Edge Security

FAQs

Issue 06

Date 2024-07-16

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

1 About the Product

1.1 What Is Edge Security?

EdgeSec (Edge Security) is a security protection service built on edge nodes.

ESA (Edge Security Acceleration) is a sub-product of EdgeSec. It provides cache acceleration and application security protection and supports multiple security functions, such as web attack defense, DDoS attack defense, and CC attack defense. ESA comprehensively improves the security protection capability of the acceleration network and ensures high-quality user experience and service security.

1.2 Can EdgeSec Be Used Independently?

Yes. EdgeSec can be used independently. It is a service built on Content Delivery Network (CDN) sites, encompassing CDN and whole-site acceleration. By purchasing EdgeSec, you gain access to CDN, whole-site acceleration, and security protection.

1.3 What Regions Does EdgeSec Support?

EdgeSec supports the following countries and regions: Singapore, Thailand, Indonesia, Malaysia, Philippines, Brazil, 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 EdgeSec Provide?

EdgeSec provides protection at the following layers:

Layer 3 (network layer), Layer 4 (transport layer), and Layer 7 (application layer).

1.5 Protected Objects

Does EdgeSec Support Application Layer Protocol- and Content-Based Access Control?

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

Can EdgeSec Defend Against XOR Injection Attacks?

Yes. EdgeSec can defend against XOR injection attacks.

Does EdgeSec Support Vulnerability Detection?

EdgeSec 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, EdgeSec detects scanners and crawlers, such as OpenVAS and Nmap.

For details, see **Configuring Anti-Crawler Rules**.

Can EdgeSec Check the Body I Add to a POST Request?

The built-in detection of EdgeSec checks POST data, and web shells are the files submitted in POST requests. EdgeSec 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 EdgeSec 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, mitigating CC attacks.

For details, see **Configuring a CC Attack Protection Rule**.

Can EdgeSec Block URL Requests That Contain Special Characters?

No. EdgeSec can detect and restrict source IP addresses.

Can EdgeSec Block Requests for Calling Other APIs from Web Pages?

There are two cases:

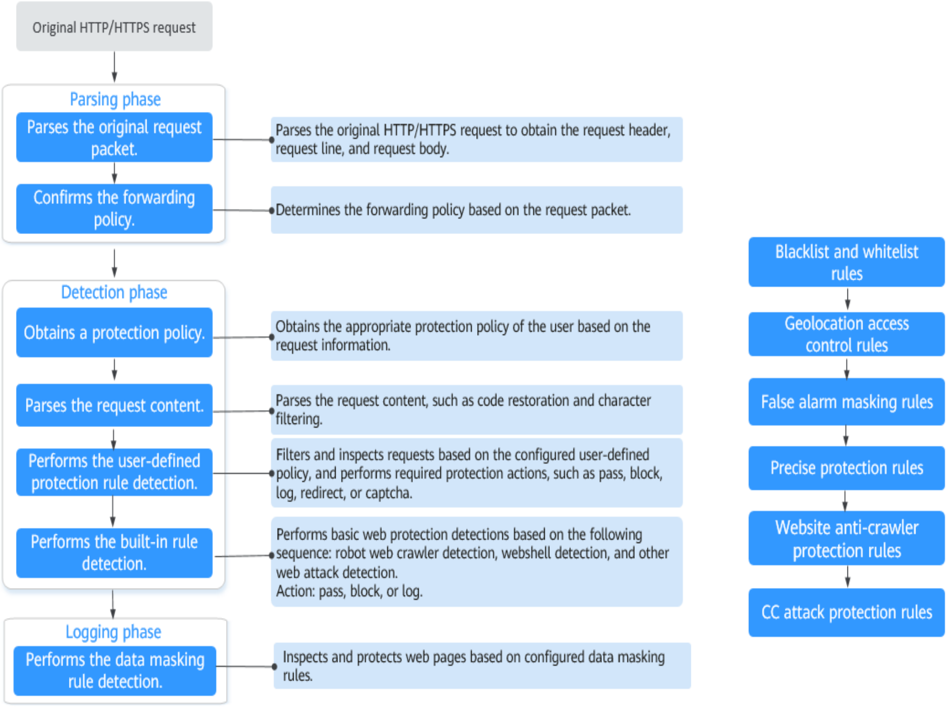
- If the request data for calling other APIs on the web page is included in the domain names protected by EdgeSec, the request data passes through EdgeSec. EdgeSec checks the request data and blocks it if it is an attack.

- If the request data for calling other APIs on the web page is not included in the domain names protected by EdgeSec, the request data does not pass through EdgeSec. EdgeSec cannot block the request data.

Does EdgeSec Block Customized POST Requests?

No. EdgeSec does not block user-defined POST requests. **Figure 1-1** shows the detection process of the EdgeSec built-in protection rules for original HTTP/HTTPS requests.

Figure 1-1 EdgeSec engine detection process


Original HTTP/HTTPS request
Parsing phase
Parses the original request packet.
Parses the original HTTP/HTTPS request to obtain the request header, request line, and request body.
Confirms the forwarding policy.
Determines the forwarding policy based on the request packet.
Detection phase
Obtains a protection policy.
Obtains the appropriate protection policy of the user based on the request information.
Parses the request content.
Parses the request content, such as code restoration and character filtering.
Performs the user-defined protection rule detection.
Filters and inspects requests based on the configured user-defined policy, and performs required protection actions, such as pass, block, log, redirect, or captcha.
Performs the built-in rule detection.
Performs basic web protection detections based on the following sequence: robot web crawler detection, webshell detection, and other web attack detection.
Action: pass, block, or log.
Logging phase
Performs the data masking rule detection.
Inspects and protects web pages based on configured data masking rules.
Blacklist and whitelist rules
Geolocation access control rules
False alarm masking rules
Precise protection rules
Website anti-crawler protection rules
CC attack protection rules

For details about the EdgeSec 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 or log only 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 EdgeSec a Hardware Firewall or a Software Firewall?

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

For details, see **Adding a Website**.

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

Yes. EdgeSec 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**.

1.6 Protocols

Does EdgeSec Support the QUIC Protocol?

No.

Does EdgeSec Support Two-Way SSL Authentication?

No.

Does EdgeSec Support HTTP/3?

No. Currently, EdgeSec supports HTTP/2.

Can EdgeSec Protect Websites in the C/S Architecture?

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

Can EdgeSec Protect Websites Accessed Through HSTS or NTLM Authentication?

Yes. EdgeSec 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, EdgeSec 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.

EdgeSec 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 EdgeSec 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 EdgeSec Detect SQL Injection Attacks?

EdgeSec detects and matches SQL keywords, special characters, 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 EdgeSec Detect XSS Attacks?

EdgeSec 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 EdgeSec Detect PHP Injection Attacks?

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

2.2 How Do I Obtain the Real IP Address of a Visitor in EdgeSec?

After you connect a website to your EdgeSec instance, EdgeSec 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 EdgeSec is visible to web visitors.

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

EdgeSec 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 EdgeSec protection process, see **Configuration Guidance**.

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

All ports can be opened.

However, to reduce network security risks, enable only ports 80 and 443.

2.5 Why Do Cookies Contain the HWEdgeSecSESID or HWEdgeSecSESTIME field?

HWEdgeSecSESID indicates the session ID, and **HWEdgeSecSESTIME** 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 EdgeSec, EdgeSec inserts fields such as **HWEdgeSecSESID** (session ID) and **HWEdgeSecSESTIME** (session timestamp) into the cookie of your customer request. These fields are used by EdgeSec to implement some functions, such as counting requests and monitoring request duration.

2.6 Does Edge Security Support Alarm Notifications for Attacks?

Edge security supports alarm notifications for attacks.

An alarm is sent when a single domain name undergoes 100,000 attacks within 5 minutes or the maximum attack bandwidth reaches 100 Mbit/s within 5 minutes.

You can click **Message Center** button in the upper right corner of the console and choose **My Messages** > **All Messages** to view detailed alarm information on the **O&M** tab page.

3 Regions and AZs

3.1 What Are Regions and AZs?

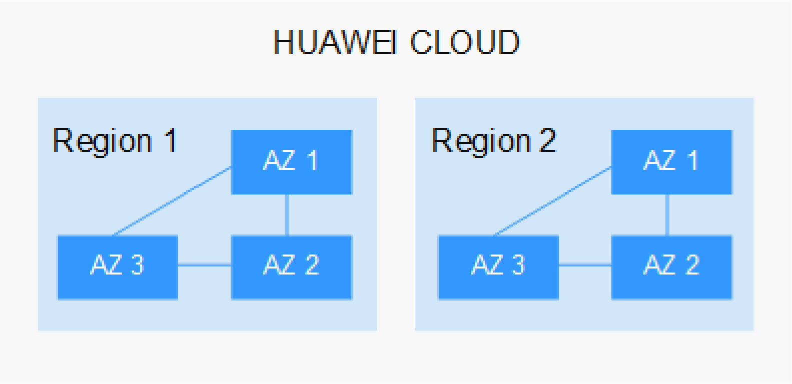
Concepts

A region or an availability zone (AZ) identifies the location of a data center. You can create resources in a specific region or an 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**.