Web Application Firewall

Service Overview

Issue	06
Date	2024-11-05

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 What Is WAF?

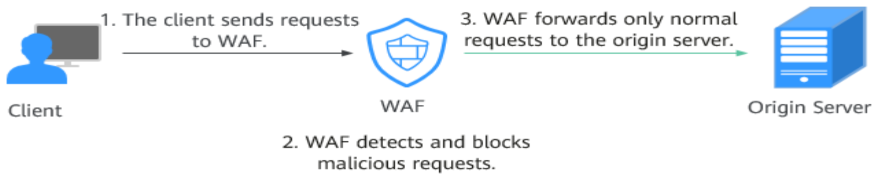
Web Application Firewall (WAF) keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

After you purchase a WAF instance, add your website domain to the WAF instance on the WAF console. All public network traffic for your website then goes to WAF first. WAF identifies and filters out the illegitimate traffic, and routes only the legitimate traffic to your origin server to ensure site security.

How WAF Works

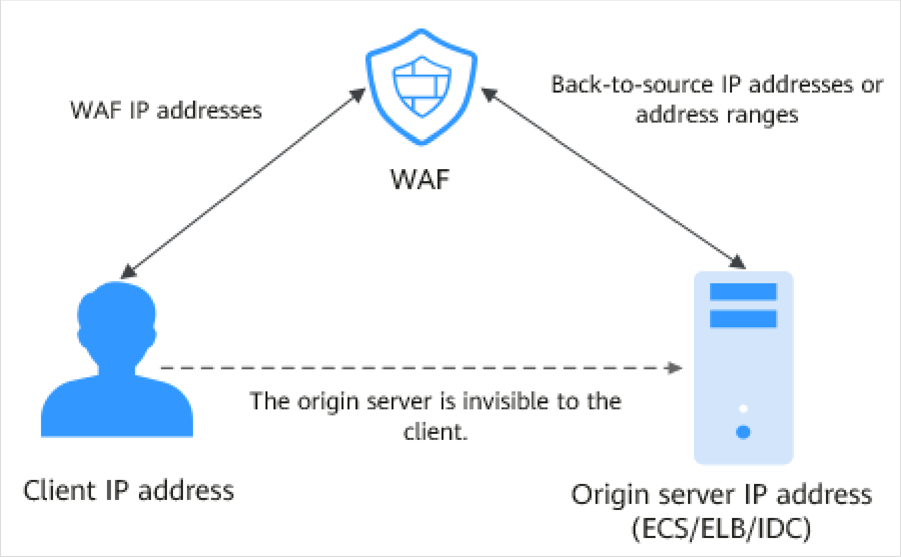
After applying for WAF, add the website to WAF on the WAF console. After a website is connected to WAF, all website access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to ensure that the origin server is secure, stable, and available.

Figure 1-1 How WAF Works


1. The client sends requests to WAF.
3. WAF forwards only normal requests to the origin server.
Client
WAF
Origin Server
2. WAF detects and blocks malicious requests.

The process of forwarding traffic from WAF to origin servers is called back-to-source. WAF uses back-to-source IP addresses to send client requests to the origin server. When a website is connected to WAF, the destination IP addresses to the client are the IP addresses of WAF, so that the origin server IP address is invisible to the client.

Figure 1-2 Back-to-source IP address


WAF IP addresses
WAF
Back-to-source IP addresses or address ranges
The origin server is invisible to the client.
Client IP address
Origin server IP address (ECS/ELB/IDC)

What WAF Protects

WAF offers the cloud and dedicated modes to protect websites. You can add either domain names or IP addresses to WAF. Before you start, get familiar with the following differences:

- Cloud mode: protects your web applications on or off the cloud through domain names.
- Dedicated mode: domain names or IP addresses (public or private IP addresses) for web services on the cloud

2 Edition Differences

WAF supports yearly/monthly and pay-per-use billing. Different billing modes support different editions. You can select a proper service edition based on your service requirements and website deployment mode.

- Access modes

  WAF provides cloud mode and dedicated mode. For details about the different access modes and service editions, see **Figure 2-1**. You can select a proper access mode and the service edition by referring to **Cloud and Dedicated WAF Modes**.

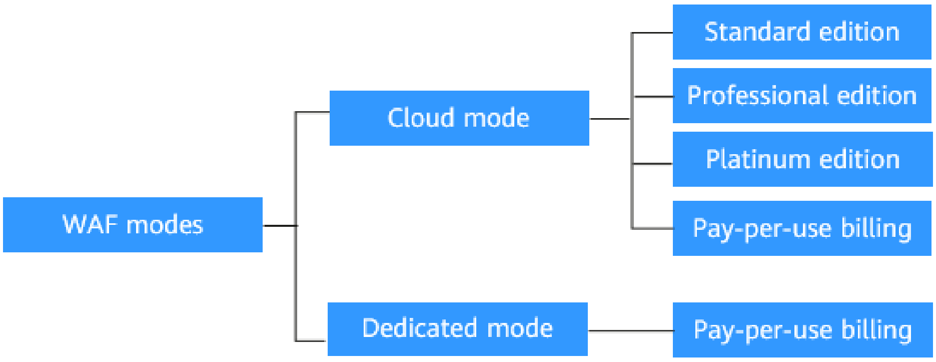
- Service edition specifications

  To support different workloads scales, WAF provides multiple editions. You can check **Specifications Supported by Each Edition** and select a service version suitable for your workloads scale.

- Service edition functions

  The service functions you can use may differ in different editions and different access modes. Before you start, check the service edition and access mode you plan to use by referring to **Functions Supported by Each Service Edition** and make sure the one you select can meet your service needs.

Figure 2-1 Service editions and modes



Cloud and Dedicated WAF Modes

To support different service scenarios, WAF provides cloud and dedicated access modes. The deployment architecture is shown in **Figure 2-2**. For details about the differences, see **Table 2-1**.

Figure 2-2 Deployment architecture

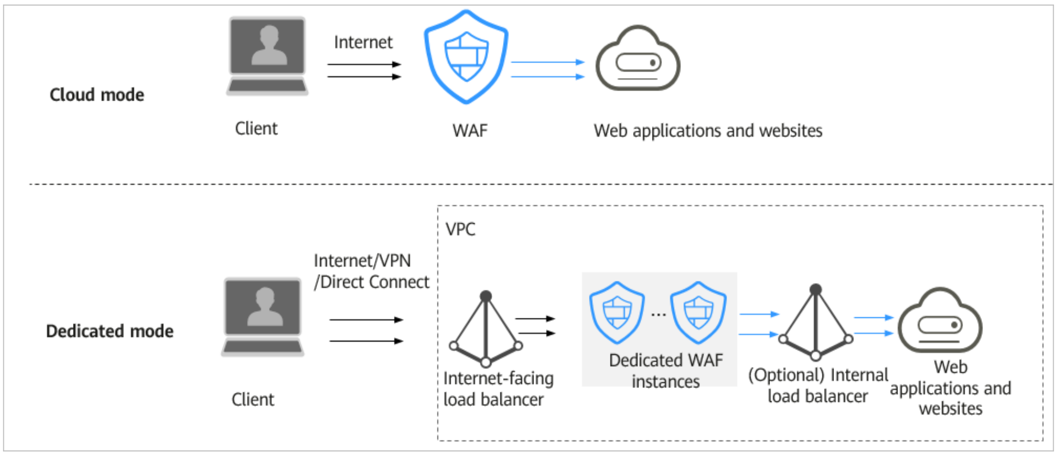


Table 2-1 Differences between WAF modes

Item	Cloud Mode	Dedicated Mode
Billing mode	● Yearly/Monthly ● Pay-per-use billing	Pay-per-use billing
Edition	The following editions support the yearly/monthly billing mode: ● Standard ● Professional ● Platinum	-

Item	Cloud Mode	Dedicated Mode
Application scenarios	Service servers are deployed on any cloud or in on-premises data centers. The application scenarios for different editions are as follows: ● Standard This edition is suitable for small and medium-sized websites that do not have special security requirements. ● Professional This edition is suitable for medium-sized enterprise websites or services that are open to the Internet, focus on data security, and have high security requirements. ● Platinum This edition is suitable for large and medium-sized enterprise websites that have a large service scale or have customized security requirements.	Service servers are deployed on Huawei Cloud. This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements.
Protected objects	Domain names	● Domain names ● IP addresses (public or private IP addresses)
Advantages	● Protection capability scaling by upgrading specifications ● Protection for cloud and on-premises web services ● IPv6 protection	● Enable cloud and on-premises deployment. ● Enable exclusive use of WAF instance. ● Meet requirements for protection against large-scale traffic attacks. ● Deploy dedicated WAF instances in a VPC to reduce network latency.

Specifications Supported by Each Edition

Table 2-2 lists the service specifications supported by each WAF edition. In cloud mode, to protect more domain names and traffic, you can either purchase domain name, QPS, and rule expansion packages or **change the edition of your cloud WAF instance**.

📖 NOTE

WAF provides the same service specifications in the **Cloud Mode - Load Balancer Access** and **Cloud Mode - CNAME Access** modes. So the two modes can share the domain name, QPS, and rule expansion package quotas.

Table 2-2 Applicable service scales

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Peak rate of normal service requests	● Service requests: 2,000 QPS ● You can purchase a QPS expansion package. One QPS expansion package can support 1000 QPS.	● Service requests: 5,000 QPS ● You can purchase QPS expansion packages. One QPS expansion package can support 1,000 QPS.	● Service requests: 10,000 QPS ● You can purchase a QPS expansion package. One QPS expansion package can support 1000 QPS.	WAF-to-Server connections: 6,000 per domain name	The following lists the specifications of a single instance. ● Specifications: WI-500. Referenced performance: – HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000. – HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000. – WebSocket service - Maximum concurrent connections: 5,000 – Maximum WAF-

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
	NOTE If the origin server is deployed on Huawei Cloud, a QPS expansion package can be used to expand the bandwidth by 50 Mbit/s. If the origin server is not deployed on Huawei Cloud, a QPS expansion package can be used to expand the bandwidth by 20 Mbit/s. ● WAF-to-Server connections: 6,000 per domain name	**NOTE** If the origin server is deployed on Huawei Cloud, a QPS expansion package can be used to expand the bandwidth by 50 Mbit/s. If the origin server is not deployed on Huawei Cloud, a QPS expansion package can be used to expand the bandwidth by 20 Mbit/s. ● WAF-to-Server connections: 6,000 per domain name	**NOTE** If the origin server is deployed on Huawei Cloud, a QPS expansion package can be used to expand the bandwidth by 50 Mbit/s. If the origin server is not deployed on Huawei Cloud, a QPS expansion package can be used to expand the bandwidth by 20 Mbit/s. ● WAF-to-Server connections: 6,000 per domain name		to-server persistent connections: 60,000 ● Specifications: WI-100. Referenced performance: – HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000. – HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600 – WebSocket service - Maximum concurrent connections: 1,000

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
					– Maximum WAF-to-server persistent connections: 60,000 **NOTICE** Maximum QPS values are for your reference only. They may vary depending on your businesses. The real-world QPS is related to the request size and the type and quantity of protection rules you customize.

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Service bandwidth threshold (The origin server is deployed on the cloud.)	● 100 Mbit/s ● You can purchase QPS expansion packages. One QPS expansion package can support a bandwidth of 50 Mbit/s. **NOTE** A QPS expansion package can support 1,000 QPS at the same time.	● 200 Mbit/s ● You can purchase QPS expansion packages. One QPS expansion package can support a bandwidth of 50 Mbit/s. **NOTE** A QPS expansion package can support 1,000 QPS at the same time.	● 300 Mbit/s ● You can purchase QPS expansion packages. One QPS expansion package can support a bandwidth of 50 Mbit/s. **NOTE** A QPS expansion package can support 1,000 QPS at the same time.	-	● Specifications: WI-500. Performance: Throughput: 500 Mbit/s ● Specifications: WI-100. Referenced performance: Throughput: 100 Mbit/s

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Service bandwidth threshold (The origin server is not deployed on Huawei Cloud.)	● 30 Mbit/s ● You can purchase QPS expansion packages. One QPS expansion package can support a bandwidth of 20 Mbit/s. **NOTE** A QPS expansion package can support 1,000 QPS at the same time.	● 50 Mbit/s ● You can purchase QPS expansion packages. One QPS expansion package can support a bandwidth of 20 Mbit/s. **NOTE** A QPS expansion package can support 1,000 QPS at the same time.	● 100 Mbit/s ● You can purchase QPS expansion packages. One QPS expansion package can support a bandwidth of 20 Mbit/s. **NOTE** A QPS expansion package can support 1,000 QPS at the same time.	-	N/A

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Number of domains	● 10 (Supports one top-level domain name.) ● You can purchase domain expansion packages. A domain expansion package supports 10 extra domain names (one top-level domain name is supported).	● 50 (Supports five top-level domain names.) ● You can purchase domain expansion packages. A domain expansion package supports 10 extra domain names (one top-level domain name is supported).	● 80 (Supports eight top-level domain names.) ● You can purchase domain expansion packages. A domain expansion package supports 10 extra domain names (one top-level domain name is supported).	200 (Supports 20 top-level domain names.)	2,000 (Supports 2,000 top-level domain names)

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Back-to-source IP address quantity (the number of WAF back-to-source IP addresses that can be allowed by a protected domain name)	20	50	80	20	N/A
Peak rate of CC attack defense	100,000 QPS	200,000 QPS	1,000,000 QPS	N/A	● Specifications: WI-500. Referenced performance: Maximum QPS: 20,000 ● Specifications: WI-100. Referenced performance: Maximum QPS: 4,000
Number of CC attack defense rules	20	50	100	200	100
Number of precise protection rules	20	50	100	200	100

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Number of reference table rules	N/A	50	100	200	100
Number of IP address blacklist or whitelist rules	● 1,000 ● You can buy rule expansion package to increase the quota. A rule expansion package supports 10 IP blacklist and whitelist protection rules.	● 2,000 ● You can buy rule expansion package to increase the quota. A rule expansion package supports 10 IP blacklist and whitelist protection rules.	● 5,000 ● You can buy rule expansion package to increase the quota. A rule expansion package supports 10 IP blacklist and whitelist protection rules.	200	1,000
Number of geolocation access control rules	N/A	50	100	200	100
Number of web tamper protection rules	20	50	100	200	100

Service Scale	Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-use Billing (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Website anti-crawler protection	N/A	50	100	200	100
Number of information leakage prevention rules	N/A	50	100	200	100
Global protection whitelist rules	1,000	1,000	1,000	2,000	1,000
Number of data masking rules	20	50	100	200	100

NOTICE

- The number of domains is the total number of top-level domain names (for example, example.com), single domain names/second-level domains (for example, www.example.com), and wildcard domain names (for example, *.example.com). For example, the standard edition WAF can protect up to 10 domain names. You can add one top-level domain name and nine subdomain names or wildcard domain names related to the top-level domain name.
- If a domain name maps to different ports, each port is considered to represent a different domain name. For example, **www.example.com:8080** and **www.example.com:8081** are counted towards your quota as two distinct domain names.
- You can upload as many certificates in WAF as the number of domain names that can be protected by your WAF instances in the same account. For example, if you purchase a standard edition WAF instance, which can protect 10 domain names, a dedicated WAF instance, which can protect 2,000 domain names, and a domain name expansion package (20 domain names), your WAF instances can protect 2,030 domain names total (2,000 + 20 +10). In this case, you can upload 2,030 certificates.

Functions Supported by Each Service Edition

WAF provides different features in different WAF editions and access modes. For details, see **Table 2-3**.

Notes:

- √: The function is included in the current edition.
- x: The function is not included in the current edition.
- -: This function is not involved because the similar functions are available in ELB.

Table 2-3 Security features

Function		Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Domain Expansion Package	One domain package can protect 10 domain names, including a maximum of one top-level domain name.	√	√	√	×

Function		Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
QPS Expansion Package	A QPS expansion package protects up to: ● For web applications deployed on Huawei Cloud – Service bandwidth: 50 Mbit/s – QPS: 1,000 ● For web applications not deployed on Huawei Cloud – Service bandwidth: 20 Mbit/s – QPS: 1,000	√	√	√	×
Rule Expansion Package	A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.	√	√	√	×
Wildcard domain name	Wildcard domain names (for example, *.example.com) can be added to WAF.	√	√	√	√
Protection for ports except 80 and 443	WAF can protect services on specific non-standard ports in addition to standard ports 80 and 443.	√	√	√	√
Protection for ports except ports 80 and 443	Non-standard ports can be protected.	×	√	√	×

Function		Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Batch configuring defense policies	You can flexibly configure protection policies for protected domain names in batches.	×	√	√	√
Batch adding domain names to a policy	Batch adding domain names to a policy	×	√	√	√
Common web application attack defense	WAF defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/ code injections.	√	√	√	√
Zero-day vulnerability protection	WAF can update protection rules against zero-day vulnerabilities to the latest on the cloud and deliver virtual patches in a timely manner	√	√	√	×
Webshell Detection	WAF can protect web applications from web shells.	√	√	√	√
Deep Inspection	WAF can identify and block evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques.	√	√	√	√

Function		Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
Header Inspection	WAF detects all header fields in the requests.	√	√	√	√
CC Attack Protection	You can customize a CC attack protection rule to restrict access to your website based on an IP address, cookie, or Referer, mitigating CC attacks.	√	√	√	√
Precise Protection	You can configure complex conditions by combining common HTTP fields to match requests precisely. You can log only, allow, or block matched requests.	√ (excluding full detection)	√	√	√
Reference Table Management	You can configure single-type protection metrics, such as paths, user agent, IP, params, cookie, referer, and headers, in batches.	×	√	√	√
IP Address Blacklist and Whitelist	You can allow or block specific IP addresses in one click. IP addresses or IP address segments can be imported in batches.	√	√	√	√
Geolocation Access Control	You can allow or block web requests based on the countries that the requests originate from.	×	√	√	√
Web Tamper Protection	You can lock website pages (such as sensitive pages) to prevent malicious content tampering.	√	√	√	√
Anti-crawler Protection	WAF can identify and block crawler behavior such as search engines, scanners, script tools, and other crawlers.	×	√	√	√

Function		Standard Edition (Cloud Mode)	Professional Edition (Cloud Mode)	Platinum Edition (Cloud Mode)	Pay-per-Use Billing (Dedicated Mode)
	WAF supports JavaScript-based anti-crawler protection.	×	√	√	√
Number of information leakage prevention rules	WAF can prevent leakage of privacy data, such as ID card numbers, phone numbers, and email addresses.	×	√	√	√
Global protection whitelist rules	You can configure global protection whitelist to ignore false positives.	√	√	√	√
Data Masking	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.	√	√	√	√
Resource requirement suggestions	When using dedicated instances, you are advised to configure resource monitoring and alarms on Cloud Eye. It is recommended that the CPU usage be no more than 70% and the memory usage be no more than 80%. **NOTE** When there are a large number of service requests or complex user-defined protection policies, the CPU and memory usage increases. In extreme cases, the performance fluctuates greatly. You are advised to evaluate the performance specifications based on the pressure tests made on your service model.	-	N/A	-	√

3 Basic Concepts

This document describes terms related to WAF.

CC Attack

Challenge Collapsar (CC) attacks are web attacks against web servers or applications. In CC attacks, attackers send a large amount of standard GET/POST requests to target system to exhaust web servers or applications. For example, attackers can send requests to URIs of databases or other resources to make the servers unable to respond to normal requests.

Cross-Site Request Forgery (CSRF)

CSRF, or XSRF is a common web attack. Attackers may trick the victim into submitting a malicious request that inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf. If the user is currently authenticated to the site, the site will have no way to distinguish between the forged request and a legitimate request sent by the victim, as browser requests always carry session cookies associated with the site.

Scanner

A scanner is a program that automatically detects security vulnerabilities on local or remote servers. It can quickly and accurately detect vulnerabilities of scanned targets and provide scanning results for users.

Web Tamper Protection

Web Tamper Protection (WTP) can protect your files, such as web pages, documents, images, and databases, in specific directories against tampering and sabotage from hackers and viruses.

Cross-site Scripting (XSS) Attack

XSS is a type of attack that exploits security vulnerabilities in web applications. The attacker injects auto-executed malicious code into webpages to steal user information when they visit the pages.

SQL Injection

SQL injection is a common web attack whereby attackers inject malicious SQL commands into query strings of backend databases for the victim web application to deceive the server into executing them. By exploiting these commands, the attacker can obtain sensitive information, add users, export files, or even gain the highest permissions to the database or system.

Command Injection

Command injection is a cyber attack that executes fabricated OS commands and escape from a blacklist by calling web APIs to attack services.

Code Injection

Code injection is an attack that exploits logic defects of web applications in input validation or code execution vulnerabilities of some script functions.

Sensitive File Access

Sensitive files, such as configuration files and permission management files related to the operating system and application service framework, are mission-critical data. If sensitive files are accessible through Internet requests, the services will be at risk.

Server-Side Request Forgery

Server-side request forgery (SSRF) is a web security vulnerability constructed by an attacker to form a request initiated by the server. Generally, the target of an SSRF attack is the internal system that cannot be accessed from the external network. If a server supports obtaining data from other server applications but not filters or restricts destination addresses, an SSRF vulnerability may be made by attackers.

Web Shell

A web shell is an attack script. After intruding into a website, an attacker adds an .asp, .php, .jsp, or .cgi script file with normal web page files. Then, the attacker accesses the file from a web browser and uses it as a backdoor to obtain a command execution environment for controlling the web server. So, web shells are also called backdoor tools.

Hotlinking

Hotlinking is an act that a crafty website links to files hosted on your servers, instead of storing files on their own servers. Generally, the crafty website links to large files, such as images and videos, as large files use much more bandwidth than small ones. So you have to pay for access traffic of the bad actors. They steal your server bandwidth, making your website slow.

Multi-pattern Matching

Multi-pattern matching is a highly efficient multi-mode matching algorithm that is used for feature detection of request traffic, which greatly improves the performance of the detection engine.

Precise Protection

You can create a custom precise protection rule that combines multiple common HTTP fields, such as the URL, IP, Params, Cookie, Referer, User-Agent, and Header. You can also combines logic conditions to block or allow traffic precisely.

Blacklist and Whitelist

The IP address whitelist includes trusted IP addresses. Requests from the trusted IP addresses are forwarded without inspection. The IP address blacklist includes malicious IP addresses. The traffic from these IP addresses is handled based on inspection policies.

Intelligent Decoding

This is a method that intelligently identifies multiple codes in a request for infinite multi-layer obfuscation and performs in-depth decoding to obtain the original attack intent of the attacker.

Semantic Analysis-based Detection

A syntax tree is constructed based on the semantic context to analyze and determine whether the payload is an attack payload.

Rate Limit

Access control policies are used to limit the access over a specific interface.

Anti-Crawler

An extensive crawler feature library is provided to detect many types of crawlers (search engines, scanners, script tools, and other crawlers).

A Record

An address (A) record maps a host name (or domain name) to the IP address of the server hosting the domain name.

SQL Injection Attack

SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution.

Non-standard Port

Non-standard ports are the ports other than ports 80 and 443.

4 Functions

WAF helps you protect services from various web security risks. The following table lists the functions of WAF.

Function		Description
Service configuration	Protection for IP addresses and domain names (wildcard, top-level, and second-level domain names)	WAF offers the cloud and dedicated modes to protect websites. You can add either domain names or IP addresses to WAF. Before you start, get familiar with the following differences: ● Cloud mode: protects your web applications on or off the cloud through domain names. ● Dedicated mode: domain names or IP addresses (public or private IP addresses) for web services on the cloud
	HTTP/HTTPS service protection	WAF can protect HTTP and HTTPS traffic for a website.
	WebSocket/ WebSockets	WAF can check WebSocket and WebSockets requests, which is enabled by default.
	Non-standard port protection	In addition to standard ports 80 and 443, WAF also supports non-standard ports.

Function		Description
Web application security protection	Basic Web Protection **NOTE** If you set **Protective Action** to **Block**, you can use the known attack source function. It means that if WAF blocks malicious requests from a visitor, you can enable this function to let WAF block requests from the same visitor for a period of time.	With an extensive preset reputation database, WAF defends against Open Web Application Security Project (OWASP) top 10 threats, vulnerability exploits, web shells, and other threats. ● General Check WAF defends against attacks such as SQL injections, XSS, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. ● Web shell detection WAF protects against web shells from upload interface. ● Precise identification – WAF uses built-in semantic analysis engine and regex engine and supports configuring of blacklist/whitelist rules, which reduces false positives. – WAF supports anti-escape and automatic restoration of common codes, which improves the capability of recognizing deformation web attacks. WAF can decode the following types of code: url_encode, Unicode, XML, OCT, hexadecimal, HTML escape, and base64 code, case confusion, JavaScript, shell, and PHP concatenation confusion ● Deep inspection WAF identifies and blocks evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques. ● Header detection WAF detects all header fields in the requests. ● Shiro Decryption Check WAF uses AES and Base64 to decrypt the rememberMe field in cookies and checks whether this field is attacked.

Function		Description
	CC attack protection rules	WAF can restrict access to a specific URL on your website based on a unique IP address, cookie, or referer field, mitigating CC attacks.
	Precise protection rules **NOTE** If you set **Protective Action** to **Block**, you can use the known attack source function. It means that if WAF blocks malicious requests from a visitor, you can enable this function to let WAF block requests from the same visitor for a period of time.	WAF enables you to combine common HTTP fields (such as IP, path, referer, user agent, and params) to configure powerful and precise access control policies. You can configure precision protection rules to protect workloads from hotlinking and block requests with empty fields.
	Blacklist and whitelist rules **NOTE** If you set **Protective Action** to **Block**, you can use the known attack source function. It means that if WAF blocks malicious requests from a visitor, WAF will proactively block requests from the same visitor for a period of time.	You can configure blacklist and whitelist rules to block, log only, or allow access requests from specified IP addresses.
	Geolocation access control rules	You can customize these rules to allow or block requests from a specific country or region.
	Web tamper protection rules	You can configure these rules to prevent a static web page from being tampered with.

Function		Description
	Website anti-crawler protection	WAF dynamically analyzes your website service models and accurately identifies more than 700 types of crawler behavior based on data risk control and bot identification systems ● Feature library Blocks web page crawling with user-defined scanner and crawler rules. This feature improves protection accuracy. ● JavaScript Identifies and blocks JavaScript crawling with user-defined rules.
	Information leakage prevention rules	You can add two types of information leakage prevention rules. ● Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, and email addresses). ● Response code interception: blocks the specified HTTP status codes.
	Global protection whitelist rules	This function ignores certain attack detection rules for specific requests.
	Data masking rules	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.
Advanced settings	IPv6 protection	● WAF can inspect requests that use both IPv4 and IPv6 addresses for the same domain name. ● For web services that still use the IPv4 protocol stack, WAF supports the NAT64 mechanism. NAT64 is an IPv6 conversion mechanism that enables communication between the IPv6 and IPv4 hosts using network address translation (NAT). WAF can convert an IPv4 source site to an IPv6 website and converts external IPv6 access traffic to internal IPv4 traffic.

Function		Description
	Configuring connection timeout	● The default timeout for connections from a browser to WAF is 120 seconds. The value varies depending on your browser settings and cannot be changed on the WAF console. ● The default timeout for connections between WAF and your origin server is 30 seconds. You can customize a timeout on the WAF console as long as you are using a dedicated WAF instance or professional or platinum cloud WAF.
Event management		● WAF allows you to view and handle false alarms for blocked or logged events. ● You can download events data over the past five days.
Notifications		This topic describes how to enable notifications for attack logs. Once this function is enabled, WAF sends you SMS or email notifications if an attack is detected. You can configure certificate expiration reminders. When a certificate is about to expire, WAF notifies you by the way you configure, such as email or SMS.
GUI-based security data		WAF provides a GUI-based interface for you to monitor attack information and event logs in real time. ● Centralized policy configuration On the WAF console, you can configure policies applicable to multiple protected domain names in a centralized manner so that the policies can be quickly delivered and take effect. ● Traffic and event statistics WAF displays the number of requests, the number and types of security events, and log information in real time.

Function	Description
High flexibility and reliability	WAF can be deployed on multiple clusters in multiple regions based on the load balancing principle. This can prevent single points of failure (SPOFs) and ensure online smooth capacity expansion, maximizing service stability.

5 Product Advantages

WAF examines web traffic from multiple dimensions to accurately identify malicious requests and filter attacks, reducing the risks of data being tampered with or stolen.

Precisely and Efficiently Identify Threats

- WAF uses rule and AI dual engines and integrates our latest security rules and best practices.
- You can configure enterprise-grade policies to protect your website more precisely, including custom alarm pages, combining multiple conditions in a CC attack protection rule, and blacklisting or whitelisting a large number of IP addresses.

Zero-Day Vulnerabilities Patched Fast

A specialized security team provides 24/7 service support to fix zero-day vulnerabilities within 2 hours.

Strong Protection for User Data Privacy

- Sensitive information, such as accounts and passwords, in attack logs can be anonymized.
- PCI-DSS checks for SSL encryption are available.
- The minimum TLS protocol version and cipher suite can be configured.

6 Application Scenarios

Common protection

WAF helps you defend against common web attacks, such as command injection and sensitive file access.

Protection for online shopping mall promotion activities

Countless malicious requests may be sent to service interfaces during online promotions. WAF allows configurable rate limiting policies to defend against CC attacks. This prevents services from breaking down due to many concurrent requests, ensuring response to legitimate requests.

Protection against zero-day vulnerabilities

Services cannot recover quickly from impact of zero-day vulnerabilities in third-party web frameworks and plug-ins. WAF updates the preset protection rules immediately to add an additional protection layer to such web frameworks and plug-ins, and this layer can react faster than fixing the vulnerabilities.

Data leakage prevention

WAF prevents malicious actors from using methods such as SQL injection and web shells to bypass application security and gain remote access to web databases. You can configure anti-data leakage rules on WAF to provide the following functions:

- Precise identification

  WAF uses semantic analysis & regex to examine traffic from different dimensions, precisely detecting malicious traffic.
- Distortion attack detection

  WAF detects a wide range of distortion attack patterns with 7 decoding methods to prevent bypass attempts.

Web page tampering prevention

WAF ensures that attackers cannot leave backdoors on your web servers or tamper with your web page content, preventing damage to your credibility. You can configure web tamper protection rules on WAF to provide the following functions:

- Website malicious code detection

  You can configure WAF to detect malicious code injected into web servers and ensure secure visits to web pages.

- Web page tampering prevention

  WAF prevents attackers from tampering with web page content or publishing inappropriate information that can damage your reputation.

7 Project and Enterprise Project

Project

Projects in IAM are used to group and isolate OpenStack resources (computing resources, storage resources, and network resources). Resources in your account must be mounted under projects. A project can be a department or a project team. Multiple projects can be created under one account.

Enterprise Project

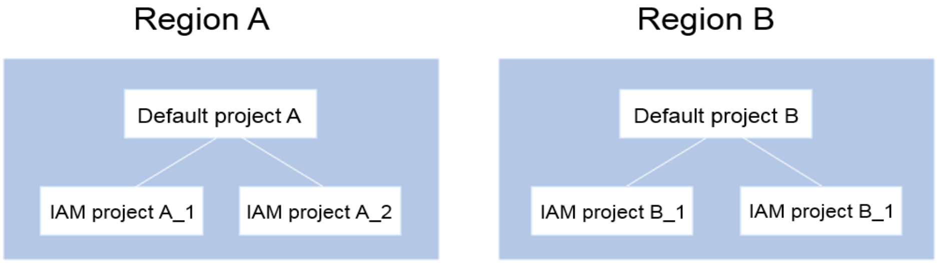
Enterprise projects are used to categorize and manage multiple resources. Resources of the same type can be put under an enterprise project. The use of enterprise projects does not affect the use of HSS.

You can classify resources by department or project group and put related resources into one enterprise project for management. Resources can be moved between enterprise projects.

Differences Between Projects and Enterprise Projects

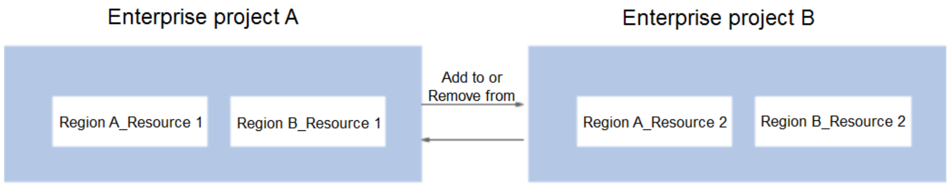
- IAM Project

  Projects are used to categorize and physically isolate resources in a region. Resources in an IAM project cannot be transferred. They can only be deleted and then rebuilt.



- Enterprise Project

  Enterprise projects are upgraded based on IAM projects and used to categorize and manage resources of different projects of an enterprise. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects. If you have enabled enterprise management, you cannot create an IAM project and can only manage existing projects. In the future, IAM projects will be replaced by enterprise projects, which are more flexible.



Both projects and enterprise projects can be managed by one or more user groups. Users who manage enterprise projects belong to user groups. After a policy is granted to a user group, users in the group can obtain the permissions defined in the policy in the project or enterprise project.

8 Personal Data Protection Mechanism

To ensure that website visitors' personal data, such as the username, password, and mobile phone number, will not be obtained by unauthorized or unauthenticated entities or people and to prevent data leakage, WAF encrypts your personal data before storing it to control access to the data and records logs for operations performed on the data.

Personal Data to Be Collected

WAF records requests that trigger attack alarms in event logs. **Table 8-1** provides the personal data collected and generated by WAF.

Table 8-1 Personal data

Type	Collection Method	Can Be Modified	Mandatory
Request source IP address	Attacker IP address that is blocked or recorded by WAF when the domain name is attacked.	No	Yes
URL	Attacked URL of the protected domain name, or URL of the protected domain name that is blocked or recorded by WAF.	No	Yes

Type	Collection Method	Can Be Modified	Mandatory
HTTP/HTTPS header information (including the cookie)	Cookie value and header value entered on the configuration page when you configure a CC attack or precise protection rule.	No	No If the configured cookie and header fields do not contain users' personal information, the requests recorded by WAF will not collect or generate such personal data.
Request parameters (Get and Post)	Request details recorded by WAF in protection logs.	No	No If request parameters do not contain users' personal information, the requests recorded by WAF will not collect or generate such personal data.

Storage Mode

The values of sensitive fields are saved after being anonymized, and the values of other fields are saved in plaintext in logs.

Access Control

Users can view only logs related to their own services.

9 WAF Permissions Management

To assign different permissions to employees in your enterprise to access your WAF resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your cloud resources.

With IAM, you can use your Huawei ID to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use WAF resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using WAF resources.

If your Huawei ID does not need individual IAM users for permissions management, then you may skip over this chapter.

IAM can be used free of charge. You pay only for the resources in your account. For more details, see **IAM Service Overview**.

WAF Permissions

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

WAF is a project-level service deployed and accessed in specific physical regions. To assign WAF permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing WAF, the users need to switch to a region where they have been authorized to use the WAF service.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. You need to also assign other dependent roles for the permission control to take effect. Roles are not ideal for fine-grained authorization and secure access control.

- Policies: A fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you can grant WAF users only the permissions for managing a certain type of resources. Most policies define permissions based on APIs. For the API actions supported by WAF, see **Permissions Policies and Supported Actions**.

Table 9-1 lists all the system roles supported by WAF.

Table 9-1 System policies supported by WAF

Role/Policy Name	Description	Category	Dependencies
WAF Administrator	Administrator permissions for WAF	System-defined role	Dependent on the **Tenant Guest** and **Server Administrator** roles. ● **Tenant Guest**: A global role, which must be assigned in the global project. ● **Server Administrator**: A project-level role, which must be assigned in the same project.
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

WAF FullAccess Policy Content

```
{    "Version": "1.1",
      "Statement": [
          {
             "Action": [
               "waf:*:*",
               "lts:groups:get",
               "lts:groups:list",
               "lts:topics:get",
               "lts:topics:list",
               "smn:*:list*",
               "vpc:*:get*",
               "vpc:*:list*",
               "ecs:*:get*",
               "ecs:*:list*",
               "elb:*:get*",
               "elb:*:list*"
            ],
               "Effect": "Allow"
         }
```

```
                ]
}
```

WAF ReadOnlyAccess Policy Content

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
              "waf:*:get*",
              "waf:*:list*",
              "lts:groups:get",
              "lts:groups:list",
              "lts:topics:get",
              "lts:topics:list",
              "smn:*:list*",
              "vpc:*:get*",
              "vpc:*:list*",
              "ecs:*:get*",
              "ecs:*:list*",
              "elb:*:get*",
              "elb:*:list*"
          ],
              "Effect": "Allow"
        }
    ]
}
```

10 WAF and Other Services

This topic describes WAF and other cloud services.

CTS

Cloud Trace Service (CTS) records all WAF operations for you to query, audit, and backtrack.

Cloud Eye

Cloud Eye monitors the indicators of WAF, so that you can learn of the protection status of WAF in a timely manner, and set protection policies accordingly. For details, see the *Cloud Eye User Guide*.

For details about monitored WAF metrics, see **WAF Monitored Metrics**.

ELB

You can add your WAF instances to a load balancer so that your website traffic is distributed by the load balancer across WAF instances for detection and then forwarded by WAF to the origin server. In this way, website traffic will be protected even if one of your WAF instances becomes faulty.

IAM

Identity and Access Management (IAM) provides the permission management function for WAF. Only users granted WAF Administrator permissions can use WAF. To obtain this permission, contact the users who have the Security Administrator permissions.

LTS

Log Tank Service (LTS) collects log data from hosts and cloud services. WAF allows you to transfer WAF attack logs and access logs to LTS so that you can handle with logs in real time.

SMN

Simple Message Notification (SMN) service provides the notification function. After you enable the notification function in WAF, alarm information will be sent to you as configured once your domain name is attacked.

Enterprise Management

You can manage multiple projects in an enterprise, separately settle their costs, and assign different personnel for them. A project can be started or stopped independently without affecting others. With Enterprise Management, you can easily manage your projects after creating an enterprise project for each of them.

WAF can be interconnected with Enterprise Management. You can manage WAF resources by enterprise project and grant different permissions to users.