Web Application Firewall

Service Overview

Issue	85
Date	2025-01-17

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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.

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).

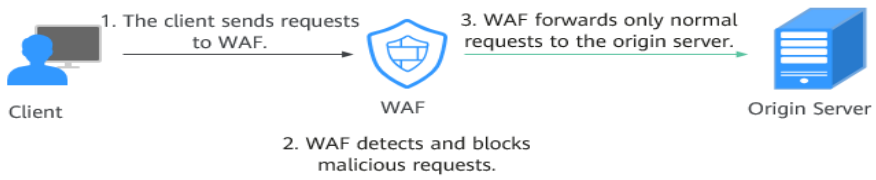
How WAF Works (Cloud Mode - CNAME Access Mode and Dedicated Mode)

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.

NOTE

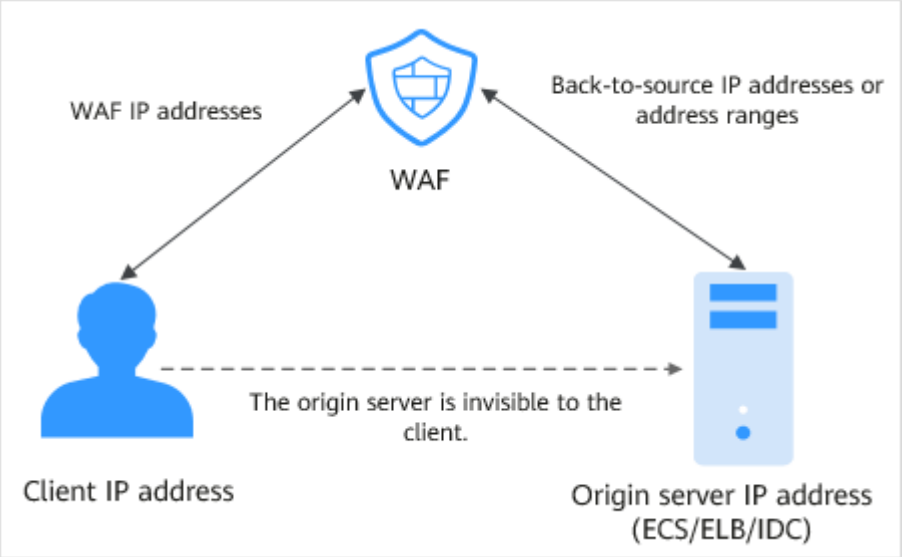
Dedicated WAF instances are not available in some regions. For details, see **Notice on Web Application Firewall (Dedicated Mode) Discontinued**.

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

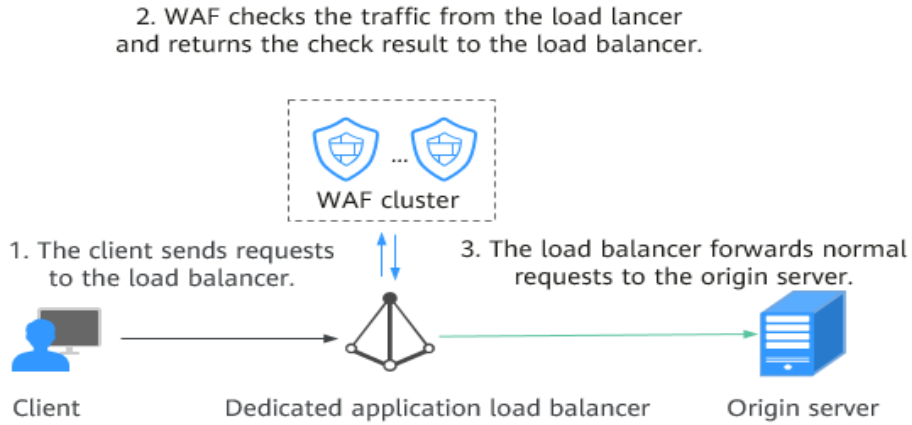


How WAF Works (Cloud Mode - Load Balancer Access)

If you connect a website to WAF in cloud load balancer access mode, WAF works as follows:

- In this mode, 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 load balancer access mode works



What WAF Protects

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

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

2 Edition Differences

WAF provides cloud and dedicated instances. The access mode varies depending on the instance type you are using. This topic summaries comparisons on access modes, service specifications, and functions between different editions, so you can quickly know which type of instance best fits your service requirements.

Service Edition Overview

When you make a purchase decision, consider the access mode, specifications, and functions the WAF edition you plan to use supports.

- **Access modes**

  You can connect a website to WAF in **cloud mode** or **dedicated mode**. In cloud mode, **Cloud Mode - CNAME** and **Cloud Mode - Load balancer** access modes are supported. For more details, see **Access Mode Description**.

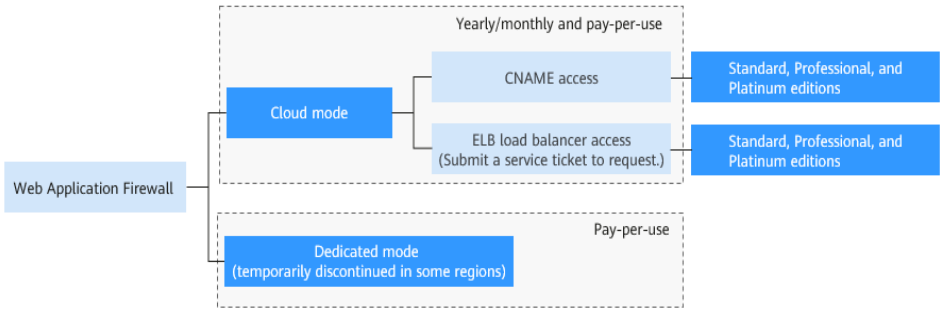
- **Service editions**

  To support different service scenarios, WAF provides multiple editions. For details about the specifications of different editions, see **Specifications Supported by Each Edition**. For details about the supported functions and features, see **Functions Supported by Each Service Edition**.

  - **For cloud mode**, WAF can be billed on a **yearly/monthly** or **pay-per-use** basis. In yearly/monthly billing mode, you can use the **standard**, **professional**, or **platinum** edition. For details about the different access modes and service editions, see **Figure 2-1**.

    In cloud mode, you can change the billing mode between yearly/monthly and pay-per-use. For more details, see **Changing the Billing Mode**.
  - **For dedicated mode**, WAF can be billed only in **pay-per-use** mode.

Figure 2-1 Service editions and access modes



NOTE

- To use **cloud mode - load balancer** access mode, you need to purchase the standard, professional, or platinum edition billed on a yearly/monthly basis first. Then you can **submit a service ticket** to request for the use of this mode. For details about regions supported by **Cloud Mode - Load Balancer Access**, see **Function Overview**.
- Dedicated WAF instances are not available in some regions. For details, see **Notice on Web Application Firewall (Dedicated Mode) Discontinued**. There is no impact on your use or renewal of dedicated WAF instances you already purchased.

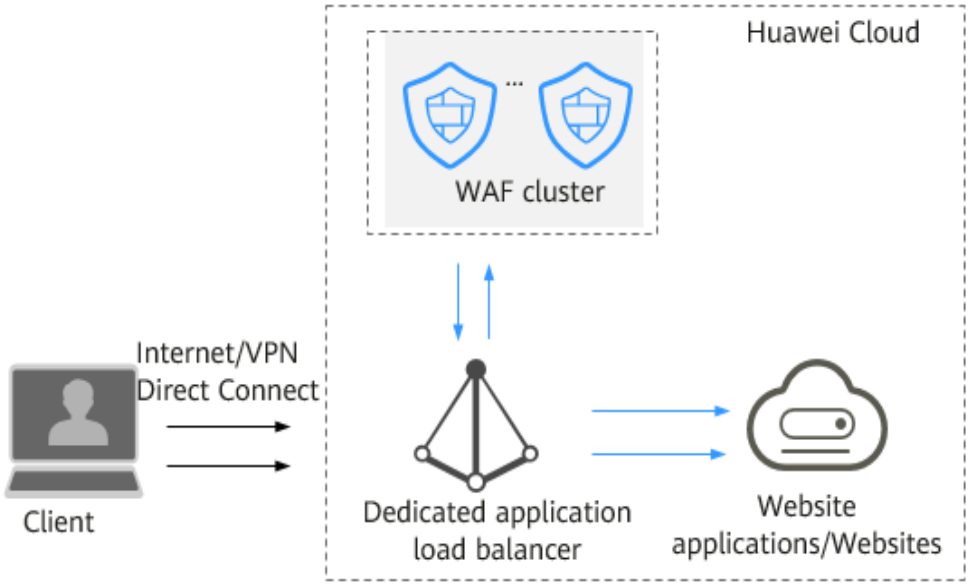
Access Mode Description

The service edition you can use is restricted by the access mode you want to use. So, before making a purchase, check which WAF access mode best fits your need.

WAF provides three access modes: **cloud mode - CNAME**, **cloud mode - load balancer**, and **dedicated mode**. The following figure shows the deployment architecture. For details about the differences, see **Table 2-1**.

Cloud Mode - CNAME Access

Cloud Mode - Load Balancer Access



Dedicated Mode

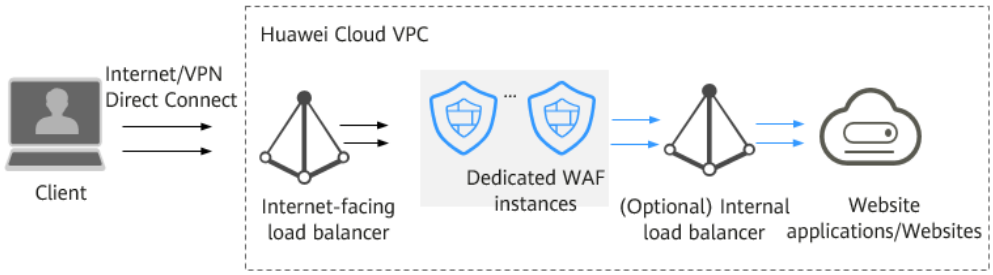


Table 2-1 Access Mode Description

Item	Cloud Mode - CNAME Access	Cloud Mode - Load Balancer Access	Dedicated Mode
Application scenarios	Suitable for service scenarios of various scales. For details about service scales and cloud mode editions, see **Service Editions**.	This mode is suitable for large enterprise websites having high security requirements on service stability.	This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements.
Where web services are deployed	Service servers are deployed on any cloud or in on-premises data centers.	Service servers are deployed on Huawei Cloud.	Service servers are deployed on Huawei Cloud.

Item	Cloud Mode - CNAME Access	Cloud Mode - Load Balancer Access	Dedicated Mode
Protected objects	Domain names	Domain names and IP addresses (public or private IP addresses)	Domain names and IP addresses (public or private IP addresses)
Billing mode	Yearly/Monthly and pay-per-use billing	Yearly/Monthly and pay-per-use billing	Pay-per-use billing
Service editions	Standard, professional, and platinum editions	Standard, professional, and platinum editions	-
Advantages	• Protection capability scaling by upgrading specifications • Protection for cloud and on-premises web services • IPv6 protection	• 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.
Access Guide	**Connecting Your Website to WAF (Cloud Mode - CNAME Access)**	**Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**	**Connect Your website to WAF (Dedicated Mode)**

Specifications Supported by Each Edition

After selecting an access mode, you need to select a proper service edition based on your service scale. **Table 2-2** lists the service specifications supported by different service editions.

NOTE

- In cloud mode, the domain name, QPS, and rule expansion package quotas can be shared by the load balancer and CNAME access modes. This is because the same service specifications are provided for the two modes.
- 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**. Service edition rankings are as follows: **standard**, **professional**, and **platinum**, in ascending order.

Table 2-2 Applicable service scales

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
Service scale	This edition is suitable for small and medium-sized websites that do not have special security requirements.	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.	This edition is suitable for large and medium-sized enterprise websites that have a large service scale or have customized security requirements.	The mode is recommended if you expect frequent service usage changes.	This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements.

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
Peak rate of normal service requests	• Service requests: 2,000 QPS • Support for **QPS expansion packages** – Origin servers deployed on Huawei Cloud: Each expansion package supports 1,000 QPS and 50 Mbit/s bandwidth. – Origin servers not deployed on Huawei Cloud: Each expansion package supports	• Service requests: 5,000 QPS • Support for **QPS expansion packages** – Origin servers deployed on Huawei Cloud: Each expansion package supports 1,000 QPS and 50 Mbit/s bandwidth. – Origin servers not deployed on Huawei Cloud: Each expansion package supports 1,000 QPS	• Service requests: 10,000 QPS • Support for **QPS expansion packages** – Origin servers deployed on Huawei Cloud: Each expansion package supports 1,000 QPS and 50 Mbit/s bandwidth. – Origin servers not deployed on Huawei Cloud: Each expansion package supports 1,000	WAF-to-Server connections: 6,000 per domain name	The following lists the specifications of a single instance. • Specifications: WI-500. Estimated performance: – HTTP services: 5,000 QPS (recommended) – HTTPS services: 4,000 QPS (recommended) – WebSocket service - Maximum concurrent connections: 5,000 – Maximum WAF-to-server persistent connections: 60,000 • Specifications: WI-100.

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
	1,000 QPS and 20 Mbit/s bandwidth. • WAF-to-Server connections: 6,000 per domain name	and 20 Mbit/s bandwidth. • WAF-to-Server connections: 6,000 per domain name	QPS and 20 Mbit/s bandwidth. • WAF-to-Server connections: 6,000 per domain name		Estimated performance: – HTTP services: 1,000 QPS (recommended) – HTTPS services: 800 QPS (recommended) – WebSocket service - Maximum concurrent connections: 1,000 – Maximum WAF-to-server persistent connections: 60,000

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
					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 bandwidth threshold (origin servers deployed on Huawei Cloud)	• 100 Mbit/s • Support for **QPS expansion packages**. (Each package supports 1,000 QPS and 50 Mbit/s bandwidth.)	• 200 Mbit/s • Support for **QPS expansion packages**. (Each package supports 1,000 QPS and 50 Mbit/s bandwidth.)	• 300 Mbit/s • Support for **QPS expansion packages**. (Each package supports 1,000 QPS and 50 Mbit/s bandwidth.)	300Mbit/s	• Specifications: WI-500. Estimated performance: Throughput: 500 Mbit/s • Specifications: WI-100. Estimated performance: Throughput: 100 Mbit/s

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
Service bandwidth threshold (origin servers not deployed on Huawei Cloud)	• 30 Mbit/s • Support for **QPS expansion packages**. (Each package supports 1,000 QPS and 20 Mbit/s bandwidth.)	• 50 Mbit/s • Support for **QPS expansion packages**. (Each package supports 1,000 QPS and 20 Mbit/s bandwidth.)	• 100 Mbit/s • Support for **QPS expansion packages**. (Each package supports 1,000 QPS and 20 Mbit/s bandwidth.)	100Mbit/s	N/A
Number of domain names	• 10 • Support for **domain expansion packages**. (Each package supports 10 domain names.)	• 50 • Support for **domain expansion packages**. (Each package supports 10 domain names.)	• 80 • Support for **domain expansion packages**. (Each package supports 10 domain names.)	200	2,000

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
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	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
Quantity of supported ports	• Standard ports: two (80 and 443) • Non-standard ports: any ports listed in **Ports Supported by WAF**. The number of ports is not limited.	• Standard ports: two (80 and 443) • Non-standard ports – Any ports listed in **Ports Supported by WAF**. The number of ports is not limited. – To protect ports not listed in **Ports Supported by WAF**, **submit a service ticket** to enable it.	• Standard ports: two (80 and 443) • Non-standard ports – Any ports listed in **Ports Supported by WAF**. The number of ports is not limited. – To protect ports not listed in **Ports Supported by WAF**, **submit a service ticket** to enable it.	• Standard ports: two (80 and 443) • Non-standard ports: any ports listed in **Ports Supported by WAF**. The number of ports is	• Standard ports: two (80 and 443) • Non-standard ports: any ports listed in **Ports Supported by WAF**. The number of ports is not limited.

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
				not limited.	
Peak rate of CC attack protection	100,000 QPS	200,000 QPS	1,000,000 QPS	1,000,000QPS	• Specifications: WI-500. Estimated performance: Maximum QPS: 20,000 • Specifications: WI-100. Estimated performance: Maximum QPS: 4,000
CC attack protection rules	20	50	100	200	100
Precise protection rules	20	50	100	200	100
Number of reference table rules	-	50	100	200	100

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
IP address blacklist and whitelist rules	• 1,000 • Support for **rule expansion packages**. (Each expansion package supports 10 IP blacklist and whitelist protection rules.)	• 2,000 • Support for **rule expansion packages**. (Each expansion package supports 10 IP blacklist and whitelist protection rules.)	• 5,000 • Support for **rule expansion packages**. (Each expansion package supports 10 IP blacklist and whitelist protection rules.)	200	1,000
Number of geolocation access control rules	-	50	100	200	100
Web tamper protection rules	20	50	100	200	100
Website anti-crawler protection	-	50	100	200	100

Service Scale	Cloud Mode			Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
	Standard	Professional	Platinum		
Number of information leakage prevention rules	-	50	100	200	100
Global protection whitelist rules	1,000	1,000	1,000	2,000	1,000
Data masking rules	20	50	100	200	100
Security report templates	5	10	20	-	20

How to count protected domain names:

- The number of domain names 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).
- 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

After determining the access mode and service edition, you need to consider whether the security functions supported by the selected access mode and service edition meet your service requirements. 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. For details about ELB load balancers, see **Differences Between Dedicated and Shared Load Balancers**.

Table 2-3 Security features

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
Domain Expansion Package	A domain expansion package can protect a maximum of 10 domain names.	√	√	√	√	×	×

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
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.	√	√	√	√	√	√

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
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	You can **submit a service ticket** to apply for protection for non-standard ports except standard ports 80 and 443.	×	√	√	-	×	×
Batch configuring defense policies	You can flexibly configure protection policies for protected domain names in batches.	×	√	√	√	√	√

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
Applying a protection policy to a domain name	When adding a domain name, you can apply a protection policy to it. • **System-generated policy** (default): This option is unavailable if the number of added protection policies reaches the quota. • Custom protection policy: A policy you create based on your security requirements. For more details, see **Configuring a Protection Policy**.	x (**System-generated policy** supported only)	√	√	√	√	√
Batch adding domain names to a policy	Batch adding domain names to a policy	×	√	√	√	√	√

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
Common web application attack defense	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	√	√	√	√	√	√
Zero-day vulnerability protection	Updating protection rules against zero-day vulnerabilities to the latest on the cloud and delivering virtual patches in a timely manner	√	√	√	√	√	×
Webshell Detection	Protects web applications from web shells.	√	√	√	√	√	√

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
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.	√	√	√	√	√	√
Header Inspection	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)	√	√	√ (excluding full detection)	√ (excluding full detection)	√

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
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	Identification and blocking of crawler behavior such as search engines, scanners, script tools, and other crawlers.	×	√	√	√	√	√
	JavaScript-based anti-crawler protection	×	√	√	×	×	√

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
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.	√	√	√	√	√	√

Function	Function Description	Cloud Mode - CNAME Access			Cloud Mode - Load Balancer Access (Standard/ Professional/ Platinum Edition)	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode (Pay-per-Use)
		Standard	Professional	Platinum			
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	N/A	N/A	-	√

3 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 Mode - CNAME**, **Cloud Mode - Load balancer**, or **Dedicated Mode**. Before you start, get familiar with their differences: • **Cloud Mode - CNAME**: protects your web applications that have domain name and are deployed on any clouds or in on-premises data centers. • **Cloud Mode - Load balancer**: protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses (public or private IP addresses). • **Dedicated Mode**: protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses (public or private 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 nine cipher suites. You can select the one best fits your security 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.

4 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.

5 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.

6 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

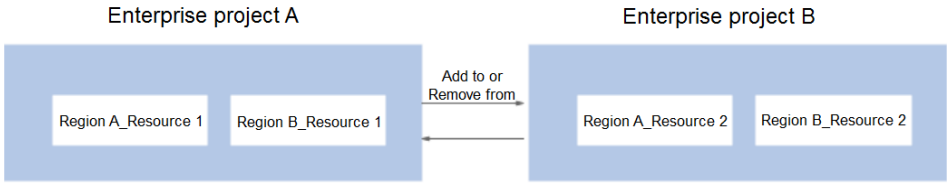
- IAM Project

  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**.

7 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 7-1** provides the personal data collected and generated by WAF.

Table 7-1 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.

8 Security

8.1 Shared Responsibilities

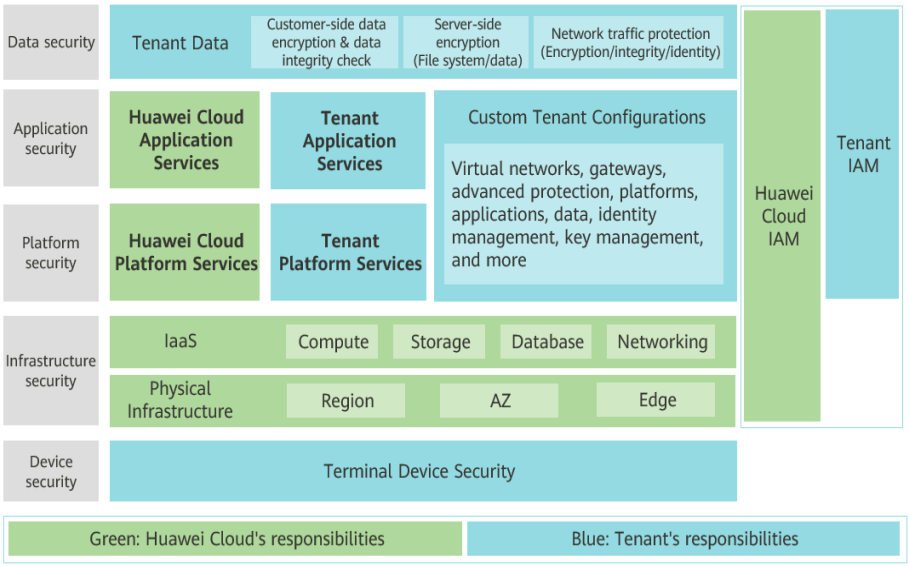
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 8-1 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 8-1 Huawei Cloud shared security responsibility model



8.2 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**.

8.3 Data Protection Controls

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

Table 8-1 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**.

8.4 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**.

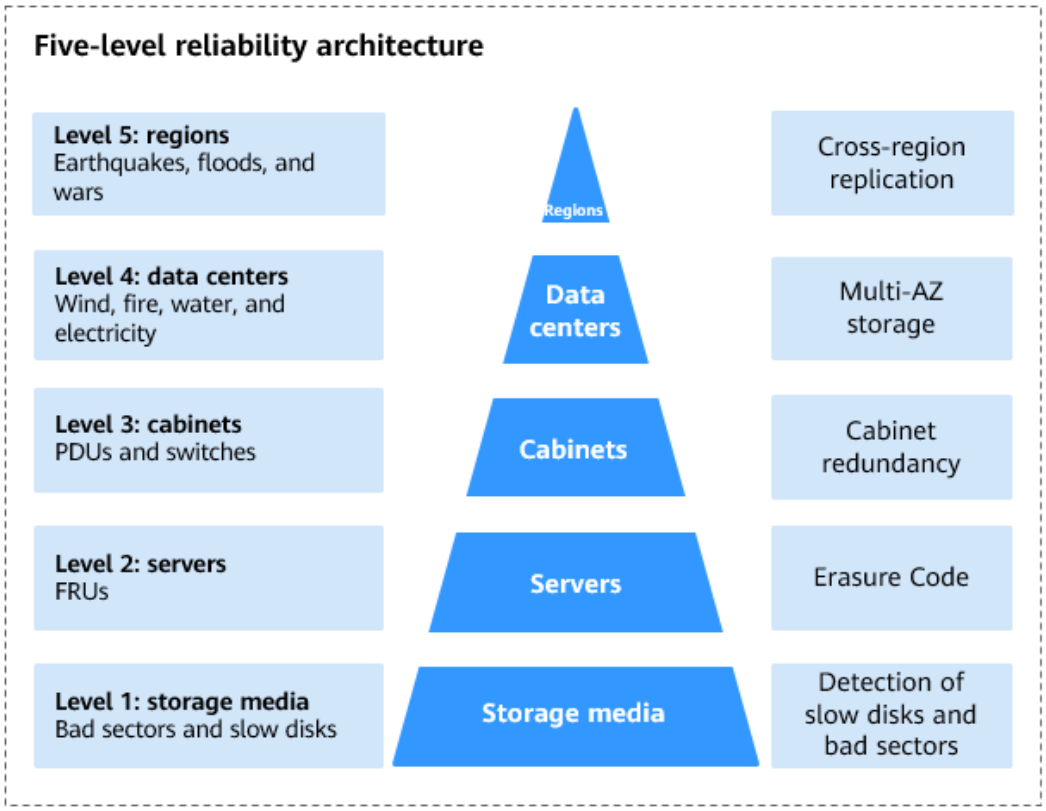
8.5 Service Resilience

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.



8.6 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:

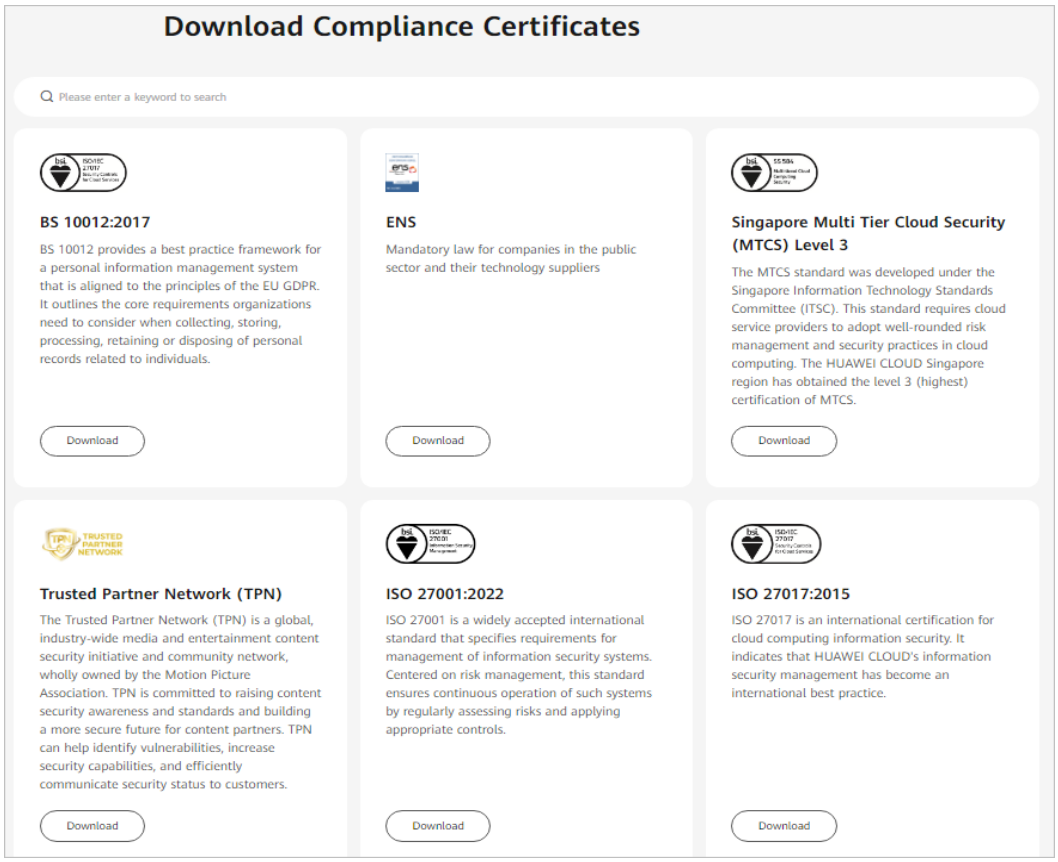
- **WAF Monitored Metrics**
- **Configuring Alarm Monitoring Rules**
- **Viewing Monitored Metrics**

8.7 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.

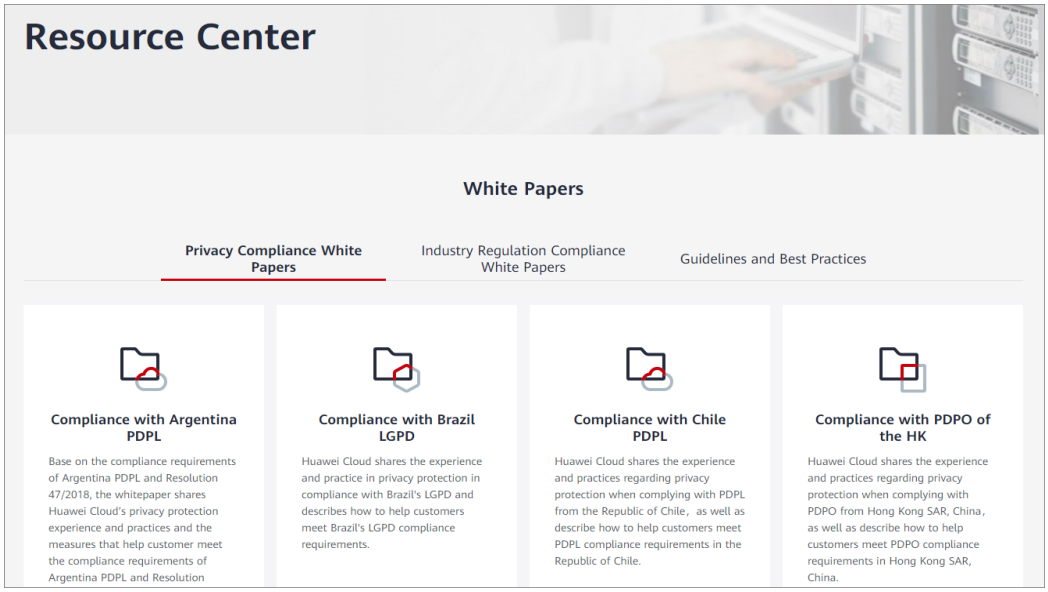
Figure 8-2 Downloading compliance certificates



Resource Center

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

Figure 8-3 Resource center



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 user 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	

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"
      }
   ]
}
```

10 Limitations and Constraints

This topic describes some limitations and constraints on using WAF.

Protection Object Limitations

Table 10-1 Protection object limitations

Access Mode	Protected Object
Cloud mode - CNAME access	• Domain names only • Protection for web services on Huawei Cloud, other clouds, and on-premises
Cloud mode - Load balancer	• Domain names • IP addresses • Protection for only web services on Huawei Cloud
Dedicated mode	• Domain names • IP addresses • Protection for only web services on Huawei Cloud

Service Edition Limitations

- Only one edition can be selected in a larger geographical region using the same account.

  For example, in the **CN East** region, only one WAF edition can be selected under an account in CN East-Shanghai1 and CN East-Shanghai2.

  NOTE

  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.

- Service edition selection:
  - You can use **Cloud Mode - Load balancer** access mode only after you purchase the standard, professional, or platinum edition in cloud mode.
  - In dedicated mode, your dedicated instances and origin servers should be in the same VPC. If they are not in the same VPC, you need to use a **VPC Peering Connection** to connect the two VPCs.

Constraints on Protected Domain Names

- 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.
- A protected object 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.

Certificate Constraints

- 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.

ELB Load Balancer Constraints

- Dedicated WAF instances can use only dedicated ELB load balancers. 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 load balancer access mode, only dedicated load balancers with **Specifications** set to **Application load balancing (HTTP/HTTPS)** can be used.

Specifications Limitations

- For details about the service specifications supported by each WAF edition, see **Specifications Supported by Each Edition**.
- After your website is connected to WAF, the size of the file each time you can upload to the website is limited as follows:

  - Cloud mode - CNAME access: 1 GB
  - Cloud mode - load balancer access or dedicated mode: 10 GB
- The bandwidth limit applies only to websites connected to the cloud CNAME access mode. There is no bandwidth limit but only QPS limit for websites connected to WAF in load balancer access mode.

11 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.

12 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. For more details about how to use WAF to defend against this type of attacks, see **Configuring CC Attack Protection Rules to Defend Against CC Attacks**.

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. Basic web protection can defend against cross-site request forgery attacks. For details, see **Enabling Basic Web Protection**.

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. In WAF anti-crawler protection, you can enable **Scanner** to block or only log scanners and crawlers. For details, see **Configuring an Anti-Crawler Rule**.

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. For details about how to configure WTP, see **Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With**.

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. By default, **General Check** in basic web protection is enabled to defend against XSS attacks. For details, see **Enabling Basic Web Protection**.

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. By default, **General Check** in basic web protection is enabled to defend against SQL injections. For details, see **Enabling Basic Web Protection**.

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. By default, **General Check** in basic web protection is enabled to defend against command injections. For details, see **Enabling Basic Web Protection**.

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. By default, **General Check** in WAF basic web protection is enabled to defend against code injections. For details, see **Enabling Basic Web Protection**.

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. By default, **General Check** in WAF basic web protection is enabled to defend against unauthorized access to files. For details, see **Enabling Basic Web Protection**.

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. WAF basic web protection can defend against such attacks. For details, see **Enabling Basic Web Protection**.

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. If you enable web shell detection in basic web protection, WAF detects web Trojans implanted through the upload interface. For details, see **Enabling Basic Web Protection**.

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. For details about how to use WAF to defend against this type of attacks, see **Defending Hotlinking**.

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 combine logic conditions to block or allow traffic precisely. For more details, see **Configure Precise Protection Rules to Enable Custom Protection**.

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. For details about how to use WAF to establish an IP address whitelist or blacklist, see **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.

Anti-Crawler

An extensive crawler feature library is provided to detect many types of crawlers (search engines, scanners, script tools, and other crawlers). For more details about how to use WAF to defend against crawlers, see **Configuring an Anti-Crawler Rule**.

Non-standard Port

Non-standard ports defined in WAF are the ports other than ports 80 and 443. For more details, see **Ports Supported by Huawei Cloud WAF**.

