Web Application Firewall

Service Overview

Issue 83

Date 2024-06-05

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

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

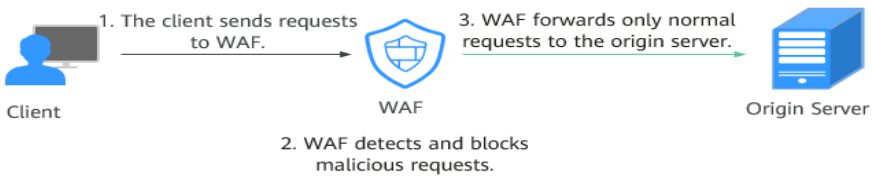
1 What Is WAF?

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).

How WAF Works (Cloud - CNAME and Dedicated Access)

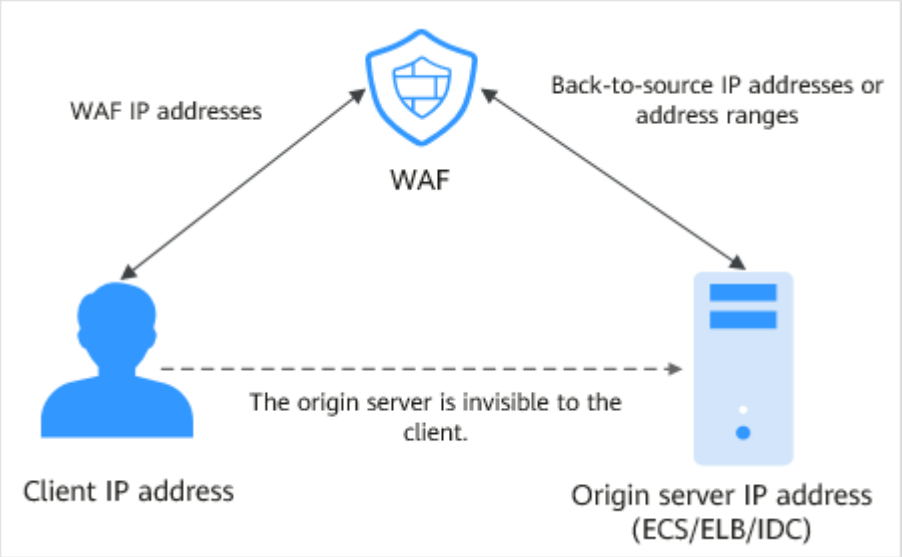
After a website is connected to cloud WAF through a CNAME record, all website access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to ensure that the origin server is secure, stable, and available.

Figure 1-1 How WAF Works



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

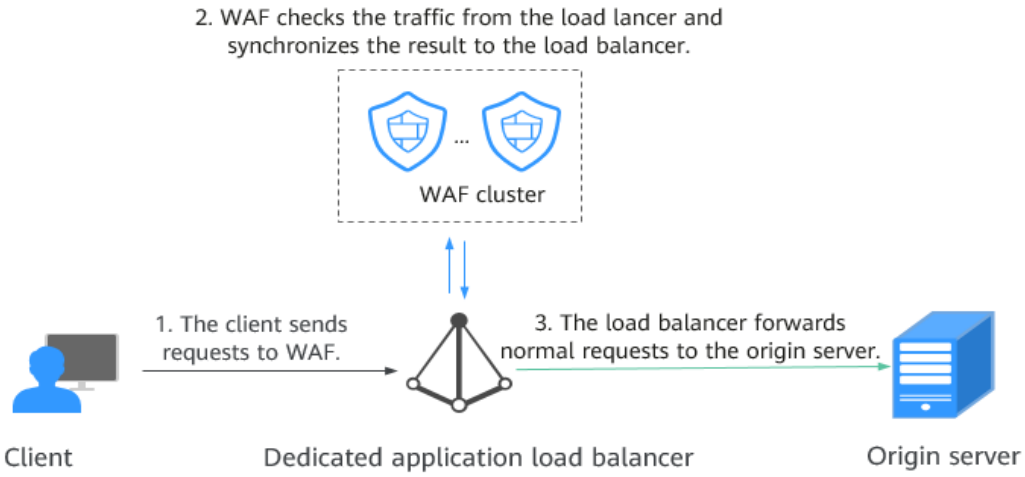


How WAF Works (Cloud - ELB Access)

Cloud WAF provides an ELB access method.

- In this method, WAF is integrated into the gateway of an ELB load balancer through an SDK module. WAF extracts traffic through the SDK module embedded in the gateway for inspection.
- WAF synchronizes the inspection result to the load balancer, and the load balancer determines whether to forward client requests to the origin server based on the inspection result.
- In this method, WAF does not forward traffic. This reduces compatibility and stability problems.

Figure 1-3 How WAF in ELB access mode works



What WAF Protects

When adding a website to WAF, you can select **Cloud - CNAME**, **Cloud - Load balancer**, or **Dedicated** for **Protection**. Before you start, get familiar with the following differences:

- **Cloud - CNAME**: protects your web applications that have domain name and are deployed on any clouds or in on-premises data centers.
- **Cloud - Load balancer**: protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses.
- **Dedicated**: protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses.

2 Edition Differences

WAF provides cloud and dedicated deployments. In cloud deployment, you can select the CNAME access or ELB access method. For more details, see **Cloud and Dedicated WAF Modes**.

NOTE

- To use ELB-access cloud WAF, you need to **submit a service ticket** to enable it for you first. ELB-access cloud WAF is available in some regions. For details, see **Functions**.
- If you want to use the ELB access mode, make sure you are using standard, professional, or platinum cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule extension packages are shared between the ELB access and CNAME access modes.

Cloud and Dedicated WAF Modes

You can select CNAME access or ELB access in cloud mode or dedicated mode to deploy WAF instances for your workloads. **Figure 2-1** shows the deployment architectures. **Table 2-1** describes the differences between them.

Figure 2-1 Deployment architecture

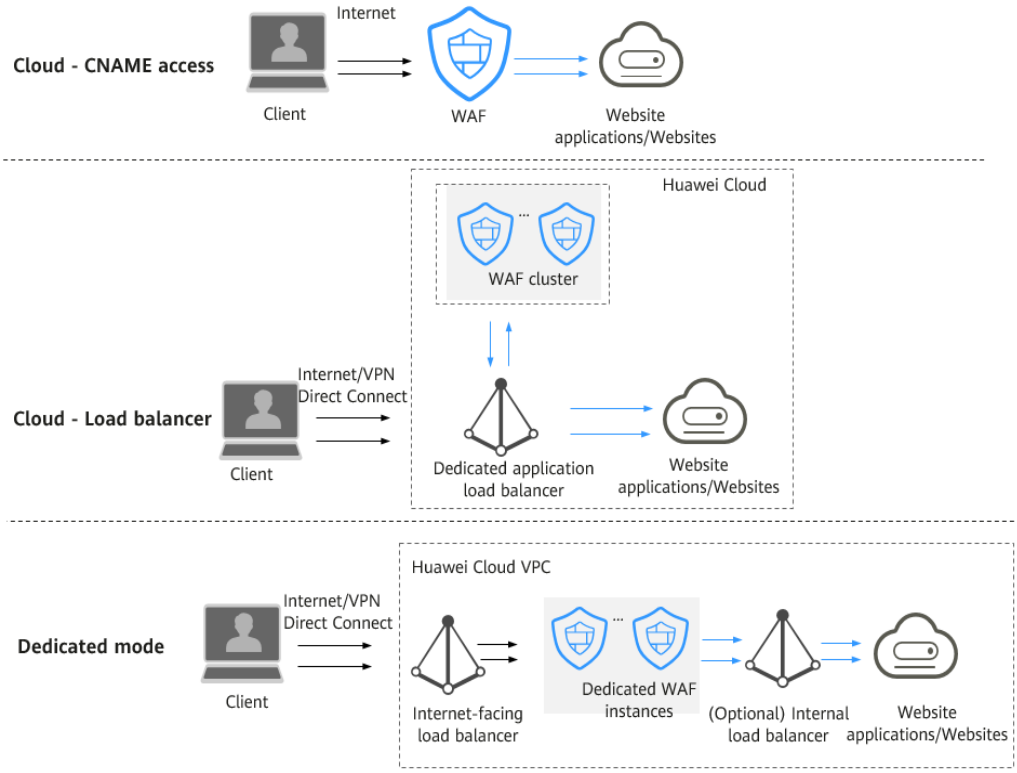


Table 2-1 Description of how to use different modes of WAF instances

Item	Cloud Mode		Dedicated Mode
	CNAME Access	ELB Access	
Billing mode	• Yearly/Monthly • Pay-per-use **NOTE** If you buy a cloud WAF instance, you can change its billing mode anytime you want.	If you have purchased cloud WAF (standard, professional, or platinum edition), CNAME and ELB access methods share the domain name, bandwidth, and rule extension packages you have purchased.	Pay-per-use
Edition	The following editions support the yearly/monthly billing mode: • Standard • Professional • Platinum	N/A	N/A

Item	Cloud Mode		Dedicated Mode
	CNAME Access	ELB Access	
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 edition Suitable for small- and medium-sized websites that do not have special security requirements • Professional edition Suitable for medium-sized enterprise websites or services that are open to the Internet, focus on data security, and have high security requirements • Platinum edition 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. Large enterprise websites having high security requirements on service stability	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.
Protection object	Domain names	• Domain names • IP addresses	• Domain names • IP addresses

Item	Cloud Mode		Dedicated Mode
	CNAME Access	ELB Access	
Advantages	• Expand protection capability by upgrading specifications. • Protect cloud and on-premises web services. • Protect IPv6 addresses.	• Scaling out of your WAF protection capabilities without changing your service architecture • Non-inline deployment and zero impacts on your website services • High reliability. If your WAF instance becomes faulty, the load balancer directly distributes your website traffic over the origin servers, eliminating adverse impact incurred such on your normal business.	• 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 describes the service specifications of each WAF mode. 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**.

NOTICE

In cloud mode, ELB access is supported in only standard, professional, and platinum editions. ELB-access WAF and cloud WAF have the same service specifications.

The restrictions and specifications of the expansion package are as follows:

- A domain package allows you to add 10 domain names to WAF, including one top-level domain and nine subdomains or wildcard domains related to the top-level domain.
- The QPS limit and bandwidth limit of a QPS expansion package:
  - For web applications deployed on Huawei Cloud

Service bandwidth: 50 Mbit/s

QPS: 1,000 (Each HTTP GET request is a query.)

- For web applications not deployed on Huawei Cloud

  Service bandwidth: 20 Mbit/s

  QPS: 1,000 (Each HTTP GET request is a query.)

NOTICE

- If you want to use the ELB access mode, make sure you are using standard, professional, or platinum cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule extension packages are shared between the ELB access and CNAME access modes.
- The bandwidth limit applies only to websites accessed in cloud mode. Websites accessed in ELB mode have no bandwidth limit but only QPS limit.

- A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

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.

Table 2-2 WAF editions and applicable service scales

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
Peak rate of normal service requests	• Service requests: 2,000 QPS • WAF-to-Server connections: 6,000 per domain name	• Service requests: 5,000 QPS • WAF-to-Server connections: 6,000 per domain name	• Service requests: 10,000 QPS • WAF-to-Server connections: 6,000 per domain name	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-to-server persistent connections: 60,000 • Specifications: WI-100. Referenced performance:

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
					– 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 – 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	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
Service bandwidth threshold (The origin server is deployed on the cloud.)	100 Mbit/s	200 Mbit/s	300 Mbit/s	N/A	• Specifications: WI-500. Performance: Throughput: 500 Mbit/s • Specifications: WI-100. Referenced performance: Throughput: 100 Mbit/s
Service bandwidth threshold (The origin server is not deployed on Huawei Cloud.)	30 Mbit/s	50 Mbit/s	100 Mbit/s	N/A	N/A
Number of domains	10 (Supports one top-level domain name.)	50 (Supports five top-level domain names.)	80 (Supports eight top-level domain names.)	30 (Supports three top-level domain names.)	2,000 (Supports 2,000 top-level domain names)
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

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
Quantity of supported ports **NOTE** If you are using a professional or platinum cloud WAF instance, you can configure any non-standard ports for your protected website. To do so, **submit a ticket** to enable customized non-standard ports.	• Standard ports: two (80 and 443) • Non-standard ports: You can use as many ports as you want as long as the port is supported by WAF. For details, see **Ports Supported by WAF**.	• Standard ports: two (80 and 443) • Non-standard ports: You can use as many ports as you want as long as the port is supported by WAF. For details, see **Ports Supported by WAF**.	• Standard ports: two (80 and 443) • Non-standard ports: You can use as many ports as you want as long as the port is supported by WAF. For details, see **Ports Supported by WAF**.	N/A	• Standard ports: two (80 and 443) • Non-standard ports: You can use as many ports as you want as long as the port is supported by WAF. For details, see **Ports Supported by WAF**.

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
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
Number of reference table rules	N/A	50	100	200	100
Number of IP address blacklist or whitelist rules	1,000	2,000	5,000	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	Professional	Platinum	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
Security report templates	5	10	20	-	20

Functions Supported by Each Edition

For details about cloud and dedicated WAF instances, see **Table 2-3**. The standard, professional, and platinum editions provide cloud WAF instances. You can upgrade the WAF edition you are using to a higher one to meet your changing requirements. For details, see **Changing Cloud WAF Edition and Specifications**.

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. For details about ELB load balancers, see **Differences Between Dedicated and Shared Load Balancers**.

Table 2-3 Security features

Function	Cloud - CNAME Access			Cloud - ELB Access	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
	Standard	Professional	Platinum			
Domain name, QPS, and rule expansion packages	√	√	√	√ (Quota shared with CNAME access)	×	×
Adding wildcard domain names	√	√	√	√	√	√
Protection for ports except 80 and 443	√	√	√	-	√	√
Customization of standard ports other than ports 80 and 443	×	√	√	-	×	×
Batch configuring defense policies	×	√	√	√	√	√
Batch adding domain names to a policy	×	√	√	√	√	√
Protection against common web 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	√	√	√	√	√	√

Function	Cloud - CNAME Access			Cloud - ELB Access	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
	Standard	Professional	Platinum			
Updating protection rules against zero-day vulnerabilities to the latest on the cloud and delivering virtual patches in a timely manner	√	√	√	√	√	×
Web shell detection	√	√	√	√	√	√
Deep anti-evasion inspection to 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	√	√	√	√	√	√
Inspection of all header fields in the requests	√	√	√	√	√	√
CC attack prevention	√	√	√	√	√	√
Precise protection	√ (excluding full detection)	√	√	√ (excluding full detection)	√ (excluding full detection)	√
Reference table management	×	√	√	√	√	√

Function	Cloud - CNAME Access			Cloud - ELB Access	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
	Standard	Professional	Platinum			
IP address whitelist and blacklist and batch importing of IP addresses/IP address ranges	√	√	√	√	√	√
Allowing or blocking web requests based on the countries that the requests originate from.	×	√	√	√	√	√
Web page tampering protection	√	√	√	√	√	√
Identification and blocking of crawler behavior such as search engines, scanners, script tools, and other crawlers	×	√	√	√	√	√
JavaScript-based anti-crawler protection	×	√	√	×	×	√
Information leakage prevention	×	√	√	√	√	√
Global Protection Whitelist Rule	√	√	√	√	√	√
Data masking	√	√	√	√	√	√

Function	Cloud - CNAME Access			Cloud - ELB Access	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
	Standard	Professional	Platinum			
Resource requirement suggestions	N/A	N/A	N/A	N/A	N/A	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%.

Function	Cloud - CNAME Access			Cloud - ELB Access	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
	Standard	Professional	Platinum			
						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 perform pressure

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

A powerful crawler feature library is used to detect varied types of crawlers, such as engine crawlers, script crawlers, and scanning tools.

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)	When adding a website to WAF, you can select **Cloud - CNAME**, **Cloud - Load balancer**, or **Dedicated** for **Protection**. Before you start, get familiar with the following differences: • **Cloud - CNAME**: protects your web applications that have domain name and are deployed on any clouds or in on-premises data centers. • **Cloud - Load balancer**: protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses. • **Dedicated**: protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses.
	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	PCI DSS/PCI 3DS compliance certification and TLS checks	• TLS has three versions (TLS v1.0, TLS v1.1, and TLS v1.2) and seven cipher suites. You can select the one best fits your business needs. • WAF supports PCI DSS and PCI 3DS compliance certification check.

Function		Description
	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.
	Break Protection	When the 502/504 error requests and pending URL requests reach the thresholds you configure, WAF enables corresponding protection for your website.
	Traffic identifier for a known attack source	WAF allows you to configure traffic identifiers by IP address, session, or user tag to block possibly malicious requests from known attack sources based on **IP address**, **Cookie**, or **Params**.
	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. • You can use Log Tank Service (LTS) on Huawei Cloud to record all WAF logs, including attack and access logs.

Function	Description
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.
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

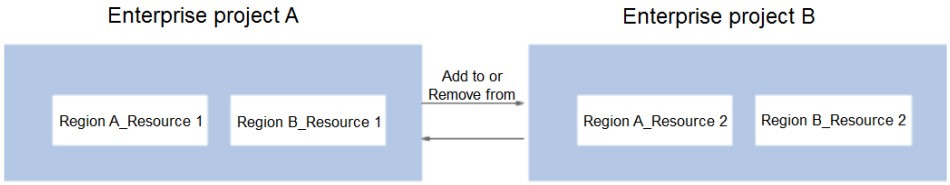
- IAM Project

  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.

For details about how to create a project, create an enterprise project, and grant policies, see **Project and 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 Security

9.1 Shared Responsibilities

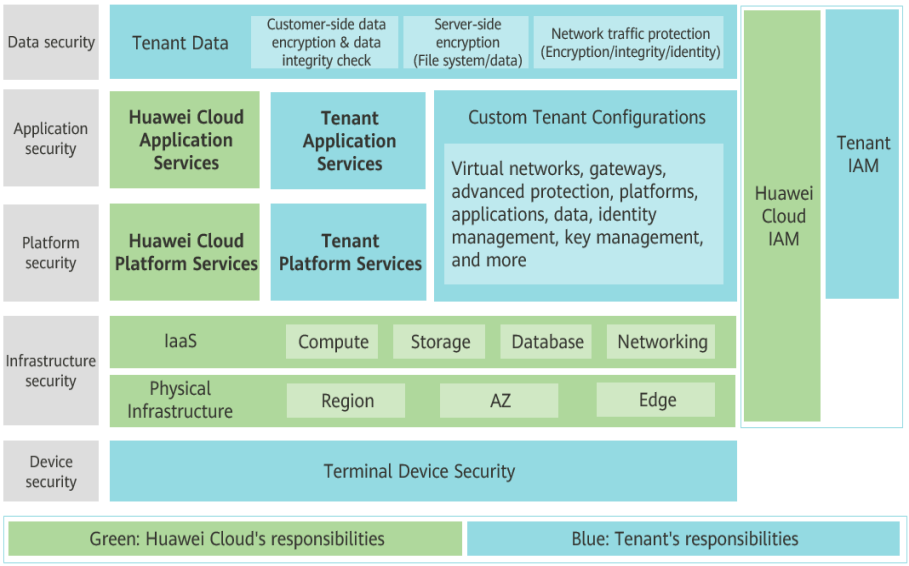
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 9-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 9-1 Huawei Cloud shared security responsibility model



9.2 Identity Authentication and Access Control

WAF works with Identity and Access Management (IAM). WAF authenticates user identities and controls access to WAF through IAM.

Identity and Access Management (IAM) is a basic service of Huawei Cloud that provides permissions management to help you securely control access to the WAF service. With IAM, you can add users to a user group and configure policies to control their access to WAF resources. You can allow or deny access to a specific WAF resource in a fine-grained manner. For details about access permissions for WAF resources, see **WAF Permission Management**.

9.3 Data Protection Controls

WAF takes different controls to keep data in WAF secure and reliable.

Table 9-1 Data protection controls and features

Measure	Description
Protection for data at rest	WAF encrypts sensitive data in your website traffic to keep the data from leakage.
Protection for data in transit	Data is encrypted when it is transmitted between microservices to prevent leakage or tampering during transmission. WAF keeps your configuration data secure as the configuration data is transmitted over HTTPS.

Measure	Description
Data integrity verification	When the WAF process is started, the configuration data is obtained from the configuration center instead of directly reading local files.
Data isolation mechanism	WAF isolates its tenant zone from its management plane. Operation permissions for WAF are isolated by user. Your policies and logs are isolated from those of others.
Data destruction mechanism	To prevent information leakage caused by residual data, Huawei Cloud sets different retention periods based on the customer level. If the customer does not renew the subscription or recharge the account after the retention period expires, the data stored in the cloud service will be deleted and the cloud service resources will be released. WAF automatically detects cloud service subscription status and releases resources when the retention period expires.

Beyond that, WAF protects your website while making every effort to protect your privacy in accordance with applicable laws and regulations. Take intrusion prevention as an example. WAF detects traffic that matches threat signature library and scans for abnormal behavior only. WAF never collects or stores any user privacy data. For more privacy data usage and protection issues, see **Privacy Statement**.

9.4 Audit and Logging

- Audit

  Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

  After you enable CTS and configure a tracker, CTS can record management and data traces of WAF for auditing.

  For details about how to enable and configure CTS, see **What Is Cloud Trace Service?**

  For details about WAF operations that can be recorded by CTS, see **WAF Operations Recorded by CTS**.

- Logging

  After you enable CTS, the system starts recording operations on WAF. You can view the operation records of the last 7 days on the CTS console.

  For details, see **Viewing an Audit Trace**.

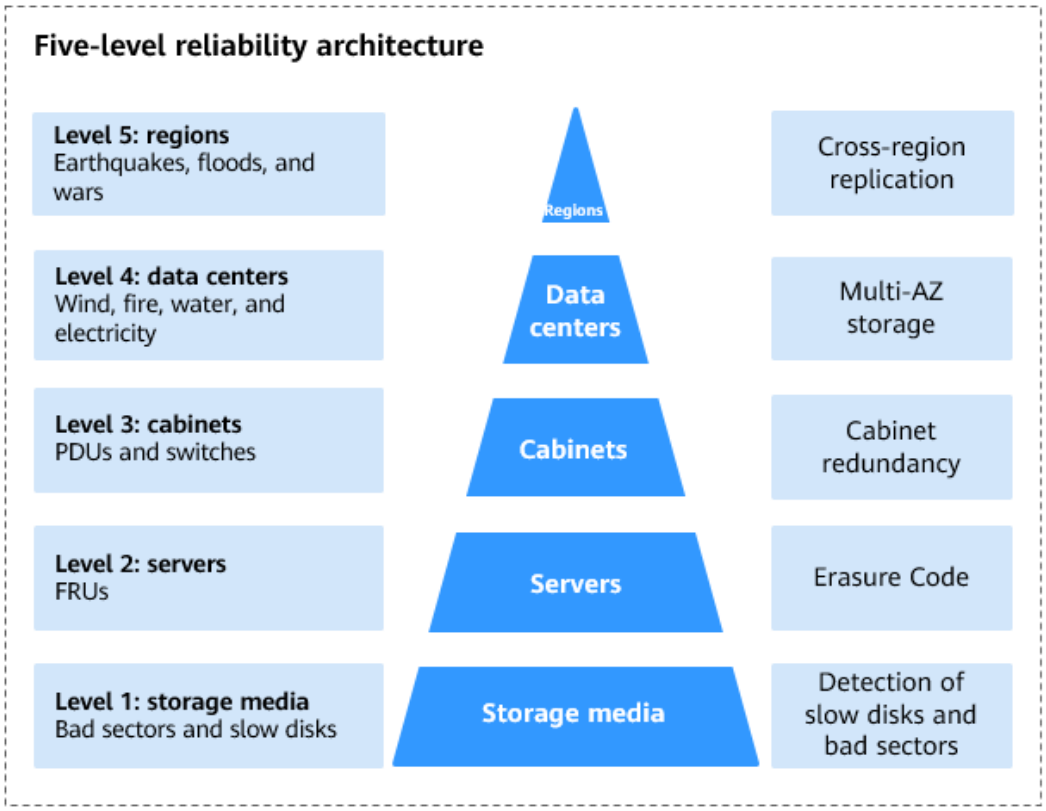
9.5 Service Resilience

Huawei Cloud WAF is deployed in data centers that are active around the world. Data centers in two cities are deployed as disaster recovery center for each other.

If a data center in city A is down, the data center in city B automatically takes over the job and serves your applications and data in compliance with the regulations to ensure service continuity. To minimize the service interruptions caused by hardware failures, natural disasters, or other disastrous events, Huawei Cloud WAF provides a DR plan:

If a fault occurs, the five-level reliability architecture of WAF supports different levels of reliability. Therefore, WAF has high availability, fault tolerance, and scalability.

Huawei Cloud WAF is available worldwide and is deployed in multiple AZs. With management planes, engines, and other components of WAF deployed in active/standby or cluster mode, WAF itself is stable enough.



9.6 Risk Monitoring

WAF has been interconnected with Cloud Eye. You can view WAF metrics on Cloud Eye to learn about the WAF protection status in a timely manner and set protection policies based on the metrics. Cloud Eye is a multi-dimensional monitoring platform provided by Huawei Cloud for a wide range of cloud resources. With Cloud Eye, you can learn about the resource usage and service running status on the cloud, receive alarms in a timely manner, and respond quickly to exceptions to keep your cloud services stable.

You can set WAF alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the WAF protection status in a timely manner.

For details about how to use Cloud Eye to monitor WAF, see:

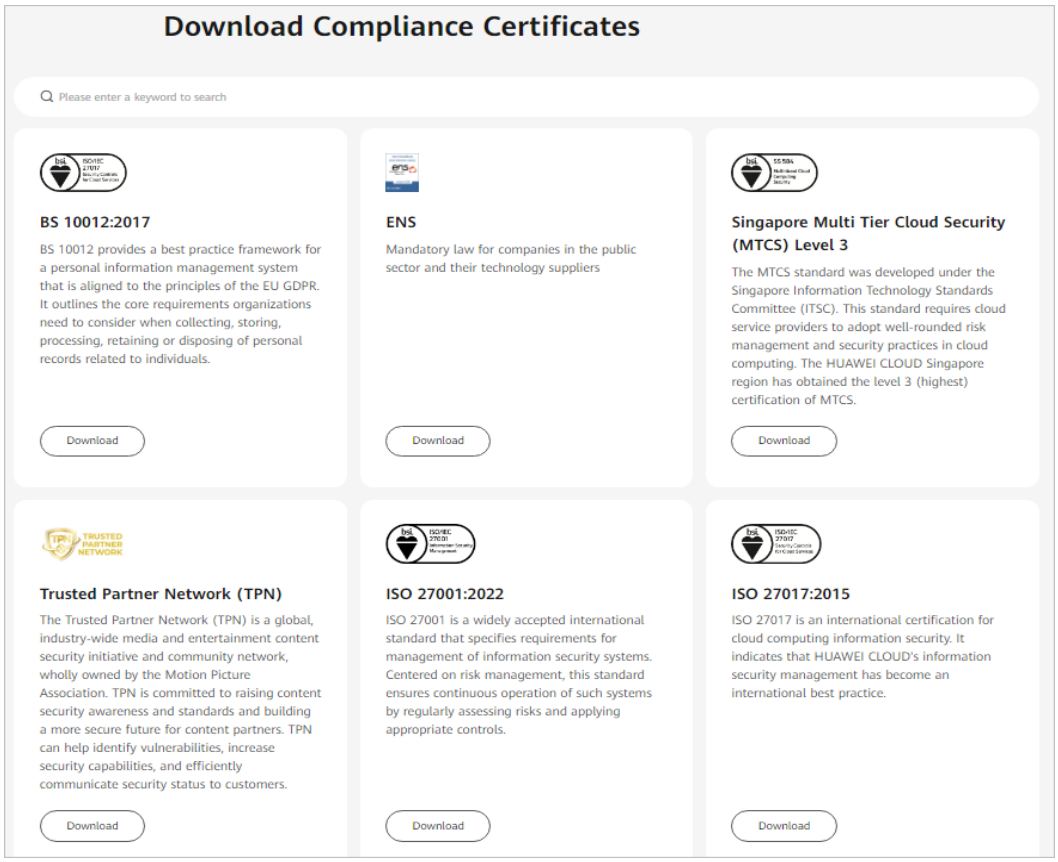
- **WAF Monitored Metrics**
- **Configuring Alarm Monitoring Rules**
- **Viewing Monitored Metrics**

9.7 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

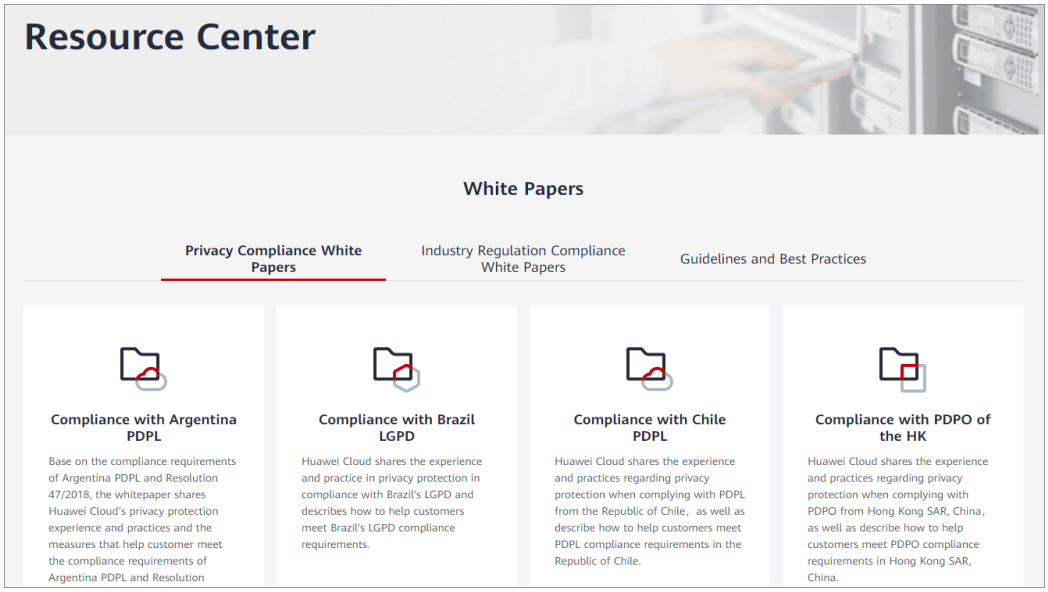
Figure 9-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 9-3 Resource center



10 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 10-1 lists all the system roles supported by WAF.

Table 10-1 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	

Helpful Links

- **IAM Service Overview**
- **Creating a User Group and User and Granting WAF Permissions**
- **WAF Custom Policies**
- **WAF Permissions and Supported Actions**

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"
      }
   ]
}
```


11 Limitations and Constraints

This topic describes the restrictions on using WAF.

Restrictions on Purchasing WAF Specifications

- Only one WAF edition can be selected under an account in the same great region such as CN East, including CN East-Shanghai1 and CN East-Shanghai2 regions.

  NOTE

  For details about supported regions, see **In Which Regions Is WAF Available?**

  Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster, select the region nearest to your services.

- If dedicated WAF instances and origin servers they protect are not in the same VPC, you can use a **VPC peering connection** to connect two VPCs. This method is not recommended as VPC peering connections may be not stable enough sometimes.
- If you want to use the ELB access mode, make sure you are using standard, professional, or platinum cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule extension packages are shared between the ELB access and CNAME access modes.
- Expansion Package Specifications:
  - A domain package allows you to add 10 domain names to WAF, including one top-level domain and nine subdomains or wildcard domains related to the top-level domain.
  - The QPS limit and bandwidth limit of a QPS expansion package:
    - For web applications deployed on Huawei Cloud

      Service bandwidth: 50 Mbit/s

      QPS: 1,000 (Each HTTP GET request is a query.)
    - For web applications not deployed on Huawei Cloud

      Service bandwidth: 20 Mbit/s

      QPS: 1,000 (Each HTTP GET request is a query.)

NOTICE

- If you want to use the ELB access mode, make sure you are using standard, professional, or platinum cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule extension packages are shared between the ELB access and CNAME access modes.
- The bandwidth limit applies only to websites accessed in cloud mode. Websites accessed in ELB mode have no bandwidth limit but only QPS limit.

  - A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

- For details, see **WAF Edition Differences**.

Website Connection Restrictions

- Access mode restrictions:
  - In cloud CNAME access mode, only domain names can be added to WAF. In dedicated mode and cloud ELB access mode, you can add domain names or IP addresses WAF, but these two modes require origin servers to be deployed on Huawei Cloud.
  - In cloud mode, only the professional and platinum editions support IPv6 protection, HTTP/2, and load balancing algorithms.
  - In cloud mode, if you are using WAF standard edition, only **System-generated policy** can be selected for **Policy**.
- Domain name restrictions:
  - You can enter a multi-level single domain name (for example, top-level domain name example.com and level-2 domain name www.example.com) or a wildcard domain name (*.example.com).

    NOTICE

    The wildcard domain name ***** can be added to WAF. When the domain name is set to *****, only non-standard ports except 80 and 443 can be protected.

    The following are the rules for adding wildcards to domain names:

    - If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can add the wildcard domain name ****.example.com*** to WAF to protect all three.
    - If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.

  - A protected domain name can only be added to WAF once.

    Each combination of a domain name and a non-standard port is counted towards the domain name quota of the WAF edition you are using. For

example, www.example.com:8080 and www.example.com:8081 use two domain names of the quota. If you want to protect web services over multiple ports with the same domain name, add the domain name and each port to WAF.

  - If a domain name is added to WAF in cloud CNAME access mode, make sure the domain name has been registered with an ICP license. WAF will check the domain name ICP license. Domain names that are not licensed cannot be added to WAF.
- ELB load balancer restrictions:
  - If you want to use dedicated WAF, a dedicated Elastic Load Balance (ELB) load balancer should be used to distribute workloads for the website. For details about load balancer types, see **Differences Between Dedicated and Shared Load Balancers**.

    NOTE

    Dedicated WAF instances issued before April 2023 cannot be used with dedicated network load balancers. If you use a dedicated network load balancer (TCP/UDP), ensure that your dedicated WAF instance has been upgraded to the latest version (issued after April 2023).
  - In cloud ELB access mode, only dedicated load balancers with **Specifications** set to **Application load balancing (HTTP/HTTPS)** can be used.
- Certificate restrictions:
  - Only .pem certificates can be used in WAF.
  - Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used.
  - Only accounts with the **SCM Administrator** and **SCM FullAccess** permissions can select SCM certificates.
- Specification restrictions:

  After your website is connected to WAF, you can upload a file no larger than 10 GB each time.

Security Report Usage Restrictions

- WAF offers a quota for creating report templates.
  - Cloud mode - professional edition: 10
  - Cloud mode - platinum or dedicated edition: 20
  - Cloud mode - standard edition: 5
- WAF stores security reports for six months only. You are advised to regularly download reports to meet compliance and audit requirements.

Restrictions on Using Protection Logs

- On the WAF console, you can view the event data for all protected domain names over the last 30 days. You can enable LTS for long-term log storage and quick queries of details about attack logs and access logs.
- Only attack events blocked or recorded by built-in basic web protection rules and features in anti-crawler protection can be handled as false alarms.

- Only event data for the last five days can be downloaded through the WAF console.

Protection Policy Restrictions

- A protected website domain name can use only one policy.
- For details about the differences between rules supported by different editions, see **Specifications Supported by Each Edition** and **Edition Differences**.

12 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 understand 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.

A Change History

Released On	Description
2024-06-05	This issue is the eighty-third official release. Added the following content: • **Limitations and Constraints**
2024-04-10	This issue is the eighty-second official release. Modified the following content: • **Functions**
2024-01-31	This issue is the eighty-first official release. Modified the following content: • **What Is WAF?** • **Edition Differences**
2023-11-10	This issue is the eightieth official release. **Edition Differences**: Modified some descriptions.
2023-10-23	This issue is the seventy-ninth official release. • Modified the following content: **Functions**
2023-07-26	This issue is the seventy-eighth official release. **CTS**: Modified some descriptions.
2023-06-30	This issue is the seventy-seventh official release. **Edition Differences**: Modified some descriptions.
2023-06-21	This issue is the seventy-sixth official release. **Edition Differences**: Added resource requirement suggestions.

Released On	Description
2023-06-01	This issue is the seventy-fifth official release. Modified the following content: • **Edition Differences** • **Functions**
2023-05-09	This issue is the seventy-fourth official release. Modified the following content: • **Functions** • **Application Scenarios** • **Edition Differences**
2023-03-25	This issue is the seventy-third official release. **Edition Differences**: Modified some descriptions.
2023-03-03	This issue is the seventy-second official release. Modified the following content: • **Edition Differences** • **Functions**
2023-02-08	This issue is the seventy-first official release. Modified the following content: • **Edition Differences** • Billing Description
2022-11-16	This issue is the seventieth official release. **Edition Differences**: Added the description of certificates.
2022-11-09	This issue is the sixty-ninth official release. Added **Security**.
2022-11-04	This issue is the sixty-eighth official release. Modified the following content: • **Edition Differences** • Billing Description
2022-10-25	This issue is the sixty-seventh official release. **What Is WAF?**: Modified some descriptions.
2022-10-10	This issue is the sixty-sixth official release. Modified section "Billing Description".
2022-09-07	This issue is the sixty-fifth official release. Modified the following content: • **Edition Differences** • **Functions**

Released On	Description
2022-08-03	This issue is the sixty-fourth official release. Modified the following content and deleted the description of enabling the dedicated mode by submitting a service ticket: • **Edition Differences** • Billing Description
2022-07-04	This issue is the sixty-third official release. Modified the following content as the global protection whitelist function is provided: • **Functions** • **Edition Differences** • **WAF Permissions Management** • **WAF and Other Services**
2022-06-22	This issue is the sixty-second official release. Modified **Edition Differences**.
2022-06-09	This issue is the sixty-first official release. Modified **Functions**: Added the website connection timeout settings and connection protection.
2022-05-30	This issue is the sixtieth official release. Modified **Functions**: Resorted the non-standard ports.
2022-05-26	This issue is the fifty-ninth official release. Modified the following content: • **Edition Differences** • Billing Description • **Functions**
2022-05-12	This issue is the fifty-eighth official release. Modified the following content: • **Edition Differences** • Billing Description • **Product Advantages**
2022-05-07	This issue is the fifty-seventh official release. Modified **Personal Data Protection Mechanism**.
2022-03-07	This issue is the fifty-sixth official release. Modified the following content as dedicated WAF instances are provided: • **Edition Differences** • Billing Description

Released On	Description
2022-02-10	This issue is the fifty-fifth official release. Optimized descriptions in **Edition Differences**.
2022-01-21	This issue is the fifty-fourth official release. Optimized descriptions in **Edition Differences**.
2021-12-30	This issue is the fifty-third official release. Added content related to Cloud Eye in **WAF and Other Services**.
2021-12-10	This issue is the fifty-second official release. Modified descriptions of specifications in **Edition Differences**.
2021-11-08	This issue is the fifty-first official release. Modified descriptions of specifications in **Edition Differences**.
2021-11-04	This issue is the fiftieth official release. Modified descriptions of specifications in **Edition Differences**.
2021-10-12	This issue is the forty-ninth official release. Optimized part of descriptions in **Functions**.
2021-09-23	This issue is the forty-eighth official release. Optimized descriptions of policies in **WAF Permissions Management**.
2021-09-17	This issue is the forty-seventh official release. Optimized part of descriptions in **Edition Differences**.
2021-08-12	This issue is the forty-sixth official release. Optimized part of descriptions in **Edition Differences**.
2021-08-06	This issue is the forty-fifth official release. Renamed WAF editions: Rename professional edition standard edition, enterprise edition professional edition, and premium edition platinum edition.
2021-08-02	This issue is the forty-fourth official release. Optimized part of descriptions in **Functions**.
2021-07-06	This issue is the forty-third official release. Optimized part of descriptions in **What Is WAF?**.
2021-06-16	This issue is the forty-second official release. Optimized part of descriptions in **Edition Differences**.

Released On	Description
2021-05-27	This issue is the forty-first official release. Optimized part of descriptions in **Edition Differences**.
2021-05-24	This issue is the fortieth official release. Added the description of new features in **Functions**.
2021-05-18	This issue is the thirty-ninth official release. Added the description of protection objects in **What Is WAF?**
2021-04-30	This issue is the thirty-eighth official release. Billing Description: Added the billing description of the QPS expansion package.
2021-04-07	This issue is the thirty-seventh official release. Added the description of security features in **Edition Differences**.
2021-03-02	This issue is the thirty-sixth official release. Modified the deployment architecture diagram. For details, see **Edition Differences**.
2021-02-25	This issue is the thirty-fifth official release. • Added **Project and Enterprise Project**. • Added the description of the Enterprise Management service in **WAF and Other Services**.
2021-02-23	This issue is the thirty-fourth official release. Modified the description in **Edition Differences**.
2021-02-05	This issue is the thirty-third official release. Billing Description: Added description about the pay-per-use billing mode.
2021-01-25	This issue is the thirty-second official release. Optimized part of descriptions in **Edition Differences**.
2020-12-31	This issue is the thirty-first official release. Optimized part of descriptions in **Functions**.
2020-12-25	This issue is the thirtieth official release. Optimized some descriptions.
2020-12-11	This issue is the twenty-ninth official release. Deleted the description of the pay-per-use billing mode for the cloud mode.
2020-10-22	This issue is the twenty-eighth official release. Modified specifications of pay-per-use WAF instances in **Edition Differences**.

Released On	Description
2020-09-23	This issue is the twenty-seventh official release. Optimized part of descriptions in **WAF and Other Services**.
2020-09-11	This issue is the twenty-sixth official release. • Added the description of ports supported by cloud instances billed on a pay-per-use basis in **Functions**. • Billing Description: Added the description of the pay-per-use billing mode for cloud instances.
2020-07-31	This issue is the twenty-fifth official release. Billing Description: Optimized some descriptions.
2020-07-08	This issue is the twenty-fourth official release. • Optimized part of descriptions in **Edition Differences**. • Billing Description: Optimized some descriptions.
2020-06-24	This issue is the twenty-third official release. Optimized part of descriptions in **Edition Differences**.
2020-06-22	This issue is the twenty-second official release. Added descriptions of fine-grained policy in **WAF Permissions Management**.
2020-06-16	This issue is the twenty-first official release. Optimized the domain name description in **Edition Differences**.
2020-06-11	This issue is the twentieth official release. Optimized part of descriptions in **Edition Differences**.
2020-05-26	This issue is the nineteenth official release. Added descriptions in **Functions** and **Edition Differences**.
2020-05-19	This issue is the eighteenth official release. Added section "Billing Description".
2020-03-19	This issue is the seventeenth official release. Modified supported non-standard ports in for **Functions**.
2020-01-20	This issue is the sixteenth official release. Optimized part of descriptions in **WAF Permissions Management**.
2019-12-26	This issue is the fifteenth official release. Optimized part of descriptions in **Functions**.
2019-12-09	This issue is the fourteenth official release. • Optimized part of descriptions in **Edition Differences**. • Optimized part of descriptions in **Functions**.

Released On	Description
2019-11-28	This issue is the thirteenth official release. • Optimized part of descriptions in **Functions**. • Optimized part of descriptions in **Edition Differences**.
2019-10-25	This issue is the twelfth official release. Added **Personal Data Protection Mechanism**.
2019-10-14	This issue is the eleventh official release. • Optimized part of descriptions in **What Is WAF?**. • Optimized part of descriptions in **Functions**. • Optimized part of descriptions in **Edition Differences**. • Optimized part of descriptions in **Application Scenarios**.
2019-05-16	This issue is the tenth official release. Optimized part of descriptions in **Functions**.
2019-05-14	This issue is the ninth official release. • Added **Functions**. • Optimized part of descriptions in **What Is WAF?**. • Optimized part of descriptions in **WAF and Other Services**.
2018-11-08	This issue is the eighth official release. Optimized some descriptions.
2018-10-29	This issue is the seventh official release. Optimized part of descriptions in **What Is WAF?**.
2018-04-26	This issue is the sixth official release. Added **WAF Permissions Management**.
2018-04-12	This issue is the fifth official release. Added content about sensitive data leakage protection in **What Is WAF?**
2018-04-02	This issue is the fourth official release. Optimized part of descriptions in **What Is WAF?**.
2018-03-27	This issue is the third official release. • Added function description in **What Is WAF?** • Deleted section "Concepts."
2018-01-11	This issue is the second official release. Added the description about WAF and CTS in **WAF and Other Services**.
2017-10-30	This issue is the first official release.