

## Edge Security

# FAQs

**Issue** 04  
**Date** 2023-09-20



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI 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.

## **Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

---

# Contents

---

<b>1 About the Product.....</b>	<b>1</b>
1.1 What Is Edge Security?.....	1
1.2 Can EdgeSec Be Used Independently?.....	1
1.3 What Regions Does EdgeSec Support?.....	1
1.4 How Many Layers of Protection Does Edge WAF Provide?.....	1
1.5 What Is the Difference Between QPS and the Number of Requests?.....	2
1.6 Protected Objects.....	2
1.7 Protocols.....	5
<b>2 About Functions.....</b>	<b>7</b>
2.1 How Does Edge WAF Detect SQL Injection, XSS, and PHP Injection Attacks?.....	7
2.2 How Do I Obtain the Real IP Address of a Visitor in Edge WAF?.....	8
2.3 How Does Edge WAF Block Requests?.....	8
2.4 Do I Need to Enable All Ports When Configuring an Edge WAF Whitelist in a Security Group?.....	9
2.5 Why Do Cookies Contain the <b>HWWAFSESID</b> or <b>HWWAFSESTIME</b> field?.....	9
<b>3 Regions and AZs.....</b>	<b>10</b>
3.1 What Are Regions and AZs?.....	10
<b>4 Change History.....</b>	<b>12</b>

# 1 About the Product

---

## 1.1 What Is Edge Security?

Edge Security (EdgeSec) is a security service based on the edge nodes of Huawei Cloud Content Delivery Network (CDN). It provides functions such as Edge Anti-DDoS, CC attack protection, Web protection, and bot behavior analysis. If you have purchased CDN or Whole Site Acceleration (WSA), you can enable security protection for acceleration domain names to safeguard content delivery.

## 1.2 Can EdgeSec Be Used Independently?

No. EdgeSec is supported by Huawei Cloud Content Delivery Network (CDN) sites. You need to purchase CDN or WSA before using EdgeSec.

## 1.3 What Regions Does EdgeSec Support?

EdgeSec supports the following countries and regions: Singapore, Thailand, Indonesia, Malaysia, Philippines, and adjacent regions of these countries.

If your service is deployed far away from the preceding countries and regions, the access latency increases. Consider the service location before determining whether to use EdgeSec.

## 1.4 How Many Layers of Protection Does Edge WAF Provide?

Edge WAF provides layer-7 (application layer) protection.

## 1.5 What Is the Difference Between QPS and the Number of Requests?

Queries Per Second (QPS) indicates the number of requests per second. For example, an HTTP GET request is also called a query. The number of requests is the total number of requests in a specific time range.

Queries Per Second (QPS) is the number of requests a server can handle per second.

### NOTE

QPS is used to measure the number of queries, or requests, per second.

For details about QPS on the **Dashboard** page, see [Table 1-1](#).

**Table 1-1** QPS calculation

Time Range	Average QPS Description	Peak QPS Description
Yesterday or Today	The QPS curve is made with the average QPSs in every minute.	The QPS curve is made with each peak QPS in every minute.
Past 3 days	The QPS curve is made with the average QPSs in every five minutes.	The QPS curve is made with each peak QPS in every five minutes.
Past 7 days	The QPS curve is made with the maximum value among the average QPSs in every five minutes at a 10-minute interval.	The QPS curve is made with each peak QPS in every 10 minutes.
Past 30 days	The QPS curve is made with the maximum value among the average QPSs in every five minutes at a one-hour interval.	The QPS curve is made with the peak QPSs in every hour.

## 1.6 Protected Objects

### Does Edge WAF Support Application Layer Protocol- and Content-Based Access Control?

Edge WAF supports access control over content at the application layer. HTTP and HTTPS are both application layer protocols.

### Can Edge WAF Defend Against XOR Injection Attacks?

Yes. Edge WAF can defend against XOR injection attacks.

## Does EdgeSec Support Vulnerability Detection?

Edge WAF enables anti-crawler rules to detect and block threats such as third-party security tool vulnerability attacks. If you enable the scanner item when configuring anti-crawler rules, Edge WAF detects scanners and crawlers, such as OpenVAS and Nmap.

For details, see [Configuring Anti-Crawler Rules](#).

## Can Edge WAF Check the Body I Add to a POST Request?

The built-in detection of Edge WAF checks POST data, and web shells are the files submitted in POST requests. Edge WAF checks all data, such as forms and JSON files in POST requests based on the default protection policies.

You can configure a precise protection rule to check the body added to POST requests. For details, see [Configuring a Precise Protection Rule](#).

## Can Edge WAF Limit the Access Speed of a Domain Name?

No.

However, you can customize a CC attack protection rule to restrict access to a specific URL on your website based on an IP address, cookie, or Referer, mitigating CC attacks.

For details, see [Configuring a CC Attack Protection Rule](#).

## Can Edge WAF Block URL Requests That Contain Special Characters?

Not. Edge WAF can detect and restrict source IP addresses.

## Can Edge WAF Block Requests for Calling Other APIs from Web Pages?

There are two cases:

- If the request data for calling other APIs on the web page is included in the domain names protected by Edge WAF, the request data passes through Edge WAF. Edge WAF checks the request data and blocks it if it is an attack.
- If the request data for calling other APIs on the web page is not included in the domain names protected by Edge WAF, the request data does not pass through Edge WAF. Edge WAF cannot block the request data.

## Can I Configure Session Cookies in Edge WAF?

No. Edge WAF does not support session cookies.

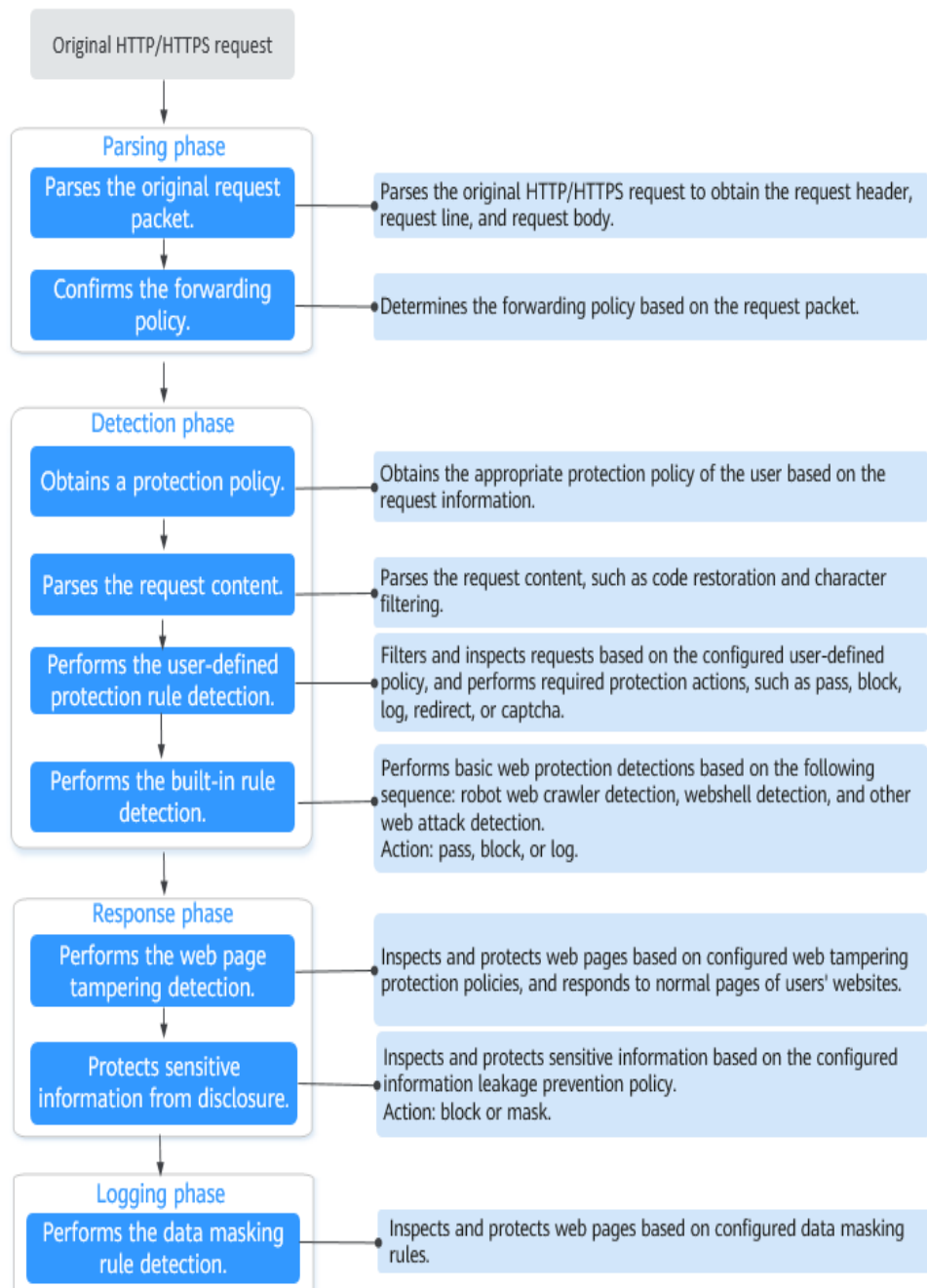
Edge WAF allows you to configure CC attack protection rules to limit the access frequency of a specific path (URL) in a single cookie field, accurately identify CC attacks, and effectively mitigate CC attacks. For example, if a user whose cookie ID is **name** accesses the **/admin\*** page under the protected domain name for more than 10 times within 60 seconds, you can configure a CC attack protection rule to forbid the user from accessing the domain name for 600 seconds.

For details about how to configure a CC attack protection rule, see [Configuring CC Attack Protection Rules](#).

## Does EdgeSec Block Customized POST Requests?

No. EdgeSec does not block user-defined POST requests. [Figure 1-1](#) shows the detection process of the Edge WAF built-in protection rules for original HTTP/HTTPS requests.

**Figure 1-1** EdgeSec engine detection process



For details about the Edge WAF protection process, see [Configuration Guidance](#).

## Does EdgeSec Support the CORS-Denied Policy?

No. EdgeSec does not support the configuration of a protection rule that denies Cross-Origin Resource Sharing (CORS) requests. For details about features of EdgeSec, see [Functions](#).

## Can EdgeSec Limit Access Through Domain Names?

No.

EdgeSec supports the blacklist and whitelist rules to block, log only, or permit access requests from specified IP addresses or IP address segments. For details, see [Configuring an IP Address Blacklist or Whitelist Rule](#).

## Does EdgeSec Have the IPS Module?

Unlike the traditional firewalls, EdgeSec does not have an Intrusion Prevention System (IPS). EdgeSec supports intrusion detection of only HTTP/HTTPS requests.

## Is Edge WAF a Hardware Firewall or a Software Firewall?

Edge WAF is a software firewall. After purchasing Edge WAF, you only need to connect your domain name to use Edge WAF to protect your web applications.

For details, see [Adding a Website to Edge WAF](#).

## Can EdgeSec Defend Against the Apache Struts2 Remote Code Execution Vulnerability (CVE-2021-31805)?

Yes. Edge WAF basic web protection rules can defend against the Apache Struts2 remote code execution vulnerability (CVE-2021-31805).

For details, see [Configuring Basic Web Protection Rules](#).

# 1.7 Protocols

## Does EdgeSec Support the QUIC Protocol?

No.

## Does Edge WAF Support Two-Way SSL Authentication?

No.

## Does EdgeSec Support HTTP/3?

No. Currently, Edge WAF supports HTTP/2.

## Can EdgeSec Protect Websites in the C/S Architecture?

In the C/S architecture, Edge WAF can protect only websites that use the layer-7 HTTP/HTTPS protocol.



## Can EdgeSec Protect Websites Accessed Through HSTS or NTLM Authentication?

Yes. Edge WAF can protect HTTP and HTTPS applications.

- If a website uses the HTTP Strict Transport Security (HSTS) policy, the client (such as a browser) is forced to use HTTPS to communicate with the website. This reduces the risk of session hijacking. Websites configured with HSTS policy use the HTTPS protocol. So, Edge WAF can protect these websites.
- Windows New Technology LAN Manager (NTLM) is an authentication method over HTTP. NTLM uses a three-way handshake to authenticate a connection. NTLM authenticates a client (such as a browser) the same way the Windows remote login authentication does.

Edge WAF can protect applications that use NTLM to authenticate connection between a server and client, such as a browser.

# 2 About Functions

---

## 2.1 How Does Edge WAF Detect SQL Injection, XSS, and PHP Injection Attacks?

A Structured Query Language (SQL) injection is a common web attack. The attacker injects malicious SQL commands into database query strings to deceive the server into executing commands. 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.

XSS attacks exploit vulnerabilities left during web page development to inject malicious instruction code into web pages so that attackers can trick visitors into loading and executing malicious web page programs attackers fabricated. These malicious web page programs are usually JavaScript, but they can also include Java, VBScript, ActiveX, Flash, or even common HTML. After an attack succeeds, the attacker may obtain various content, including but not limited to higher permissions (for example, permissions for certain operations), private content, sessions, and cookies.

### How Does Edge WAF Detect SQL Injection Attacks?

Edge WAF detects and matches SQL keywords, special characters, operators, operators, and comment symbols.

- SQL keywords: union, Select, from, as, asc, desc, order by, sort, and, or, load, delete, update, execute, count, top, between, declare, distinct, distinctrow, sleep, waitfor, delay, having, sysdate, when, dba\_user, case, delay, and the like
- Special characters: ', ; ( )
- Mathematical operators: ±, \*, /, %, and |
- Operators: =, >, <, >=, <=, !=, +=, and -=
- Comment symbols: - or /\*\*/

## How Does Edge WAF Detect XSS Attacks?

Edge WAF checks HTML script tags, event processors, script protocols, and styles to prevent malicious users from injecting malicious XSS statements through client requests.

- XSS keywords (such as **javascript**, **script**, **object**, **style**, **iframe**, **body**, **input**, **form**, **onerror**, and **alert**)
- Special characters (<, >, ', and ")
- External links (href="http://xxx/",src="http://xxx/attack.js")

### NOTE

Rich text can be uploaded using multipart upload instead of body. In multipart upload, rich text is stored in forms and can be decoded even if it is encoded using Base64. Analyze your services and do not use quotation marks and angle brackets as far as possible.

## How Does Edge WAF Detect PHP Injection Attacks?

If a request contains keywords similar to system(xx), the keywords may cause PHP injection attacks. Edge WAF will then block such requests.

## 2.2 How Do I Obtain the Real IP Address of a Visitor in Edge WAF?

After you connect a website to your Edge WAF instance, Edge WAF works as a reverse proxy between the client and the server. The real IP address of the server is hidden and only the IP address of Edge WAF is visible to web visitors.

Generally, a proxy, such as CDN, WAF, and AAD, is deployed between the client and server. Web visitors cannot directly access the server. For example, **web visitor > CDN/WAF/AAD > origin server**.

When forwarding requests to the downstream server, the transparent proxy server adds an **X-Forwarded-For** field to the HTTP header to identify the web visitor's real IP address in the format of **X-Forwarded-For: real IP address of the web visitor, proxy 1-IP address, proxy 2-IP address, proxy 3-IP address, .....->....**

Therefore, you can obtain the web visitor's real IP address from the **X-Forwarded-For** field. The first IP address in this field is the web visitor's real IP address.

## 2.3 How Does Edge WAF Block Requests?

Edge WAF detects the request header and body, such as the form, XML, and JSON data, and blocks requests that do not comply with protection rules.

For details about the Edge WAF protection process, see [Configuration Guidance](#).

## 2.4 Do I Need to Enable All Ports When Configuring an Edge WAF Whitelist in a Security Group?

All ports can be opened. To reduce network security risks, enable only ports 80 and 443.

## 2.5 Why Do Cookies Contain the HWWAFSESID or HWWAFSESTIME field?

**HWWAFSESID** indicates the session ID, and **HWWAFSESTIME** indicates the session timestamp. These two fields are used to mark the request, for example, they can be used to count the requests for a CC protection rule.

After a domain name or IP address is connected to Edge WAF, Edge WAF inserts fields such as **HWWAFSESID** (session ID) and **HWWAFSESTIME** (session timestamp) into the cookie of your customer request. These fields are used by Edge WAF to implement some functions, such as counting requests and monitoring request duration.

# 3 Regions and AZs

## 3.1 What Are Regions and AZs?

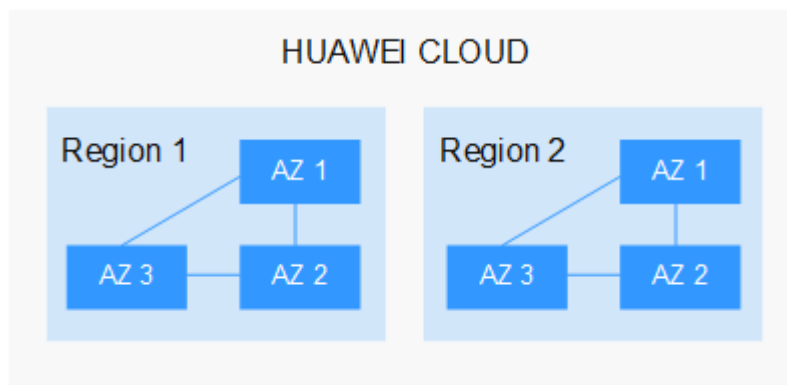
### Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

**Figure 3-1** shows the relationship between the regions and AZs.

**Figure 3-1** Region and AZ



Huawei Cloud provides services in many regions around the world. You can select a region and AZ as needed.

## Selecting a Region

When selecting a region, consider the following factors:

- Location  
You are advised to select a region close to you or your target users. This reduces network latency and improves access rate.
  - If you or your users are in the Asia Pacific region and outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your users are in Africa, select the **AF-Johannesburg** region.
  - If you or your users are in Latin America, select the **LA-Santiago** region.
- Resource price  
Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

## Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

## Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

# 4 Change History

Date	Description
2023-09-20	This issue is the fourth official release. Added: <ul style="list-style-type: none"><li>• <a href="#">How Many Layers of Protection Does Edge WAF Provide?</a></li><li>• <a href="#">What Is the Difference Between QPS and the Number of Requests?</a></li><li>• <a href="#">Protected Objects</a></li><li>• <a href="#">Protocols</a></li><li>• <a href="#">How Does Edge WAF Detect SQL Injection, XSS, and PHP Injection Attacks?</a></li><li>• <a href="#">How Do I Obtain the Real IP Address of a Visitor in Edge WAF?</a></li><li>• <a href="#">How Does Edge WAF Block Requests?</a></li><li>• <a href="#">Do I Need to Enable All Ports When Configuring an Edge WAF Whitelist in a Security Group?</a></li><li>• <a href="#">Why Do Cookies Contain the HWWAFSESID or HWWAFSESTIME field?</a></li></ul>
2023-08-08	This issue is the third official release. Added: <a href="#">What Regions Does EdgeSec Support?.</a>
2023-07-15	This issue is the second official release. Added: <ul style="list-style-type: none"><li>• <a href="#">How Do I Change the Editions of EdgeSec?</a></li><li>• <a href="#">How Do I Renew EdgeSec?</a></li><li>• <a href="#">Can I Unsubscribe from EdgeSec?</a></li></ul>
2023-03-30	This issue is the first official release.

