page, click Add rule, and the rule adding window will pop up.
4. Enter the name of the rule (e.g. "001"), select an option (such as "source IP") for Field, select "Belong to" for Operator, and enter the source IP (e.g. 192.168.1.1) banned from access for Content. Then select an action (e.g. "Block"), and click OK to save the rule.

Note:

WAF access control rules allow you to use masks to control access requests from source IPs within a

range. We can enter a specific IP address range (e.g. 10.10.10.10/24) in Content.

5. Now, the rule will take effect immediately, and block all HTTP access requests from specific source IPs.

Example 2: Banning public network users from access to specified Web resources

If the webmaster does not want a public network user to access specified web resources, such as administration backend /admin.html , he or she can configure as follows: select "Request Path" for Field, select "Include" for Operator, enter /admin.html in Content, select "Block" for Action, and click OK.

Example 3: Banning an external site from hot-linking certain resources

To block hotlink attacks by external sites, such as www.test.com , the webmaster can use access control rules to capture and block the Referer in a hotlink request. The configuration is as follows: select "Referer" for Field, select "Include" for Operator, enter www.test.com in Content, select "Block" for Action, and click OK.

Example 4: Copying rules to target domain names

You can copy the rule you configured to other domain names by using the copy operation.

1. Log in to the WAF console and click Protection Policies > Basic Security on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click Access control.
3. On the access control page, select the required policy, click Copy, and the custom policy copy window will pop up.
4. In the pop-up window, select a domain name and click OK to copy the rules to the target domain name.

CC Protection Rule Settings

CC protection can safeguard the access to websites. CC protection settings 2.0 are upgraded with emergency CC protection and custom CC rules. Emergency CC protection can perform big data analysis on websites' access history and their real servers' exceptional responses such as timeout and response delay, to generate protection policies for emergencies, blocking frequent access requests in real time. Custom CC rules support customizing protection based on user source IPs or session frequency, with actions including blocking, precise blocking, JS validation, observing, CAPTCHA, or precise CAPTCHA.

Note:

- Emergency CC protection and custom CC rules cannot be enabled at the same time.
- SESSION must be set before using the session-based CC protection policy.
- Slow Attack Protection: When forwarding traffic, web application firewalls aggregate and clean slow requests, providing a certain level of slow attack protection capabilities.

Slow Attack Protection

Slowloris, RUDY, and other slow attacks are techniques that slow down server response times, typically by sending a large number of slow or incomplete requests to consume server resources, preventing normal users from accessing web applications.

- When forwarding traffic, web application firewalls aggregate and clean slow requests by default, providing slow attack protection capabilities and the ability to clean slow attacks similar to Slowloris.
- When a web application firewall cleans slow requests, HTTP protocol type requests will return a status code of 400, while TCP protocol type requests will return a TCP RST.

Directions

Log in to the Web Application Firewall console, and at the top of the left sidebar, switch the console to the instance location.

Example 1: Emergency CC protection settings

Emergency CC protection is disabled by default. Before enabling it, please make sure that the custom CC rule feature is disabled.

1. Log in to the WAF console and select Protection Policies > Basic Security on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click CC Protection.



3. Click  in the emergency CC protection module and confirm the operation to configure emergency CC protection.

Configuration item description:

Status switch: After emergency CC protection is enabled, if a website is under massive CC attacks (with a website QPS of 1000 or above), the protection will be automatically triggered. If there are no specific protection paths, we recommend enabling emergency CC protection. As there may be some false alarms, you can click IP Query on the left sidebar to view the information of blocked IPs and handle them in time.

Note:

If there are specific protection paths, we recommend using custom CC rules.

Example 2: Access source IP-based CC protection settings

An IP-based CC protection policy can be directly configured without setting SESSION.

1. Log in to the WAF console and select Protection Policies > Basic Security on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click CC Protection.
3. On the CC protection page, click Add rule, and the rule adding window will pop up.
4. In the pop-up window, configure relevant parameters and click OK.

Field description:

- Rule name: Name of the CC protection rule. It can contain up to 50 characters.
- Recognition mode: Supports two modes: IP recognition (default) and SESSION recognition. To use SESSION recognition, set the SESSION position first.
- Condition: Specifies the match parameter, logical operator, and match content to control access frequency. The match parameter defaults to URL. For the same rule, you can set up to 10 conditions with the logical AND operator. Refer to *Match Mode Field Description* for more details.
- Frequency limiting method: You can choose between Penalty QPS and Traffic throttling and frequency limiting.
 - Penalty QPS: Applies a custom-duration action to clients that trigger the frequency rule, and the action is executed for requests initiated within the set time period.
 - Traffic throttling and frequency limiting: Strictly controls the number of requests from clients that trigger the frequency rule and limits the maximum number of requests per unit of time. Available only for instances that have purchased BOT Protection or API Security.

- Access frequency: Set based on actual business requirements. Recommended value: 3–10× normal access frequency.
 - Example: If your website is accessed 20 times per minute per visitor, set 60–200 times per minute.
- Action: Defaults to "Block". You can change this field as needed.

Action Type	Description
Observe	Requests that meet the matching conditions will be monitored and logged.
Block	Requests that meet the rate-limiting conditions will trigger the block action, preventing the IP or Session from accessing all pages of the website.
Precise block	Requests that meet the rate-limiting conditions will trigger the precision block action. Unlike regular blocking, precision block only intercepts requests within the effective scope.
CAPTCHA	Browser-based access only. Requests that meet the matching conditions will be challenged with a CAPTCHA. Failure triggers block; success allows access.
Precise CAPTCHA	Executes CAPTCHA challenge for IP/Session access. Failure triggers block; success allows access.
JS validation	Executes JavaScript validation and logs the result.

- Penalty duration: 1 minute–1 week. Default: 10 minutes.
- Priority: Integer 1–100 (default: 50). Smaller value = higher priority.

5. You can select a created rule to disable, edit, or delete it.

6. Requests that match the rules will execute the corresponding protection actions as configured.

Example 3: CC Protection Settings Based on SESSION

CC protection based on SESSION access rate can effectively solve misinterceptions caused by users sharing IP exits in office networks, supermarkets, or public Wi-Fi scenarios.

1. Log in to the WAF console, select Configuration Center > Basic Security in the left sidebar, and enter the basic security page.
2. On the basic security page, select the domain requiring protection in the upper left corner, click CC Protection, and enter the CC protection page.
3. Click New in the SESSION settings, and a pop-up for adding a new SESSION will appear.
4. In the SESSION Popup Settings, select COOKIE as the test content, identified as security , with a start position of 0 and an end position of 9. Click Next after completing the configuration.

Field Descriptions:

- Session name: Custom SESSION name, up to 32 characters.
- Session position: COOKIE, GET, HEADER, or POST. GET/POST refer to HTTP request content parameters.
- Match mode: String pattern matching or position match.
- Session ID: Value identifier.
- Start position: Starting position of the match.
- End position: Ending position of the match.

5. Enter the SESSION test page, set content as `security = 0123456789...`. WAF uses the 10-digit string following "security" as the SESSION identifier. SESSION information can be deleted and reconfigured.
6. Set a CC protection policy based on SESSION. The configuration process is consistent with Example 1. Select SESSION as the identification method and choose the application target as needed.
7. Configuration complete. The CC protection policy based on SESSION takes effect.

Note:

Using SESSION-based CC protection mechanism: blocking information cannot be viewed in IP blocking status.

API Security Management

API Traffic Analysis

The API traffic analysis feature supports the summary and analysis of several dimensions of APIs including the asset status, activity, sensitivity, and risk events, providing an intuitive understanding of trends across various dimensions of the current APIs.

Directions

1. Log in to the Web Application Firewall Console, and choose API traffic analysis in the left sidebar.
2. On the API traffic analysis page, click the All domains dropdown in the top left corner, and select the domain name you want to view. Whether API security is enabled for the current domain name is displayed on the right side.
 - If the API security switch is enabled, you can start using the related features.
 - If the API security switch is not enabled, go to the Access Management page, filter the domain



name under the instances that have purchased API security, and click to enable the switch.

3. On the API traffic analysis page, API assets and API security risks are displayed at the top.

Field Name	Description
Total APIs	The total number of API assets under the current domain name.
Discovered APIs	The total number of API assets under the current domain name with the status <i>Newly Discovered</i> .
Active APIs in the past 7 days	The total number of API assets accessed in the past 7 days under the current domain name.
7-day inactive APIs	The total number of API assets not accessed in the past 7 days under the current domain name.
Unsafe APIs	The total number of API assets under the current domain name with risk levels classified as low-risk, medium-risk, or high-risk.
Sensitive APIs	The total number of API assets under the current domain name involved in the transmission of sensitive data.
Security events	The total number of API risk events under the current domain name.

4. On the API traffic analysis page, retrieve API-related statistics within a specified time range.

5. In the API Activity Analysis category, there are two modules: Top 5 active APIs and Active/Inactive API trends.
 - Top 5 active APIs: View the Top 5 active API assets in the selected domain name's API traffic within the selected time range.
 - API Asset Management: Click to navigate to the API asset management page.
 - See more: View the Top 10/50/100 active API assets in the selected domain name's API traffic within the selected time range.
 - Active/Inactive API trends: View the trends of active/inactive API assets in the selected domain name's API traffic within the selected time range.
6. In the Sensitive Analysis Classification category, there are three modules: Sensitive APIs by sensitivity, Top 5 sensitive APIs, and Types of sensitive data.
 - Sensitive APIs by sensitivity: View the number of API assets with different risk levels in the selected domain name's API traffic within the selected time range.
 - Top 5 sensitive APIs: View the Top 5 ranked API assets by the number of sensitive data entries in the selected domain name's API traffic within the selected time range.
 - Types of sensitive data: View the proportion of sensitive data types in the selected domain name's API traffic within the selected time range.
 - View all sensitive APIs: Click to navigate to the API asset management page and filter the list of all sensitive API assets within the selected time range.
7. In the API Event Analysis category, there are three modules: Discovered API security events by severity, Top 5 API security events, and Event types proportion.
 - Discovered API security events by severity: View the risk level classification of discovered events in the selected domain name's API traffic within the selected time range.
 - Top 5 API security events: View the ranking of the number of API-related events in the selected domain name's API traffic within the selected time range.
 - Event types: View the proportion of event types in the selected domain name's API traffic within the selected time range.
 - View all events: Click to go to the event management page and filter the list of all event types within the selected time range.
8. In the API Event Trend Analysis category, view the total number of events and the number of processed events in the selected domain name's API traffic within the selected time range.

View all events: Click to go to the event management page and filter the list of all event types within the selected time range.

Blocklist/Allowlist Protection Settings Features

The blocklist/allowlist feature of WAF allows you to add access source IPs that pass WAF-protected domains to the blocklist or allowlist and add multiple HTTP sections to the precise allowlist. Key features include IP blocklist/allowlist settings and precise allowlist settings.

- IP blocklist/allowlist setting: You can set domain name-specific, IP range-specific, or global IP blocklist/allowlist rules.
- Precise allowlist setting: You can add the access requests from specified public network users to the allowlist by combining and matching HTTP message sections such as request path, GET parameters, POST parameters, Referer , and User-Agent .

Meanwhile, you can add a domain name-specific or global blocklist/allowlist which will take effect in the following priority order:

- The priority of the blocklist/allowlist is only lower than that of the custom precise allowlist, but higher than that of other detection logic.
- The priority of blocklist/allowlist settings is in descending order: precise allowlist > global allowlist > domain name-specific allowlist > domain name-specific blocklist > global blocklist > other WAF module logic.

IP Blocklist

Adding IPs to Blocklist

Adding IPs manually

1. Log in to the WAF console and select Configuration Center > Blocklist/Allowlist on the left sidebar.
2. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP blocklist.
3. On the IP blocklist page, click Add address.
4. On the page that appears, configure relevant parameters and click OK.

Field description:

- IP address: IP address such as 10.0.0.10 or FF05::B5 . CIDR blocks are supported, such as 10.0.0.0/16 or FF05:B5::/60 . You can enter up to 20 items and separate them with line breaks.

Note:

If you select All for the domain name, the added IP address or range will be blocked/allowed globally.

The domain name quotas in each edition are as follows: Premium Edition: 1,000 entries/domain name; Enterprise Edition: 5,000 entries/domain name; Ultimate Edition: 20,000 entries/domain. Each IP address or range occupies one entry in the quota.

- Expiration time: Never expire or a specified date.
- Remarks: Custom remarks, which can contain up to 50 characters.

Importing IPs

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP blocklist.
2. On the IP blocklist page, click Import data > Import. After the data is parsed successfully, click OK.

Editing IP Blocklist

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP blocklist.
2. On the IP blocklist page, select a target IP address, click Edit in the Operation column, modify the expiration time and remarks, and click OK.

Deleting IPs from IP Blocklist

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP

blocklist.

2. You can delete one, multiple, or all IP addresses on the IP blocklist page as follows:

- One: Select an IP address and click Delete address or Delete in the Operation column. A window will pop up to ask you to confirm the deletion operation.

Note:

Once deleted, it cannot be restored and can take effect only after being added again.

- Multiple: Select multiple IP addresses and click Delete address. A window will pop up to ask you to confirm the deletion operation.

Note:

Once deleted, it cannot be restored and can take effect only after being added again.

- All: Click Delete all. A window will pop up to ask you to confirm the deletion operation.

Note:

This operation will clear all IP blocklist/allowlist information under the current domain name. Therefore, proceed with caution. Once deleted, the addresses cannot be restored and can take effect only after being added again.

3. In the pop-up window, click OK.

Exporting All Filtered Results

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP blocklist.
2. On the IP blocklist page, click the search box to filter IPs by IP address or click Source to filter IPs by source type.
3. After filtering required IPs, click Export all.

IP Allowlist

Adding IPs to Allowlist

Adding IPs manually

1. Log in to the WAF console and select Configuration Center > Blocklist/Allowlist on the left sidebar.
2. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP allowlist.
3. On the IP allowlist page, click Add address.
4. On the allowlist IP adding page, configure relevant parameters and click OK.

Field description:

- IP address: IP address such as 10.0.0.10 or FF05::B5 . CIDR blocks are supported, such as 10.0.0.0/16 or FF05:B5::/60 . You can enter up to 20 items and separate them with line breaks.

Note:

If you select All for the domain name, the added IP address or range will be blocked/allowed globally.

The domain name quotas in each edition are as follows: Premium Edition: 1,000 entries/domain name; Enterprise Edition: 5,000 entries/domain name; Ultimate Edition: 20,000 entries/domain. Each IP address or range occupies one entry in the quota.

- Expiration time: Never expire or a specified date.
- Remarks: Custom remarks, which can contain up to 50 characters.

Importing IPs

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP allowlist.
2. On the IP allowlist page, click Import data > Import. After the data is parsed successfully, click OK.

Editing IP Allowlist

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP allowlist.
2. On the IP allowlist page, select a target IP address, click Edit in the Operation column, modify the expiration time and remarks, and click OK.

Deleting IPs from IP Allowlist

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP

allowlist.

2. You can delete one, multiple, or all IP addresses on the IP allowlist page as follows:

- One: Select an IP address and click Delete address or Delete in the Operation column. A window will pop up to ask you to confirm the deletion operation.

Note:

Once deleted, it cannot be restored and can take effect only after being added again.

- Multiple: Select multiple IP addresses and click Delete address. A window will pop up to ask you to confirm the deletion operation.

Note:

Once deleted, it cannot be restored and can take effect only after being added again.

- All: Click Delete all. A window will pop up to ask you to confirm the deletion operation.

Note:

This operation will clear all IP blocklist/allowlist information under the current domain name. Therefore, proceed with caution. Once deleted, the addresses cannot be restored and can take effect only after being added again.

3. In the pop-up window, click OK.

Exporting All Filtered Results

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click IP allowlist.
2. On the IP allowlist page, click the search box to filter IPs by IP address or click Source to filter IPs by source type.
3. After filtering required IPs, click Export all.

Precise Allowlist Management

You can add IPs to the precise allowlist to allow access requests of specific public network users to the specified sites.

Adding to Precise Allowlist

1. Log in to the WAF console and select Configuration Center > IP Blocklist/Allowlist on the left sidebar to enter the IP blocklist/allowlist page.
2. On the blocklist/allowlist page, select the target domain name in the top-left corner and click Precise allowlist.
3. On the precise allowlist page, click Add address, and the IP adding window will pop up.
4. In the pop-up window, configure relevant parameters and click OK.

Note:

WAF precise allowlist enables you to use masks to allow access requests from source IPs within a range. We can enter a specific IP range (e.g. 10.10.10.0/24) in Content.

5. Now the rule will take effect immediately, and allow all HTTP access requests from specific source IPs.

Editing Precise Allowlist

1. On the blocklist/allowlist page, select the target domain name in the top-left corner and click Precise allowlist.
2. On the precise allowlist page, select the target rule, click Edit, and the editing window will pop up.
3. In the pop-up window, modify relevant parameters and click OK.

Removing from Precise Allowlist

1. On the blocklist/allowlist page, select the target domain name in the top-left corner and click Precise allowlist.
2. On the precise allowlist page, select the target rule, click Delete, and the deletion confirmation window will pop up.
3. In the pop-up window, click OK.

Note:

Once deleted, it cannot be restored and takes effect only after being added again.

Rule Allowlist

If normal access traffic is blocked by the WAF rule engine, you can create rules to allow the access traffic using the blocklist/allowlist feature.

Directions

1. Log in to the WAF console and select Configuration Center > IP Blocklist/Allowlist on the left sidebar to enter the IP blocklist/allowlist page.
2. On the blocklist/allowlist page, select the target domain name in the top-left corner and click Rule allowlist.
3. On the page that appears, click Add rule.
4. In the pop-up window, configure the required parameters and click OK.

Field description:

- Rule ID: ID of the rule to be allowed. You can add up to 10 rule IDs for each policy.
- Match method: Match method of the URL to be allowed. You can select "Exact match" (default value), "Prefix match", or "Suffix match".
- URL: URI path to be allowed. The URI must be unique under one domain name.
- Enable allowlist: It specifies whether to enable allowlist. The switch is enabled by default.



Statistics and Logs

Attack Logs

Converge Cloud WAF collects attack logs that record details such as attack time, attacker IP, and attack type. You can query and download logs for up to 30 days in the past using full-text search, fuzzy search, or filter-based search (supporting downloads of up to 1 million logs).

Searching Attack Logs

1. Log in to the Converge Cloud WAF Console. Select Attack Logs on the left sidebar, then go to the Log Service tab.
2. Choose the instance, domain name, attack type, action, and attack time to search attack logs.

Field Name Descriptions

Field Name	Description
Instance	Select instances. By default, all instances are selected.
Domain name	Select domain names. By default, all domain names are selected.
Attack type	Select attack types observed or blocked by security modules. By default, all attack types are selected.
Action	Select Observe or Block. By default, all actions are selected.
Risk level	Select High, Medium, or Low risk. By default, all levels are selected.
Time period	Specify a time range for the logs. Default: Last 1 hour.
Auto-refresh	Automatically refreshes logs at the specified interval (disabled by default).

3. Specify your search filters before clicking Search.

Analyzing Attack Logs



1. On the top right of the log list, click  to select displayed fields, then click OK. (For detailed information on each field, see Log Field Description below.)
2. On the left of the Raw Data section, select a field to view its percentage breakdown. Then, select a value to filter results.



3. Click  to expand log details. You can also:
- Click any field value to filter results based on that value.
 - Click JSON to view the log in JSON format.

Downloading Attack Logs



1. On the top right of the log list, click  to view your Download Tasks.

Note:

By default, your current search results will be downloaded.
Only one download task can be created at a time.
Each download task can include up to 1 million logs.
For more, create multiple tasks sequentially or contact Converge Cloud Support.
If you select a wildcard domain (e.g., *.example.com), logs from all subdomains (e.g., api.example.com , shop.example.com) will be included.

2. On the Download Task page, click Create Task.
3. Enter a task name and click Create.
4. After the task is created, you can view the total number of logs, download progress, download status, creation time, and expiration time. Click Download to export the logs in CSV format.

Note:

Downloaded logs are retained for 3 days.

See Also

Log Field Description

Basic Information

Field Name	Description
host	The domain name accessed by the client.
uri	The request URI identifying the resource.
attack_ip	The source IP of the attack.
attack_type	The type of attack detected.



Field Name	Description
rule_id	ID of the protection rule applied (AI rule ID = 0).
method	The HTTP request method used.
user_agent	Information about the attacker's browser and operating system.
risk_level	Indicates the risk level of the attack.
status	The action taken: 0 (Observe), 1 (Block).
count	Number of attacks from the same IP within 10 seconds.
domain	The domain name attacked.
pan / domain_name	The accessed domain name.
attack_time	The timestamp when the attack occurred.
attack_place	The location within the HTTP request where the attack was detected.
action	The action taken on the attack request (0: Observe, 1: Block).
ipinfo_nation	Country of the attacker IP.
ipinfo_province	Province or state of the attacker IP.
ipinfo_city	City of the attacker IP.
ipinfo_state	Country or region of the attacker IP.
ipinfo_dimensionality	Latitude of the attacker IP.
instance	Name of the Converge Cloud WAF instance.
attack_category	Attack category (currently unavailable).
edition	WAF versions: sparta-waf , clb-waf .
uuid	Unique identifier of the log.
attack_content	The specific content that was attacked.
http_log	HTTP request and response logs.
headers	Request and response headers (including custom ones).
rule_name	Rule name (currently unavailable).



Field Name	Description
count	Number of attacks of the same type from the same attacker IP within 10 seconds.
args_name	Parameters in the HTTP request.
ipinfo_isp	ISP of the attacker IP.
appid	App ID of the Converge Cloud account.
ipinfo_longitude	Longitude of the attacker IP.

Access Logs

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 up to 180 days. After enabling this feature, you can query and download access logs as needed to meet your security compliance and OPS requirements.

Note:

- To use access logging, you need to purchase an extra log services pack and enable access logging as instructed in Directions. Only after this feature is enabled for a domain name can its access requests be logged by WAF.
- To disable access logging: You can delete the corresponding billable item in Renewal Management. Note that access logging will be stopped within 2 hours and the history will be cleared within 24 hours once the billable item is removed.
- To expand logging capacity: When the required log storage exceeds the purchased log pack's capacity, new access logs will not be stored, and the historical access logs will be deleted when the retention period reaches. To avoid loss of access logs from insufficient capacity, we recommend checking your log usage and expanding the capacity in advance.

Directions

Enabling access logging

Log in to the WAF console and select Domain Name List on the left sidebar. Then toggle on the access logging switch for the domain name you choose.

Viewing logs

1. Log in to the WAF console and select Access Logs on the left sidebar. Then open the Log service tab.
2. Click the drop-down list in the top left corner of the page to select domain names, and click OK.
3. The usage capacity is displayed in the top right corner. For more details about WAF billing, click [Learn more](#).
4. To view usage capacity and set the retention period at the same time, click Storage configuration, and then click Save to save your setting.

Note:

The retention period ranges from 1 to 30 days.

Querying logs

1. Log in to the WAF console and select Access Logs on the left sidebar. Then open the Log service tab.
2. Search logs by using quick search, filters, or statements.
 - Quick search: It allows you to search logs quickly by specifying a period.
 - Search by filter: Select fields and operators, enter the field values, and click OK. You can select multiple fields.
 - Search by statement: It supports professional searches by statement and enables you to run more



complex log queries. Enter the required information, and then click .

Search statement

Reserved Character	Description
AND	"AND" logical operator, such as level:ERROR AND pid:1234
OR	"OR" logical operator, such as level:ERROR OR level:WARNING
NOT	"NOT" logical operator, such as level:ERROR NOT pid:1234
TO	"TO" logical operator, such as request_time:[0.1 TO 1.0]
" "	Double quotation mark, which quotes a phrase, such as name:"john Smith"
:	Colon, which is used for key-value search, such as level:ERROR
*	Wildcard, which is used to replace zero, one, or more characters, such as host:www.test*.com
?	Wildcard, which is used to replace one character, such as host:www.te?t.com
()	Parentheses, which is used to group clauses to form sub queries and control logic operations, such as (ERROR OR WARNING) AND pid:1234
>	Range operator, which indicates the left operand is greater than the right operand, such as status:>400
>=	Range operator, which indicates the left operand is greater than or equal to the right operand, such as status:>=400
<	Range operator, which indicates the left operand is less than the right operand, such as status:<400
<=	Range operator, which indicates the left operand is less than or equal to the right operand, such as status:<=400

Reserved Character	Description
[]	Range operator, which includes the upper and lower boundary values, such as <code>age:[20 TO 30]</code>
{}	Range operator, which excludes the upper and lower boundary values, such as <code>age:{20 TO 30}</code>
\	Escape character. An escaped character represents the literal meaning of the character, such as <code>url:\images\favicon.ico</code> . You can also use <code>"</code> to wrap special characters as a whole, e.g., <code>url:"/images/favicon.ico"</code> .
+	Logical operator (similar to AND). The term <code>+A</code> indicates A must exist, such as <code>+level:ERROR +pid:1234</code> .
-	Logical operator (similar to NOT). The term <code>-A</code> indicates A does not exist, such as <code>+level:ERROR -pid:1234</code> .
&&	Logical operator (similar to AND), such as <code>level:ERROR && pid:1234</code>
!	Logical operator (similar to NOT), such as <code>level:ERROR !pid:1234</code>
/	Regular expression identifier in the format of <code>/regExp/</code> , e.g., <code>/[mb]oat/</code> returns results containing moat or boat.
<i>exists</i>	<code>_exists_:key</code> returns results where the key value is not empty, e.g., <code>_exists_:userAgent</code> returns results where the userAgent value is not empty.
~	Fuzzy search, e.g., <code>level:erro~</code> returns results where level contains error.

Note:

- The operators are case-sensitive.
- When multiple search statements are connected with spaces, they are regarded as in the OR logic.
- The following special characters must be escaped: ``+`, `~`, `&&`, `|`, `!`, `()`, `{}`, `[]`, `^`, `\"`, `~`, `*`, `?`, `:`, `\"``
- Use `()`` to group search conditions and clarify precedence.

Displaying logs

1. Log in to the WAF console and select Access Logs on the left sidebar. Then open the Log service tab.
2. Click the field name to display the top five logs that match the field.



3. Click beside the date to view field details. To view in JSON format, click JSON.



JSON field description

Field	Description
domain	Wildcard domain name
request_time	Time that the client takes to send a request to WAF and receive a response
uuid	Unique identifier of an HTTP request
schema	Request protocol: HTTP or HTTPS
method	Client request method
url	Request URI, which resides between "/" and "?" in the client's request path
host	Client domain name
http_user_agent	Request UA
headers	HTTP request header
upstream_status	Response code returned to WAF from the origin server
status	Response code returned to the client from WAF
body_bytes_sent	Response body size
upstream_response_time	Time that WAF takes to receive the client request from the real server
ip_info.country	Country/Region
ip_info.city	City
ip_info.province	Province
ip_info.operator	ISP
ip_info.ip_type	IP type
ip_info.idc	IDC data center
ip_info.longitude	Longitude
ip_info.dimensionality	Latitude

4. Display the filtered log content in the list mode or field mode.

- Field mode: This is the default display mode. You can change to the other mode by clicking the icon in the top right corner.



- List mode: Click to change to list view.

Field description

Field	Description
msec	Timestamp of when the request is sent
schema	Request protocol: HTTP or HTTPS
method	Client request method
host	Client domain name
url	Request URI between "/" and "?" in the client's request path
query	HTTP Query String (max 1 KB)
body	Request body data
http_referer	Page source
http_user_agent	Request UA
http_x_forwarded_for	All the proxies that pass the request
cookie	Request cookie (max 1 KB)
upstream_status	Response code returned to WAF from the origin server
upstream_response_time	Time WAF takes to receive the client request from the origin server
upstream_addr	Upstream server IP
status	Response code returned to the client from WAF
upstream_response_length	Response length returned from the upstream server
edition	WAF versions: sparta-waf , clb-waf , cdn-waf

Downloading access logs

1. Log in to the WAF console and select Access Logs on the left sidebar. Then open the Log service tab.



2. Click to enter the download page, then click OK to create a download task.

**Note:**

- You cannot create more than one download task simultaneously.
- Up to 1 million logs can be downloaded at a time. To download more logs, it is recommended that you create multiple tasks to download them in batches.
- If you select a wildcard domain name (for example, *.abc.com), logs of all associated subdomain names such as those suffixed with .abc.com will also be downloaded.
- Up to five download tasks can be created.

3. On the download page, click View Task to view download details such as task number, creation time, and total number of logs.

Log field description

Field	Description
domain	Wildcard domain name
bytes_sent	Response size including headers (in bytes)
method	Client request method
request_time	Time that the client takes to send a request to WAF and receive a response
http_connection	HTTP request header Connection
upstream_connect_time	Time that WAF takes to send the client request to the real server
uuid	Unique identifier of an HTTP request
upstream_addr	Upstream server IP
host	Client domain name
upstream_response_length	Response length returned from the upstream server
schema	Request protocol: HTTP or HTTPS
http_user_agent	Request UA
headers	HTTP request header
url	Request URI between "/" and "?" in the client's request path
http_x_forwarded_for	All proxies that pass the request
http_referer	Page source



Field	Description
body	Request body data
remote_addr	Requester IP
cookie	Request cookie (max 1 KB)
bot_client_ip	Client IP (typically same as remote_addr)
request_length	Request length
http_accept	HTTP request header Accept
status	Status code returned to the client from WAF
protocol	HTTP protocol, such as 1.1, 1.0, or 2.0
msec	Timestamp of when the request is sent
pipe	Nginx built-in variable
content_type	HTTP request header Content-Type
time_local	Nginx readable local time string
upstream_response_time	Time that WAF takes to receive the client request from the real server
server_addr	WAF private IP
edition	WAF versions: sparta-waf , clb-waf , cdn-waf
upstream_status	Status code returned to WAF from the real server
body_bytes_sent	Response body size
query	HTTP Query String (max 1 KB)

Log Shipping

Log Shipping

Log shipping allows you to send logs to CLS, helping you gain more out of logs and meet user needs for operation and maintenance. To ship custom fields for your access logs, submit a ticket.

Note:

- For any exception with log shipping, contact us.
- To ship attack logs/access logs, activate the paid feature you need.
- After the shipping destination is configured, enable log shipping as instructed.
- Log shipping can be used with log service. Enable these features as needed.

Shipping Logs to CLS

To ship logs to CLS, you need to activate CLS and grant WAF required permissions.

Note:

If CLS is already activated, skip to Step 3.

1. Log in to the WAF console. Select Access Logs/Attack Logs on the left sidebar and the Log shipping tab.
2. If you have not activated CLS, click Activate now. For details, see Cloud Log Service.
3. Authorize WAF to ship data to CLS.
 - 3.1 In the Shipping to CLS section, click Configure.
 - 3.2 In the pop-up window, click Authorize now.
 - 3.3 On the CAM authorization page, click Authorize to allow WAF to ship logs to CLS. If you encounter problems during the process, see Cloud Access Management.
 - 3.4 Return to the log shipping page and click Configure now. Select the shipping region and log topic and then click OK. Alternatively, click Create to automatically create a WAF logset waf_post_logset. See the CLS console for details.
 - 3.5 After logs are sent to CLS, you can enable log shipping for the desired domain names. For details, see Enabling Log Shipping.

Note:

For any exception with authorization, submit a ticket.

Enabling Log Shipping

After shipping logs to CLS, you need to enable log delivery for the specified domain name/instance.

Note:

- Shipping attack logs is enabled at the instance level. This feature is only available for instances of Enterprise and above editions.
- Shipping access logs is enabled at the domain level. This feature is available for all instances, regardless of the edition.

Enabling attack log shipping

1. Log in to the WAF console and select Instance Management on the left sidebar.
2. On the instance management page, click Instance name to bring up the sidebar.



3. In the instance details, click to enable attack log shipping for the current instance.

Enabling access log shipping

1. Log in to the WAF console and navigate to Connection Management > Domain names.
2. On the page displayed, select a target domain name and click More > Log shipping.
3. In the advanced settings window, select logs to ship and click Save.

IP Query

This document describes how to view the IP information and blocking status using the IP query feature.

IP Query

1. Log in to the WAF console and click IP Query on the left sidebar.
2. On the page that appears, click a target domain name and enter an IP to search. Then click Search.
3. In the query results, you can view the specific IP details, and click Add to blocklist/allowlist to manually add the IP to the blocklist/allowlist.

IP Blocking Status

1. Log in to the WAF console and select IP Query on the left sidebar. Open the IP blocking status tab.
2. On the IP blocking status page, specify the IP type, triggering policy, IP address, creation time or expiration time, and click Search.
3. Click Export all. In the pop-up window, click Export record to export the query results.

Note:

- A large export may take longer time to process.
- Up to 10,000 entries can be exported.

4. In the list of query results, select an IP that you want to add to the blocklist/allowlist, and click Add to blocklist or Add to allowlist.

Rule Engine

This document describes how to perform rule protection settings through WAF to protect against web attacks.

Background Information

WAF uses a rule protection engine based on regular expressions and an AI protection engine based on machine learning to protect against web vulnerabilities and unknown threats.

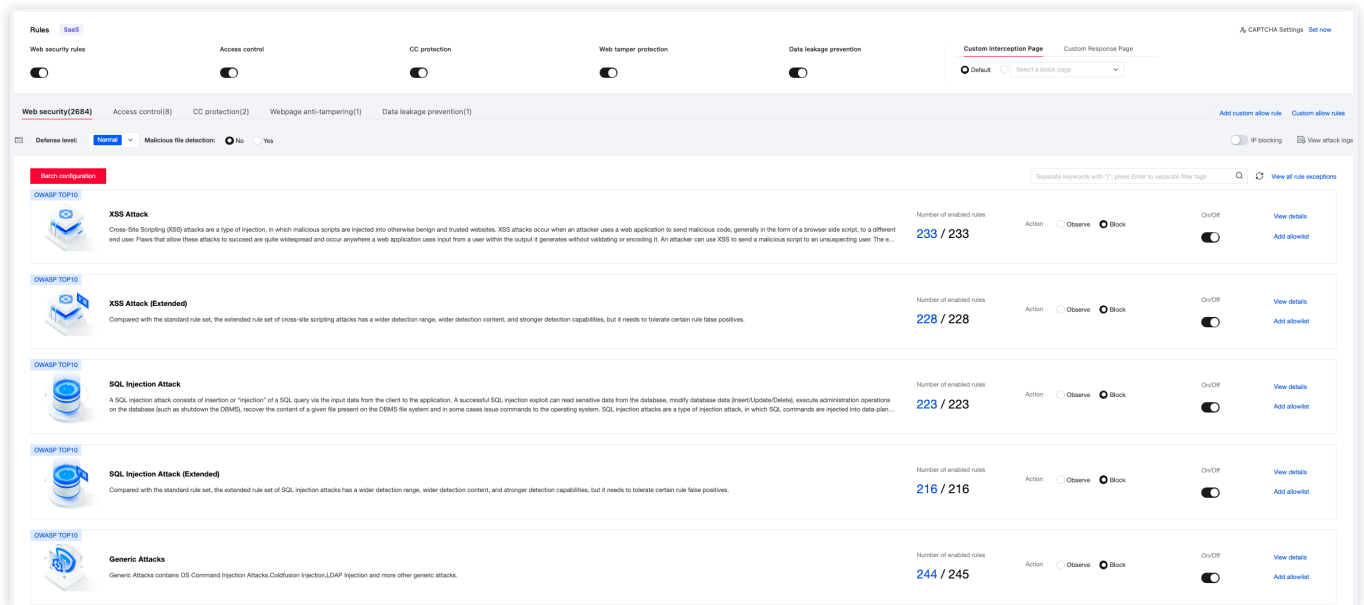
The WAF rule protection engine provides expert rule sets based on accumulated web threat intelligence to prevent OWASP top 10 attacks. Currently, it can defend against 12 categories of common web attacks, such as SQL injections, XSS attacks, malicious scans, command injection attacks, web application vulnerabilities, WebShell uploads, non-compliant protocols, Trojans, and backdoors.

The WAF rule protection engine supports rule level configuration. You can configure the rule protection level according to your actual business needs, and enable or disable rule sets, individual rules, and preset rules. You can also use the allowlist of specified URLs and rule IDs to process false positives.

Operation Steps

Settings of Domain Name Rule Protection Engine

1. Log in to the WAF console. In the left sidebar, select Configuration Center > Basic Security > WEB Security.
2. Configure the protection mode, protection level, and malicious file detection method of basic web protection on the Protection Settings page. You can also enable the anti-scanning feature and set IP address blocking rules.



Field description:

- Rule engine switch: Enabled, by default. When the switch is disabled, domain name requests transiting through the WAF will not undergo rule engine threat processing.
- Protection mode: Rule engine working mode, which is interception by default.
Observation: Does not block attack requests; makes predictions and produces observation logs.
Interception: Directly blocks web attack requests and produces interception logs.
- Protection level: Rule engine protection level, which is normal by default.
 - Normal: detects common web application attacks. If you notice excessive false interceptions at the default level, or if your workload involves significant uncontrolled user input (such as websites with rich text editors), it is recommended that you select this mode.
 - Strict: strictly detects web application attacks such as SQL injections, XSS attacks, and command execution. It is the default mode.
- Rule management: Through rule management, users can view rule engine information and set the rule engine, including viewing attack classifications, viewing rule content included in rule levels and rule set update dynamics, enabling or disabling single rules, and adding rules to the allowlist based on domain name URLs and rule IDs.
- Supported decoding types: The current rule engine supports the following decoding types by default, with manual settings not supported.
URL decoding (multiple decoding), javascript Unicode decoding, comment processing, space compression, UTF-7 decoding, HTML entity decoding, Multipart parsing, JSON parsing, XML parsing, and Form parsing.

Viewing rule classifications

1. Enter the Rule Engine Settings page.

- Method 1: Log in to the WAF console. In the left sidebar, choose Asset Center > Access Management



to enter the Domain Name List Management page. Select any domain name, and click the Protection Configuration button in the operation column to enter the Web Security Protection Configuration page of the domain name and view rule details.

o Method 2:

- Log in to the WAF console. In the left sidebar, choose Configuration Center > Basic Security.
- In the domain name list, click the domain name to be protected to enter the Web Security settings page and open the Rule Engine page.

2. Enter the Rule Base Management page.

Log in to the WAF console. In the left sidebar, choose Service Management > Web Rule Base. You can view the attack classification descriptions and rule update dynamic information supported by the current WAF for protection.

Web Rule Library			
Rules			
No	Attack type	Included rules	Web Rule Library
01000000	XSS Attack	233	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.
02000000	XSS Attack (Extended)	228	Compared with the standard rule set, the extended rule set of cross-site scripting attacks has a wider detection range, wider detection content, and stronger detection capabilities, but it needs to tolerate certain rule false positives.
03000000	SQL Injection Attack	223	A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of pre-defined SQL commands.
04000000	SQL Injection Attack (...)	216	Compared with the standard rule set, the extended rule set of SQL injection attacks has a wider detection range, wider detection content, and stronger detection capabilities, but it needs to tolerate certain rule false positives.
05000000	Generic Attacks	240	Generic Attacks contains OS Command Injection, Command Injection, LDAP Injection and more other generic attacks.
06000000	Generic Attacks(Extended)	207	Compared with the standard rule set, the extended rule set of generic attacks has a wider detection range, wider detection content, and stronger detection capabilities, but it needs to tolerate certain rule false positives.
09000000	Known Exploits	1277	Known Exploits are mainly used to detect remote arbitrary code execution vulnerabilities, remote arbitrary command execution vulnerabilities, path traversal vulnerabilities, open redirect vulnerabilities, unauthorized access vulnerabilities, etc. in various applications, web servers, middlewares, etc.
11000000	Bad Robot	65	Bad Robot detection is mainly used to detect malicious tools such as web scanners and script batch acquisition tools.
Total items: 8			
10 / 1 page			

The attack classifications supported by the current WAF for protection are as follows:

Attack Classification	Attack Description
XSS attack	The cross-site scripting (XSS) attack is a type of injection where malicious scripts are injected into other trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code (usually in the form of browser-side scripts) to different end users. The defects that allow these attacks to succeed are very common and occur whenever a web application uses input from a user in its generated output without verifying or encoding it. Attackers can use XSS to send malicious scripts to unsuspecting users. The end user's browser is unable to know that the script should not be trusted and will execute the script. Since it considers the script to come from a trustworthy source, the malicious script can access any cookies, session tokens, or other sensitive information reserved by the browser and used with that site. These scripts can even rewrite the contents of HTML pages.
XSS attack (extended)	The extended rule set of XSS attacks has a broader detection range, wider detection content, and stronger detection capability compared with the standard rule set, but it needs to tolerate certain rule false positives.



Attack Classification	Attack Description
SQL injection attack	SQL injection attacks include inserting or "injecting" SQL queries through input data from the client to the application. A successful SQL injection vulnerability can read sensitive data from the database, modify (insert/update/delete) database data, perform management operations on the database (such as shutting down the DBMS), recover the content of a given file existing in the DBMS file, and issue a command to the operating system in some cases. The SQL injection attack is a type of injection attack where SQL commands are injected into data plane inputs to impact the execution of predefined SQL commands.
SQL injection attack (extended)	The extended rule set of SQL injection attacks has a broader detection range, wider detection content, and stronger detection capability compared with the standard rule set, but it needs to tolerate certain rule false positives.
General attack	General attacks include operating system command injection attacks, Coldfusion injections, LDAP Injections, and other general attacks.
General attack (extended)	The extended rule set of general attacks has a broader detection range, wider detection content, and stronger detection capability compared with the standard rule set, but it needs to tolerate certain rule false positives.
Known weakness	Known weaknesses are primarily used to detect remote arbitrary code execution vulnerabilities, remote arbitrary command execution vulnerabilities, path traversal vulnerabilities, open redirection vulnerabilities, and unauthorized access vulnerabilities that occur in various applications, web servers, and middleware.
Bad bot	Bad bot detection is primarily used to detect malicious tools such as web scanners and script batch obtaining tools.

Rule management

1. Log in to the WAF console. In the left sidebar, choose Configuration Center > Basic Security. After selecting the domain name to be managed, enter the WEB Security page.
2. On the WEB Security Management page, you can enable or disable the rules, perform observation mode management, and add the rules to the allowlist.

Note:

The interception mode is enabled for all rules by default.



XSS Attack

OWASP TOP10

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts ar...

Number of enabled rules

233 / 233

Action

Observe

Block

On/Off

Batch Switch Rule Status

Click to select a filter

☐	Rule ID	Rule description	CVE number	Rule status	Severity	Last modi...	Creation time	Operation
☐	10000180	This signature prevents a...	--	Enable	Medium risk	2022-05-24 10:44:49	2022-05-12 13:43:28	Add allowlist View allowlist
☐	10000063	This signature prevents a...	--	Enable	Medium risk	2022-05-12 14:09:11	2022-05-12 13:43:33	Add allowlist View allowlist
☐	10000001	This signature prevents a...	--	Enable	Medium risk	2022-05-12 13:45:49	2022-05-12 13:43:30	Add allowlist View allowlist
☐	10000002	This signature prevents h...	--	Enable	Medium risk	2022-05-12 13:45:49	2022-05-12 13:43:31	Add allowlist View allowlist
☐	10000003	This signature prevents a...	--	Enable	Medium risk	2022-05-12 13:45:49	2022-05-12 13:43:33	Add allowlist View allowlist
☐	10000004	This signature prevents a...	--	Enable	Medium risk	2022-05-12 13:45:49	2022-05-12 13:43:29	Add allowlist View allowlist
☐	10000005	This signature prevents a...	--	Enable	Medium risk	2022-05-12 13:45:49	2022-05-12 13:43:31	Add allowlist View allowlist
☐	10000006	This signature prevents a...	--	Enable	Medium risk	2022-05-12 13:45:49	2022-05-12 13:43:27	Add allowlist View allowlist
☐	10000007	This signature prevents a...	--	Enable	Medium risk	2022-05-12 13:45:49	2022-05-12 13:43:32	Add allowlist View allowlist
☐	10000008	This signature prevents a...	--	Enable	Medium risk	2022-05-12 13:45:49	2022-05-12 13:43:27	Add allowlist View allowlist

Total items: 233

10 / page

1

/ 24 pages

3. Users can search for rule sets according to Rule Level, Attack Classification, and CVEID, or by entering Rule ID, and view specific rules and perform operations.

Note:
The strict rule level includes normal and strict rules.

Custom Policy

Custom policies support combining multiple characteristics of HTTP messages such as the request path, GET parameters, POST parameters, Referer, and User-Agent, and controlling the access of public network users through characteristic matching. Facing various attack behaviors from the Internet, users can use custom policies to respond flexibly and combine targeted rules to block these attack behaviors.

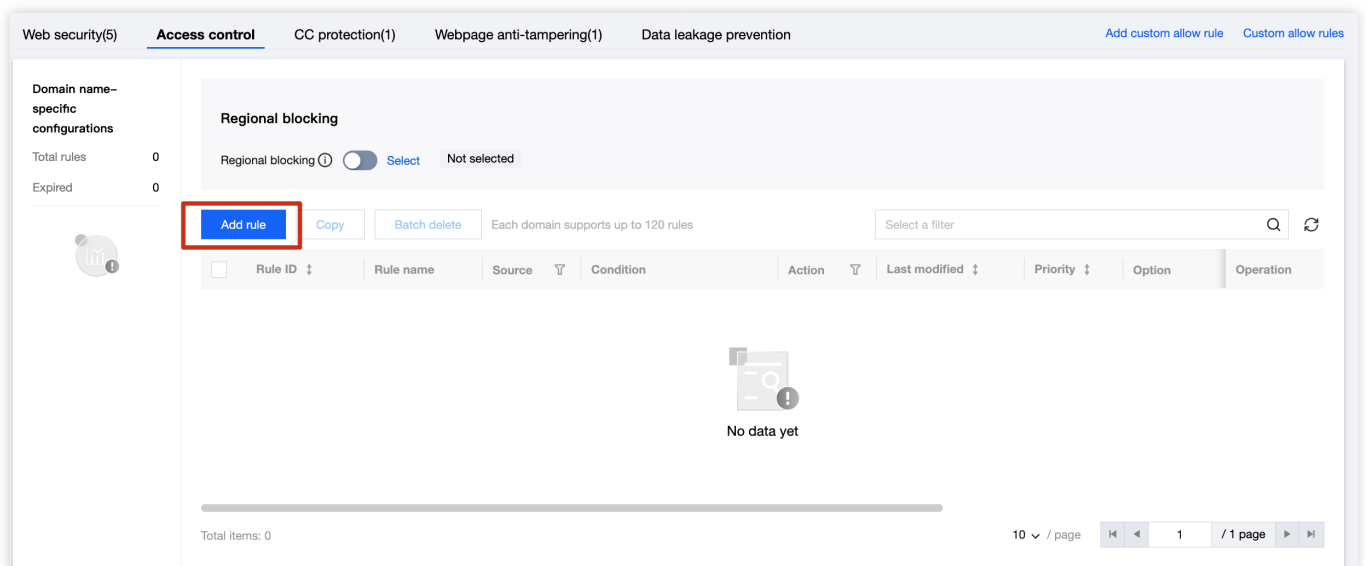
- Each custom policy can be set up to 5 conditions for characteristic control.
- The relationship between multiple conditions in each custom policy is "and", that is, all conditions should be matched for the policy to take effect.
- Two processing actions can be configured after each custom policy is matched: blocking and allowing.

Configuration Cases

Case 1: Prohibiting a Specific IP Address from Accessing a Specific Site

When website administrators need to prohibit a specific IP address from accessing a specified site, they can perform the following configurations:

1. Log in to the WAF console. In the left sidebar, select WAF > Configuration Center > Basic Security. Select a protected domain name (such as `www.cloudwaf.com`) and click to select Access Control to enter the configuration page.



2. On the Add Rule page, enter a rule name (such as 001). Select a field (such as Source IP) in the matching field and select Match for the logical symbol. Fill in the source IP to be blocked in the matching content (such as `192.168.1.1`) and select an execution action (such as Block). After completing, click Add to save

the rule.

Add custom protection rules

Rule name *

test

Condition *

Field	Parameter	Operator	Content	Operation
Source IP	N/A	Belong to	192.168.1.1	1 IPs now Delete

Add 14 more allowed (Max: 15)

Action *

Block

Option *

Permanent

Scheduled Effectiveness

Weekly Granularity Effective

Monthly Granularity Effective

Priority *

-

50

+

Enter an integer between 1-100. The smaller the number, the higher the execution priority of the rule.

OK

Back

The custom policy of WAF supports using masks to control access requests from source IP addresses in a specific IP range. We can enter a specific IP range in the matching content (such as 10.10.10.0/24).

3. The rule will take effect. HTTP access requests from the specific source IP will be blocked.

Web security(5) Access control(1) CC protection(1) Webpage anti-tampering(1) Data leakage prevention

Add custom allow rule Custom allow rules

Domain name-specific configurations

Total rules 1

Expired 0

Block

Regional blocking

Regional blocking ⓘ

Select

Not selected

Add rule

Copy

Batch delete

 Each domain supports up to 120 rules

Select a filter

☐	Rule ID ↓	Rule name	Source	Condition	Action	Last modified ↓	Priority ↓	Option	Operation
☐	1100000072	test	Domain name-specific	Source IP Belong to 192.168.1.1	Block	2025-09-26 04:35:07	50	Permanent	Edit Delete

Total items: 1

10 / page

1

 / 1 page

Case 2: Prohibiting Public Network Users from Accessing Specific Web Resources

When website administrators do not want public network users to access certain specific web resources (such as the management backend /admin.html), they can perform the following configurations:

Set the matching field to Request Path, set the logical symbol to Equal, fill in /admin.html as the matching content, and set the execution action to Block. After the configuration is completed, click Add.

**Add custom protection rules**

Rule name *

Condition *

Field	Parameter	Operator	Content	Operation
Request path	N/A	Is	/admin.html	11 characters Delete now

[Add](#) 14 more allowed (Max: 15)

Action *

Option * ☒ Permanent ☐ Scheduled Effectiveness ☐ Weekly Granularity Effective ☐ Monthly Granularity Effective

Priority * Enter an integer between 1-100. The smaller the number, the higher the execution priority of the rule.

Case 3: Prohibiting an External Site from Obtaining Resources Through Hotlink

When website administrators need to block hotlink activities from an external site (such as `www.test.com`), they can use custom policies to capture and block the Referer characteristics of hotlink requests.

The configurations are as follows: Set the matching field to Referer, set the logical symbol to Contain, fill in `www.test.com` as the matching content, and set the execution action to Block. After the configuration is completed, click Add.

Add custom protection rules

Rule name *

Condition *

Field	Parameter	Operator	Content	Operation
Referer	N/A	Is	www.test.com	12 characters Delete now

[Add](#) 14 more allowed (Max: 15)

Action *

Option * ☒ Permanent ☐ Scheduled Effectiveness ☐ Weekly Granularity Effective ☐ Monthly Granularity Effective

Priority * Enter an integer between 1-100. The smaller the number, the higher the execution priority of the rule.

Webpage Anti-Tampering

The anti-tampering feature can be used to prevent the specified page from being tampered with and displaying abnormally.

The specified page is limited to .html , .shtml , .txt , .js , .css , .jpg , .png , and other static resources.

Note:

CLB WAF instances do not support this feature.

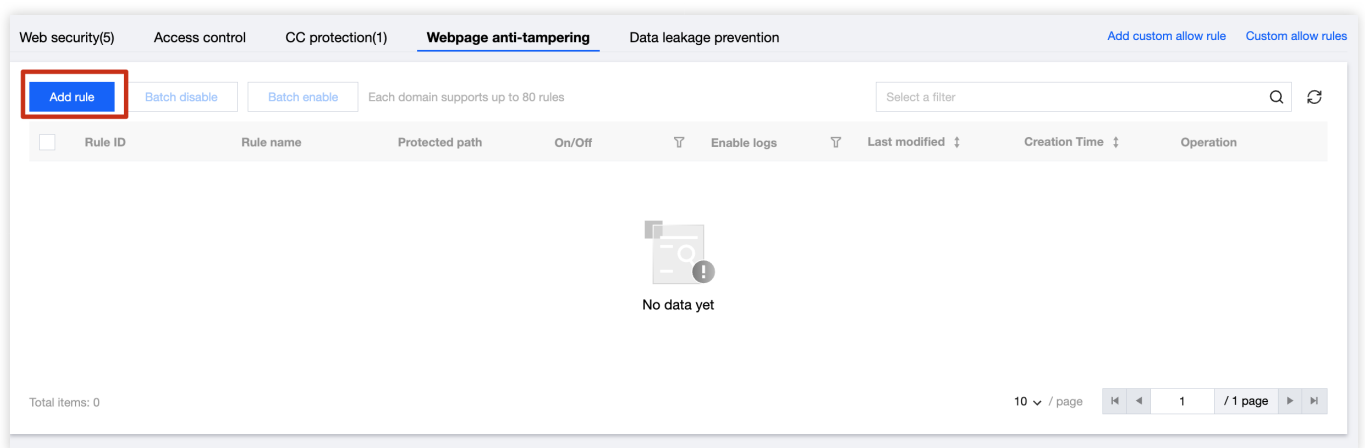
Configuration Example

Protecting Website Homepage from Tampering

1. Log in to the WAF console. In the left sidebar, select WAF > Configuration Center > Basic Security. Select a protected domain name (such as `www.cloudwaf.com`) and click to select Anti-tampering to enter the configuration page.



2. Enter the Protection Settings page. If required, replace the domain name of the site to be protected at the top. Click Anti-tampering to enter the Anti-tampering Configuration interface. Click Add Rule.



3. In the Add Anti-tampering Rule pop-up window, enter the rule name (such as homepage) and the complete URL path (such as `http://www.cloudwaf.com/index.html`) of the rule (such as homepage), and



click Add after entering to save the rule.

Add web tamper protection rule

If there is a Layer-7 proxy CDN service in front of the WAF, please refresh the CDN cache promptly to ensure the validity of testing.

Rule name

homepage

Page URL

/index.html

Please configure static resources such as .html, .shtml, .txt, .js, .css, .jpg, .png, or the access path of static resources.

Add

Cancel

4. The rule will take effect. If the rules are updated, click Refresh Cache in the right operation column to update the cache content.

Web security(5)Access controlCC protection(1)Webpage anti-tampering(1)Data leakage prevention

Add custom allow ruleCustom allow rules

Add ruleBatch disableBatch enable

Each domain supports up to 80 rules

Select a filter

☐	Rule ID	Rule name	Protected path	On/Off	Enable logs	Last modified	Creation Time	Operation
☐	3200000007	homepage	/index.html	☒	☐	2025-09-26 04:33:30	2025-09-26 04:33:30	Refresh Edit Delete

Total items: 1

10 / page

1 / 1 page

Information Leakage Prevention

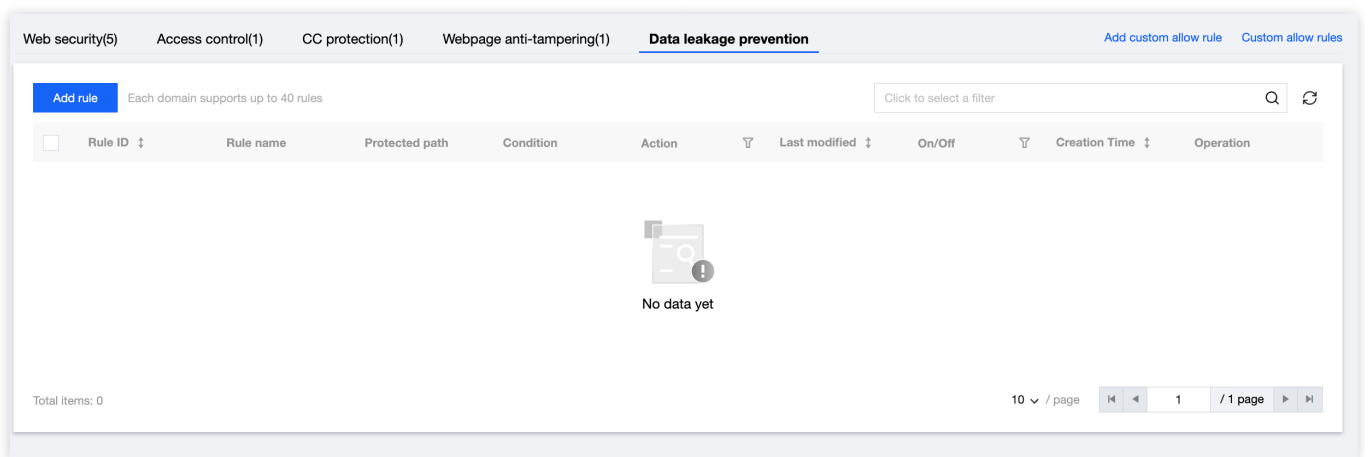
1. Feature Introduction

The information leakage prevention feature supports replacing sensitive information returned on your webpage, such as phone numbers and ID numbers.

Remarks: CLB WAF instances do not support this feature.

2. Configuration Example

1. Log in to the WAF console. In the left sidebar, select WAF > Configuration Center > Basic Security. Select a protected domain name (such as `www.waf.com`) and click to select Information Leakage Prevention to enter the configuration page. Select Information Leakage Prevention > Add Rule.



On the Add Rule page, enter the rule name, select the matching condition (the matching field is Sensitive Information, the matching condition is Contain, and the matching content is ID Card or Mobile Number) and execution action (Replace or Observe), and click OK to save.



Add data leakage prevention rule

Rule name *

test

Condition *

Sensitive data

Content *

☒ ID card ☐ Mobile ☐ Bank card

Protected path *

/

Action *

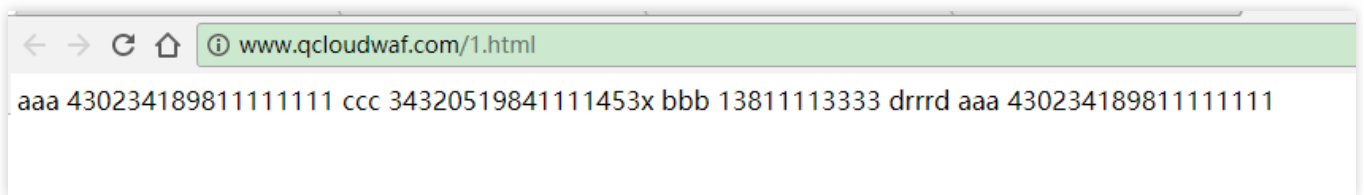
Show the first 4 digits

OK

Back

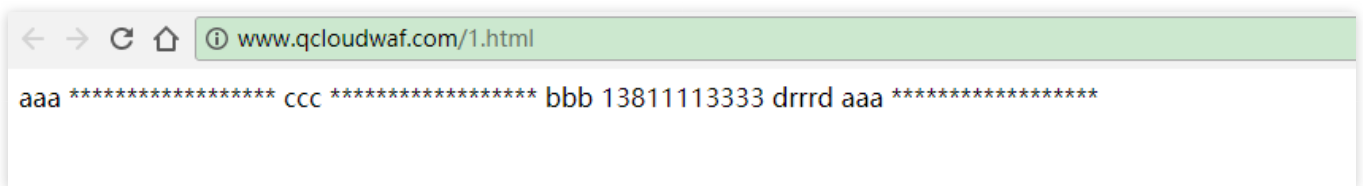
2. When the rule takes effect, it will protect the sensitive information returned from your webpage. The protection effect is as follows (the sensitive content is fictitious):

- Before the protection is enabled:



Before the protection is enabled

- After the protection is enabled:

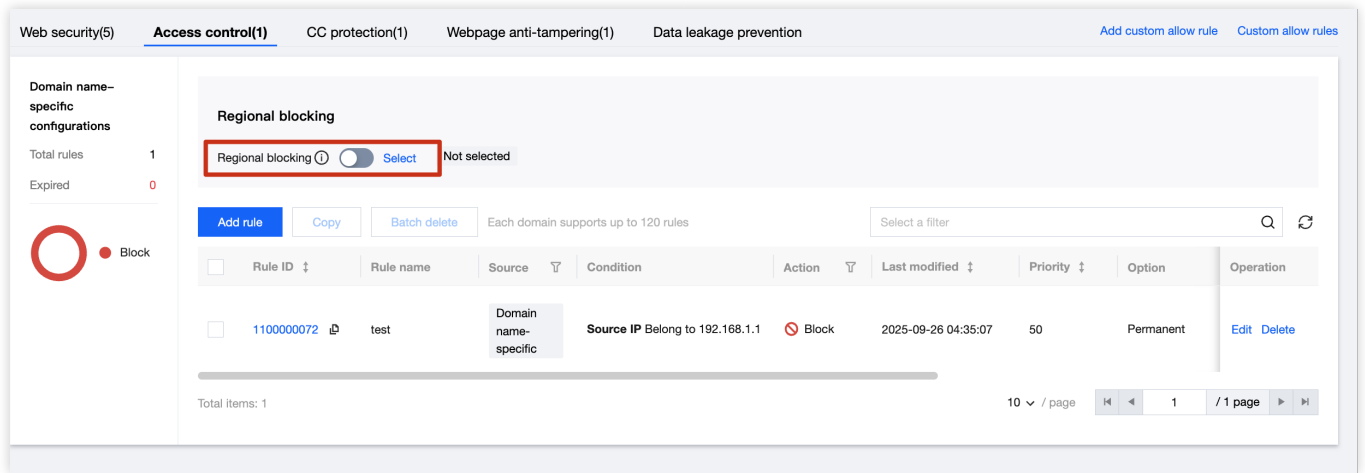


After the protection is enabled

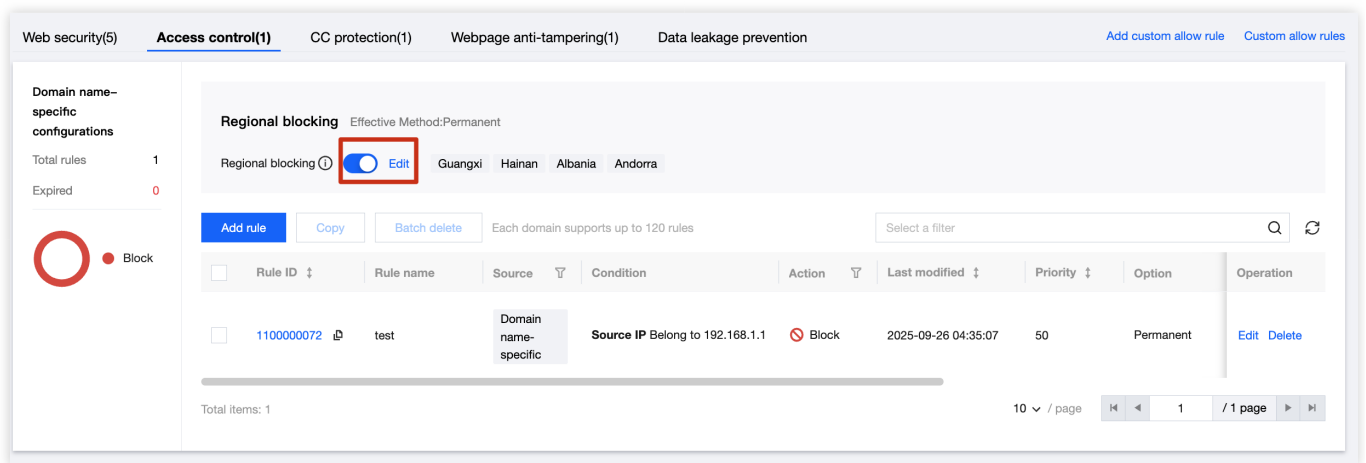
Regional Blocking

Configuration Instructions

1. Log in to the WAF console. In the left sidebar, choose Web Application Firewall (WAF) > Configuration Center > Basic Security. Select a protected domain name (such as `www.qcloudwaf.com`) and click Access Control to enter the Configuration page and perform the regional blocking configuration.



2. On the Access Control Settings page, click Select to enter the regional blocking configuration page.
3. On the Blocked Region Settings page, check the regions that need to be blocked. You can search or click the dropdown list to select. After selecting the regions, click OK.



4. After editing, enable the regional blocking status.
5. The regions you have selected to block will not be able to access your website. In this document, after all



external regions are listed as blocked regions, WAF will prompt that you have been intercepted when you use an IP address outside the allowed regions to access the protected website.

Attack Log

By default, WAF records web attack log information, including the attack occurrence time, attack source IP address, attack type, and attack details. You can query logs according to the filter conditions and download the query results as needed.

Usage Instructions

Querying Attack Logs

1. Log in to the WAF console. In the left sidebar, choose Log Service > Attack Logs to enter the Attack Log Query page. Click Log Query, select a domain name from the dropdown search list above, set query conditions as needed, and click Query to view the corresponding attack log information.

The screenshot shows the 'Attack Logs' query interface. At the top, there are dropdowns for 'All instances' and 'All domains'. Below these is a 'Log collection' section with filters for 'All attack types', 'All actions', and 'All risk levels'. A search bar is labeled 'Filter by attack source IP'. To the right of the search bar are date pickers for 'Last 30 ...' (set to 2025-08-27 08:51:01) and a range from 2025-08-26 08:51:01 to 2025-09-26 08:51:01. There is an 'Auto-refresh' toggle and a red 'Search' button. Below the filters is a 'Raw data' section with a table of log entries. The table has columns: 'Logging time', 'attack_ip', 'status', 'method', 'url', 'proto_domain', 'domain', 'attack_type', 'rule_id', 'risk_level', 'count', and 'Operation'. Three log entries are visible, all with a status of 'Block' and a count of 1. The risk levels are 'Low risk', 'Medium risk', and 'Medium risk'. The operations are 'Block source IP'.

Logging time	attack_ip	status	method	url	proto_domain	domain	attack_type	rule_id	risk_level	count	Operation
2025-09-19 12:27:46	[REDACTED]	Block	GET	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Low risk	1	Block source IP
2025-09-19 12:26:37	[REDACTED]	Block	GET	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Medium risk	1	Block source IP
2025-09-19 12:09:06	[REDACTED]	Block	GET	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Medium risk	1	Block source IP

Query condition description:

- Domain name: Select the domain name to be queried in the domain name dropdown search list.
- Time condition: 1 hour, by default. You can query the attack log information from the last 30 days at most.
- Risk level: All, by default. You can select high risk, medium risk, or low risk.
- Execution action: All, by default. You can select observing or intercepting.
- Policy ID: Enter the policy ID you need to query. (The policy ID can be viewed in the log entry.)
- Attack source IP: Enter the attack source IP to conduct a query.

2. Click the Set button in the upper right corner of the attack log. In the Custom List Fields pop-up window, select the list details to display, as shown in the figure below:



Set column fields

Please select

Field

☒ Logging time

☐ Log data

☐ attack_area

☒ attack_ip

☒ status

☒ method

☒ uri

Selected(12)

Field

Logging time

attack_ip

status

method

uri

prote_domain

domain

attack_type

×

×

×

×

×

×

×

×

↔

OK

Cancel

3. View attack details. Select the log entry you need to view and click Details in the right operation column to view attack details.

Attack Logs

All instances

All domains

Log collection

All attack types

All actions

All risk levels

Filter by attack source IP

Last 30 d...

2025-08-27 04:55:03 ~ 2025-09-26 04:55:03

Raw data

Logging time ↓	attack_ip	status	method	uri	prote_domain	domain	Operation
▶ 2025-09-19 12:27:46	192.168.1.1	Block	GET	/api/v1/...	...	...	Block source IP
▶ 2025-09-19 12:26:37	192.168.1.1	Block	GET	/api/v1/...	...	...	Block source IP
▶ 2025-09-19 12:09:06	192.168.1.1	Block	GET	/api/v1/...	...	...	Block source IP
▶ 2025-09-19 12:07:41	192.168.1.1	Block	GET	/api/v1/...	...	...	Block source IP

4. Enter the Log Details page and view corresponding fields.

Attack Logs

All instances All domains

Log collection

All attack types All actions All risk levels Filter by attack source IP Last 30 d... 2025-08-27 04:55:03 ~ 2025-09-26 04:55:03 📅 ⓘ

Raw data

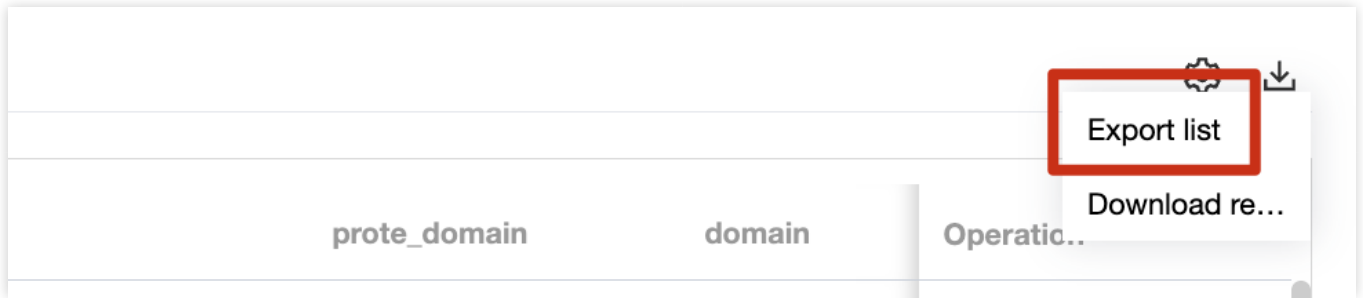
Logging time ↓	attack_ip	status	method	uri	prote_domain	domain	Operation
▼ 2025-09-19 12:27:46	[REDACTED]	Block	GET	[REDACTED]	[REDACTED]	[REDACTED]	Block source IP

Log details JSON

```
{
  "time": "2025-09-19T12:27:46Z",
  "action": "block_source_ip",
  "ai_flag": false,
  "appid": "AI-BOT-001",
  "args_name": null,
  "attack_category": "bot_attack",
  "attack_content": "[\"IP\", \"URI\"]",
  "attack_ip": "[REDACTED]",
  "attack_place": "http",
  "attack_time": "2025-09-19T12:27:46Z",
  "attack_type": "get_request",
  "bot_id_type": "header_bot",
  "count": 1,
  "create_time": "2025-09-19T12:27:46Z",
  "domain": "[REDACTED]",
  "edition": "v1.0",
  "engine": "AI",
  "headers": {
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36",
    "Accept-Language": "zh-CN,zh;q=0.9,en;q=0.8"
  },
  "host": "[REDACTED]",
  "http_log": "[REDACTED] \\naccept:\\\"\\r\\n\\\""}
}
```

Exporting Attack Logs

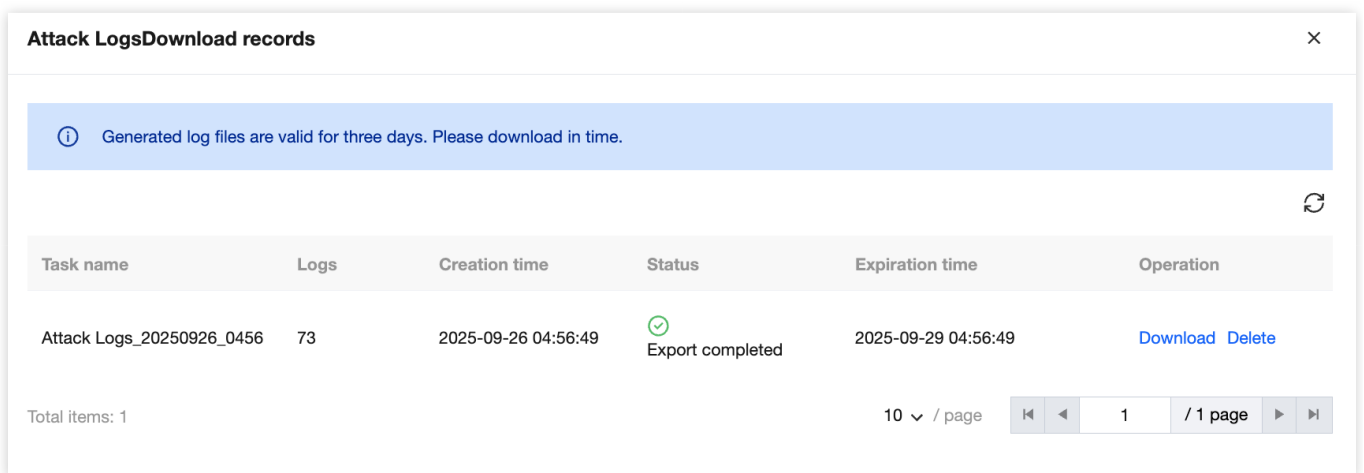
1. Log in to the WAF console. In the left sidebar, select Log Service > Attack Logs to enter the Attack Log Query page. Click Log Query, select a domain name from the dropdown search list above, set query conditions as needed, and click Query to view the corresponding attack log information. Click Export Logs to export the corresponding attack log information.



Export condition description:

- Domain name: Select the domain name to be queried in the domain name dropdown search list.
- Time condition: 1 hour, by default. You can query the attack log information from the last 30 days at most.
- Risk level: All, by default. You can select high risk, medium risk, or low risk.
- Execution action: All, by default. You can select observing or intercepting.
- Policy ID: Enter the policy ID you need to query. (The policy ID can be viewed in the log entry.)
- Attack source IP: Enter the attack source IP to conduct a query.
- Log table content cannot be empty.

2. Choose Log Service > Attack Logs > Download Task to enter the download task query page, as shown in the figure below:



3. Click Download, and a prompt "The address of the log file has been successfully copied. Open it in a new browser window" will appear. Copy the link to the browser and open it to successfully download the



compressed log file.

Attack LogsDownload records

Generated log files are valid for three days. Please download in time.

Task name	Logs	Creation time	Status	Expiration time	Operation
Attack Logs_20250926_0456	73	2025-09-26 04:56:49	Export completed	2025-09-29 04:56:49	Download Delete

Total items: 1

10 / page

1 / 1 page

Log details field description:

- Basic information

Field Name	Field Description
Domain Name	Client access domain name.
Attack Type	Information on the attack types currently supported by WAF. The default value is All.
Number of Aggregate Attacks	Total number of attacks generated every 10 seconds with the same attack source IP address and attack type.
Attack Source IP Address	Source IP address of the client attack.
Hit Rule ID	The rule ID that triggers the protection policy. For attacks detected by the AI engine, the rule ID is 0.
Hit Rule Name	The policy name that triggers the protection policy. The policy name of the rule engine and AI engine is empty.
Request Method	Client attack request method.
Risk Level	The risk level triggered by the client attack.
Attack Time	The time when the client attack is triggered.
Matching Source	Client attack matching source information, such as the source IP address.
Execution Action	Actions triggered by the client attack.
Request URI	Request URI content.



Field Name	Field Description
Attack Content	The content of the triggered client attack.

- Attack IP details

Field Name	Field Description
Region	English abbreviation of the country where the source IP address is used
IP Owner	Owner information of the used source IP address
Country	Country name of the attack source IP address
Province	Province information of the attack source IP address
City	City information of the attack source IP address
ISP	ISP information of the attack source IP address
Longitude	Longitude information of the attack source IP address
Latitude	Latitude information of the attack source IP address

- Detailed information

Field Name	Field Description
Protocol Version	HTTP protocol version information of the attack source IP address
User-Agent	Browser type and operating system identifier provided by the attack source IP address to the server

Glossary

SSL Certificate

Secure Sockets Layer (SSL) is a security protocol designed to ensure the security and data integrity of internet communication. Based on the SSL protocol, an SSL certificate can be installed on a server to achieve encrypted data transmission.

Proxy Server

Proxy server is a core server security feature which is applicable to the session layer in the Open Systems Interconnection (OSI) model. It can improve the access speed, hide real website IPs, and enhance website security.

Domain Name Resolution

Servers on the internet communicate with each other through IP addresses. However, most people are used to remembering a domain name that can be mapped to multiple IP addresses. The conversion between a domain name and an IP address is called domain name resolution.

The following are common domain name resolution types:

- A record resolution: It specifies the IPv4 address of the domain name.
 - Select "A" as the record type.
 - Enter the server IP address provided by Converge Cloud as the record value.
 - MX priority does not need to be configured.
 - Set TTL to 600 by default.
- CNAME record resolution: It is used to point a domain name to another one which will be used to provide the IP address.
 - Select "CNAME" as the record type.
 - Enter the CNAME record generated after the protected domain name is added to WAF as the record value.
 - MX priority does not need to be configured.
 - Set TTL to 600 by default.

Security Groups

A security group is a virtual firewall that features stateful data packet filtering. It is used to configure the network access control of CVM instances. You can add CVM instances with the same network security isolation requirements in the same region to the same security group to filter their inbound and outbound traffic through the network policies of the security group.

VIP Address



After you add a domain name, WAF will automatically allocate a VIP address to it accordingly, which will act as the ingress address of WAF when the real server receives access requests. The access traffic will be forwarded to the VIP after DNS resolution and then to WAF.

Intermediate IP Address

After you add a domain name, WAF will automatically allocate multiple intermediate IP addresses to it accordingly, which can be used as the egress IPs of WAF to forward filtered normal traffic to your real server.

DNS Hijacking Protection

DNS hijacking protection provides DNS hijacking detection rules for site users to avoid data theft and financial loss caused by malicious hijacking, where attackers attack the DNS server or fake a new DNS server for the client domain name to be incorrectly resolved to malicious sites.

CC Attack Protection

Challenge Collapsar (CC) attack protection refers to a protection service against CC attacks where attackers use certain tools to simulate multiple users in order to continuously send connection requests to your website and make your business unavailable. You can add CC protection rules to defend against CC attacks for webpage requests.

QPS

Queries per second (QPS) is a metric measurement how much traffic is processed by a particular query server within the specified time period. On the internet, the performance of DNS servers is often measured with QPS, which corresponds to fetches/sec (responded requests per second, i.e., the maximum throughput).