Edge Security

Service Overview

Issue 07

Date 2024-07-16

HUAWEI

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.

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 What Is Edge Security Service?

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.

How It Works

When a user request reaches the EdgeSec acceleration network, the node identifies and intercepts various attack requests. EdgeSec supports anti-DDoS traffic cleaning. The EdgeSec engine analyzes the behavior of web, BOT, and CC attacks and updates interception policies to block malicious requests from reaching customers' origin servers, ensuring smooth and stable service access and implementing dynamic and static network acceleration.

2 Basic Concepts

CDN

Content Delivery Network (CDN) is a smart virtual network on the Internet infrastructure. CDN caches origin content on points of presence (PoPs) closer to users, so content can load faster.

DDoS Attack

Common types of DDoS attacks: SYN Flood, ACK Flood, ICMP Flood, UDP Flood, NTP Flood, DNS Flood, and SSDP reflection attacks.

CC Attack

CC (Challenge Collapsar) attack is a type of DDoS attack. In a CC attack, the attacker uses a proxy server to generate and send disguised requests to the target host.

OWASP Threats

Common types of OWASP (Open Web Application Security Project) threats: SQL injection, XSS, file inclusion, directory traversal attacks, sensitive file access, command and code injections, web shells, backdoors, and malicious HTTP requests.

BOT Attack

A bot is a software application that is programmed to do certain tasks and is used to automatically execute repetitive tasks. Common BOT attacks include malicious crawlers, vulnerability scanning, DDoS attacks, credential cracking, bonus hunting, and click fraud.

API Protection

API protection: EdgeSec automatically discovers and manages API assets by category, monitors API assets for suspicious operations and abnormal callings, and quickly responds to and intercepts abnormal behaviors.

EdgeSec Acceleration Node

An EdgeSec acceleration node is a network node that has fewest intermediate steps away from end users and has security protection capabilities. Compared with other nodes, edge nodes provide end users with faster response and connection.

Concurrent Requests

The number of concurrent requests refers to the number of requests that the system can process simultaneously. When it comes to a website, concurrent requests refer to the requests from the visitors at the same time.

3 Edge Security Acceleration (ESA)

3.1 Features

DDoS Attack Protection

On the basis of advanced feature identification algorithms, Edge Anti-DDoS of EdgeSec detects traffic in a unified and accurate manner. After identifying attacks, Edge Anti-DDoS can quickly clean the traffic and defend against various heavy-traffic attacks, such as SYN flood, UDP flood, and ICMP flood, ensuring service stability.

The EdgeSec node network is built based on the distributed architecture and intelligently schedules global load balancing. When the attack traffic in a CDN edge site reaches the cleaning threshold, the traffic is scheduled to the nearest AAD equipment room with higher bandwidth to cope with ultra-large DDoS attacks and ensure smooth and stable service access in the case of burst attacks.

CC attack prevention

A CC attack protection rule can limit access to a specific path (URL) of the protected website based on a specific IP address in access requests. EdgeSec can accurately identify and mitigate CC attacks, such as brute-force attacks by exploiting weak passwords. Protective actions of CC attack protection rules include **Verification code**, **Block**, and **Log only**.

- Flexible policy configuration

  You can set rate limiting policies by IP address as required.
- Returned page customization

  You can customize returned content and page types to meet diverse service needs.

Basic Web Protection

Backed by an extensive preset reputation database, EdgeSec defends against the Open Web Application Security Project (OWASP) top 10 threats, vulnerability exploits, web shells, and other threats.

- All-around protection

  EdgeSec detects and blocks varied attacks, such as SQL injection, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory (path) traversal attacks, unauthorized sensitive file access, command/code injections, and XML or Xpath injection attacks.

- Web shell detection

  Protects against web shells from upload interface.

- Precise threat identification
  - EdgeSec uses built-in semantic analysis engine and regex engine and supports configuring of blacklist/whitelist rules so that EdgeSec has a low false positives rate.
  - EdgeSec can automatically decode common codes no matter how many times they are encoded.

    EdgeSec 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

  EdgeSec 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 Inspection

  EdgeSec detects all header fields in the requests.

- Shiro Decryption Check

  EdgeSec uses AES and Base64 to decrypt the rememberMe field in cookies and checks whether this field is attacked.

Anti-Crawler Protection

EdgeSec dynamically analyzes website service models and accurately identifies multiple crawler behaviors based on data risk control and bot identification systems.

- Anti-crawler protection with feature libraries

  EdgeSec precisely blocks web page crawlers with custom scanner and crawler rules.

- JavaScript

  EdgeSec identifies and blocks JavaScript crawling with custom rules.

3.2 Advantages

Precise Scheduling

Enhance user access experience with accurate, evolving IP geolocation database and dynamic PoP adjustment.

Easy to Use

Configure domains with CDN in several steps, customize them on the console, and call open APIs for app integration and cross-cloud management.

High-Performance Cache

Unique AICache technology and multi-level cache scheduling (memory->SSD->HDD) improve cache hit ratio and shorten access queues.

Comprehensive Security

EdgeSec leverages Huawei's years of experience in online security to protect against a variety of cyber attacks, such as DDoS attacks, web attacks, CC attacks, and malicious crawlers. EdgeSec defends against various OWASP threats, such as SQL injection, XSS, and file inclusion.

Compliance Certification

Huawei Cloud has AAA-level CDN enterprise credit assessment, IPv6 certification, and trusted cloud certification, providing assurance for acceleration.

Refined Management

Stay on top of your services by analyzing statistics about access, utilization, and traffic, and tracking offline logs.

3.3 Application Scenarios

Industry Customer	Acceleration Requirement	Protection Requirement
Media	• Website acceleration • On-demand service acceleration	• L3/L4 DDoS mitigation • CC attack mitigation • Web application protection
E-commerce	• Website acceleration • Dynamic site acceleration	• L3/L4 DDoS mitigation • CC attack mitigation • Web application protection • Bot management • API protection
Finance	• Website acceleration • Dynamic site acceleration	• L3/L4 DDoS mitigation • CC attack mitigation • Web application protection • Bot management • API protection

Industry Customer	Acceleration Requirement	Protection Requirement
Website downloading	Download acceleration	• L3/L4 DDoS mitigation • CC attack mitigation • Web application protection

4 Service Edition Differences

Currently, EdgeSec provides the enterprise edition. For details, see **Version Description** and **Functions and Features Supported by Each Version**.

Description

Table 4-1 describes each version of EdgeSec.

Table 4-1 Description

Service Scale	Enterprise Edition
Number of domain names	20
CC attack prevention rules	100
Precise protection rules	100
Reference table rules	100
IP address blacklist and whitelist rules	1,000
Geolocation access control rules	100
Web tamper protection rules	100
Information leakage prevention rules	100
Global protection whitelist rules	1,000
Data masking rules	100

Functions Supported by Each Edition

Table 4-2 lists the security features applicable to each version.

Description:

- √: The function is included in the current edition.

- x: The function is not included in the current edition.

Table 4-2 Security features

Function Template	Enterprise Edition
Domain expansion package	√
Adding wildcard domain names	√
Flexibly configuring defense policies in a batch	√
Batch adding domain names to a policy	√
Protection against common web attacks, such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections	√
Updating protection rules against zero-day vulnerabilities to the latest on the cloud and delivering virtual patches in a timely manner	√
Web shell detection	√
Deep anti-evasion inspection to identify and block evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques	√
Inspection of all header fields in the requests	√
CC attack prevention	√
Precise protection	√
Reference table management	√
IP address whitelist and blacklist and batch importing of IP addresses/IP address ranges	√
Allowing or blocking web requests based on the countries that the requests originate from.	√
Identification and blocking of crawler behavior such as search engines, scanners, script tools, and other crawlers	√
JavaScript-based anti-crawler protection	√
Information leakage prevention rules	√
Global protection whitelist rules	√
Data masking	√

5 Restrictions

Item	Description
Domain name admission	• Chinese mainland – Your HUAWEI ID has completed real-name authentication. – The domain name has been licensed by the Ministry of Industry and Information Technology (MIIT) and the Internet Content Provider (ICP) license is still valid. – The domain name has passed content moderation. • Outside the Chinese mainland – The domain name has passed content moderation. • Global – You have completed real-name authentication on Huawei Cloud. – The domain name has been licensed by the MIIT and the ICP license is still valid. – The domain name has passed content moderation.

Item	Description
Content moderation	The access of websites that violate related laws and regulations is not supported, including but not limited to: ● Websites that contain pornographic content or content related to gambling, illegal drugs, frauds, or infringement ● Gaming websites that run on illegal private servers ● Websites that provide pirated games/software/ videos ● P2P lending websites ● Unofficial lottery websites ● Unlicensed hospital and pharmaceutical websites ● Inaccessible websites or websites that do not contain any substantial information **NOTE** ● If your domain name content violates related laws and regulations, you shall bear the related risks. ● If any pornographic content or content related to gambling, illegal drugs, or frauds is found on your domain name, the domain name and other domain names that use the same origin server will be deleted from ESA and can no longer access ESA. Acceleration domain name quota of the account will be reduced to 0.
Domain name quota	The domain name quota is determined by the EdgeSec acceleration package. If the domain quota cannot meet your requirements, you can purchase extra domain name packages to increase the number of protected domain names. ● Number of domain names (enterprise edition): 20.
Request method	GET, PUT, POST, and DELETE.

6 Security

6.1 Shared Responsibilities

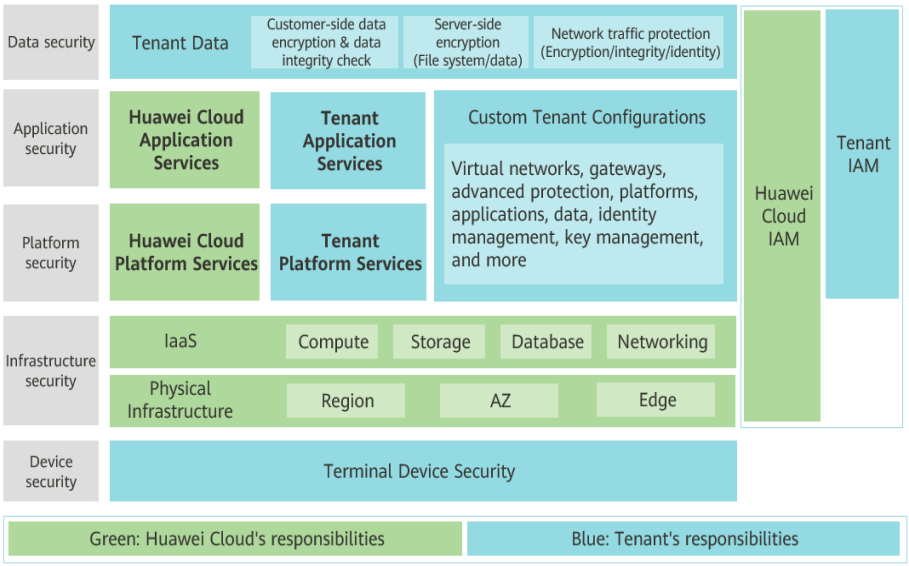
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 6-1 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 6-1 Huawei Cloud shared security responsibility model



6.2 Identity Authentication and Access Control

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

IAM is a basic permission management service provided by Huawei Cloud. It helps EdgeSec securely control access permissions. With IAM, you can add users to a user group and configure policies to control their access to EdgeSec resources. For details about access permissions on EdgeSec resources, see **Permissions Management**.

6.3 Data Protection Controls

EdgeSec uses multiple data protection methods and features to ensure data security and reliability.

Table 6-1 Data protection controls and features

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

Measure	Description
Data integrity verification	When the EdgeSec process is started, the configuration data is obtained from the configuration center instead of directly reading local files.
Data isolation mechanism	EdgeSec isolates its tenant zone from its management plane. Operation permissions for EdgeSec 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. EdgeSec automatically detects cloud service subscription status and releases resources when the retention period expires.

EdgeSec fully respects user privacy, complies with laws and regulations, and does not collect or store any user privacy data. For more privacy data usage and protection issues, see **Privacy Statement**.

6.4 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 EdgeSec for auditing.

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

- Logging

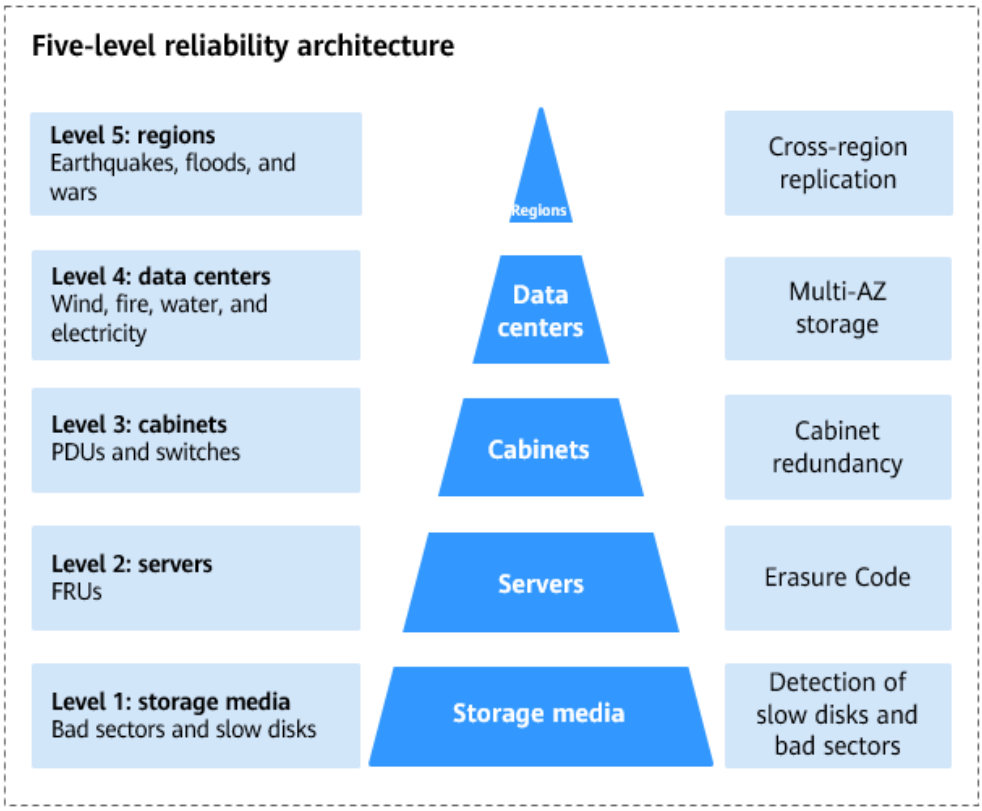
  After you enable CTS, the system starts recording operations on EdgeSec. You can view the operation records of the last 7 days on the CTS console.

6.5 Service Resilience

Huawei Cloud EdgeSec 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 EdgeSec provides a DR plan:

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

Huawei Cloud EdgeSec provides services for global users and is deployed in multiple zones. All components such as the management plane and engine of EdgeSec are deployed in active/standby or cluster mode.



6.6 Risk Monitoring

EdgeSec has been interconnected with Cloud Eye. You can view EdgeSec metrics on Cloud Eye to learn about the EdgeSec 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 EdgeSec 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 EdgeSec protection status in a timely manner.

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

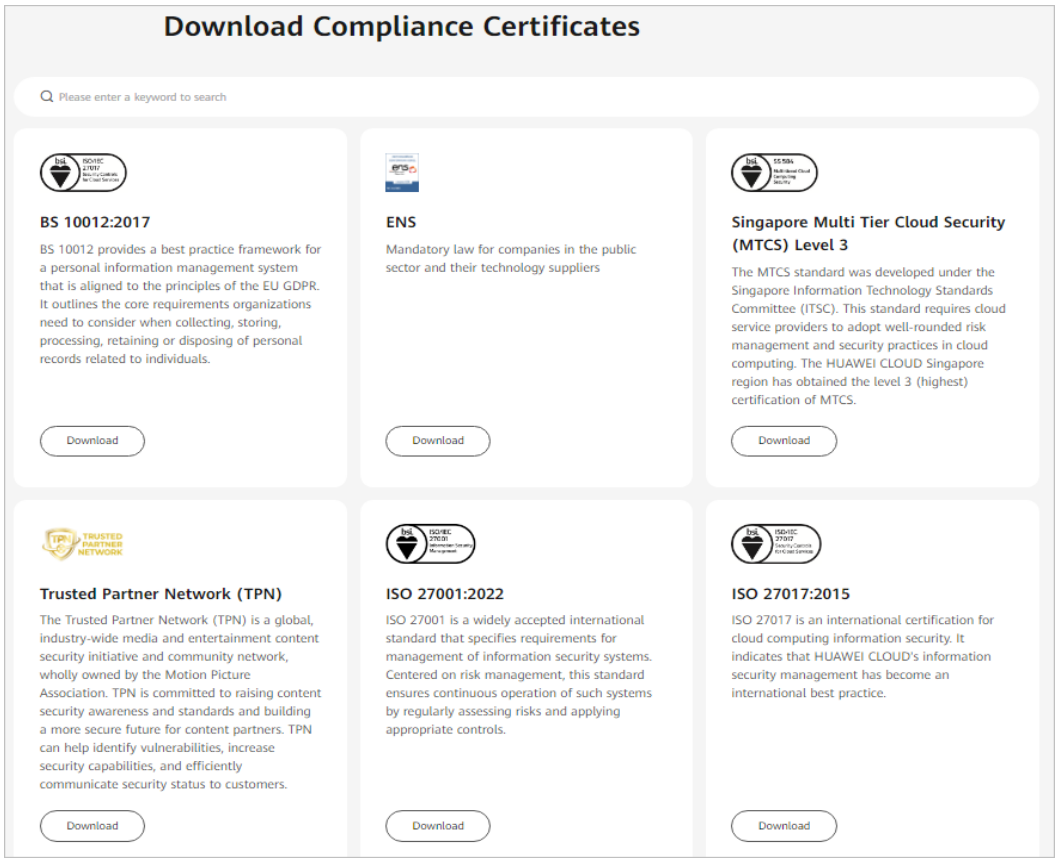
- **EdgeSec Metrics**
- **Setting Monitoring Alarm Rules**
- **Viewing Monitoring Metrics**

6.7 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.

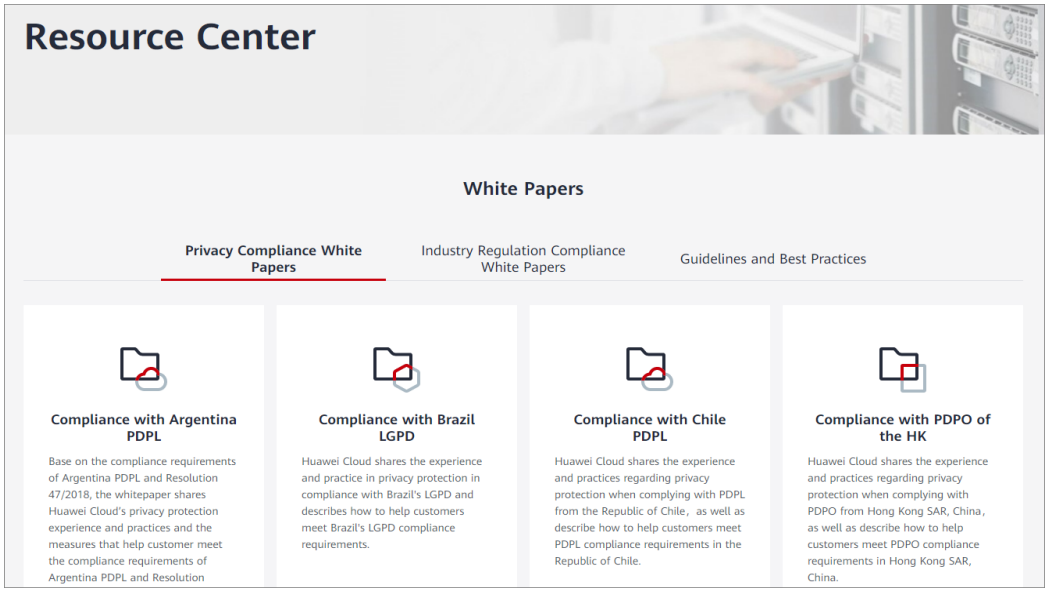
Figure 6-2 Downloading compliance certificates



Resource Center

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

Figure 6-3 Resource center



7 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your EdgeSec 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 HUAWEI 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 EdgeSec 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 EdgeSec resources.

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

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

EdgeSec Permissions

By default, new IAM users do not have 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.

EdgeSec is a project-level service divided by physical region during deployment. To assign 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 EdgeSec, the users need to switch to a region where they have been authorized to use EdgeSec.

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. This mechanism provides a limited number of service-level roles for authorization. If one role has a dependency role required for accessing AAD, assign both roles to the users. However, roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: A type of fine-grained authorization that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and ideal for secure access control. For example, EdgeSec administrators can only grant EdgeSec users the permissions needed for managing a particular type of EdgeSec resources. Most fine-grained policies split permissions based on APIs.

Table 7-1 describes all system roles of EdgeSec.

Table 7-1 EdgeSec system roles

System Role/ Policy Name	Description	Type	Dependency
EdgeSec FullAccess	All permissions of EdgeSec	System policy	None
EdgeSec ReadOnlyAccess	Read-only permission of EdgeSec	System policy	

Related Links

- IAM Service Overview
- Creating a User Group and Granting Permissions

8 EdgeSec and Other Services

This section describes the relationship between EdgeSec and other cloud services.

Content Delivery Network (CDN)

Content Delivery Network (CDN) is an intelligent virtual network built on top of existing Internet infrastructure. Origin content is cached on nodes closer to end users so content can load faster. CDN speeds up site response and improves site availability. It breaks through the bottlenecks caused by low bandwidth, heavy access traffic, and uneven distribution of edge nodes.

EdgeSec is a security protection service supported by CDN edge nodes.

Cloud Trace Service (CTS)

Cloud Trace Service (CTS) generates traces to enable you to get a history of operations performed on EdgeSec, allowing you to query, audit, and backtrack resource operation requests initiated from the management console as well as the responses to those requests.

CTS records operations related to EdgeSec, facilitating your further queries, audits, and retrievals.

Cloud Eye

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

Identity and Access Management (IAM)

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

Log Tank Service (LTS)

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

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.

EdgeSec supports enterprise management. You can manage resources on EdgeSec by enterprise project and set user permissions for each enterprise project.

