Cloud Firewall

Service Overview

Issue 12

Date 2025-03-04

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 CFW?

Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects the Internet border and VPC border on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. It employs AI for intelligent defense, and can be elastically scaled to meet changing business needs, helping you easily handle security threats. CFW is a basic service that provides network security protection for user services on the cloud.

Intelligent Defense

CFW has integrated Huawei Cloud/security capabilities and Huawei network threat intelligence. Its AI intrusion prevention engine can detect and block malicious traffic in real time. It works with other security services globally to defend against Trojans, worms, injection attacks, vulnerabilities, and phishing attacks.

High Scalability

CFW can implement refined control on all traffic, including Internet border and cross-VPC traffic, to prevent external intrusions, internal penetration attacks, and unauthorized access from internal to external networks. Its bandwidth, number of EIPs, and number of security policies can be increased without limit. Its cluster is deployed in HA mode to protect your workloads under heavy traffic.

Easy-to-Use Application

As a cloud-native firewall, CFW can be enabled easily, import multi-engine security policies with a few clicks, automatically check assets within seconds, and provide a UI for performing operations, greatly improving management and defense efficiency.

Supported Access Control Policies

- Access control based on the 5-tuple (source IP address, source port, destination IP address, destination port, and protocol)
- Access control based on the domain name
- Access control based on the intrusion prevention system (IPS). The IPS works in observation or interception mode. In block mode, CFW detects and blocks traffic that matches the IPS rules.

- ACL access control policies set for IP address groups, blacklists, and whitelists

2 Features

CFW provides the standard edition, and the professional edition. You can use access control, attack defense, traffic analysis, and log audit functions on the console.

Table 2-1 Features

Item	Description
Dashboard	You can check basic information about firewall instances, resource protection, and more statistics.
Assets	Manage and view EIPs and VPCs.
Access Control	• You can control traffic at Internet and VPC borders based on IP addresses, regions, and domain names. • You can use the policy assistant to quickly check protection rule hits and adjust rules in a timely manner.

Item	Description
Attack Defense	• IPS: It provides you with basic protection functions, and, with many years of attack defense experience, it detects and defends against a wide range of common network attacks and effectively protects your assets. – Basic defense rule database: It provides threat detection and vulnerability scan based on the built-in IPS rule database. It can scan traffic for phishing, Trojans, worms, hacker tools, spyware, brute-force attacks, vulnerability exploits, SQL injection attacks, XSS attacks, and web attacks. It can also detect protocol anomalies, buffer overflow, access control, suspicious DNS activities, and other suspicious behaviors. **NOTE** In the basic protection rule database, you can manually modify protection actions. You can query rule information by rule ID, signature name, risk level, update time, CVE ID, attack type, rule group, and current action in the basic protection rule database. – Virtual patch database: Hot patches are provided for IPS at the network layer to intercept high-risk remote attacks in real time and prevent service interruption during vulnerability fixing. New IPS rules are displayed in the virtual patch rule library. A new IPS rule will be added to the virtual patch rule library first and then to the IPS rule library. – Custom IPS signature: You can customize IPS signature rules. CFW will detect threats in data traffic based on signatures. **NOTE** HTTP, TCP, UDP, POP3, SMTP and FTP protocols can be configured in user-defined IPS signatures. • Sensitive directory scan defense: It defends against scan attacks on sensitive directories on your servers. • Reverse shell defense: It defends against reverse shells. • Anti-virus: This function identifies and processes virus files through virus feature detection to prevent data damage, permission change, and system breakdown. The antivirus function can check access via HTTP, SMTP, POP3, FTP, IMAP4, and SMB. • Security dashboard: You can easily check attack defense information on the security dashboard and adjust defense policies in a timely manner.
Traffic Analysis	The following traffic statistics are displayed: • Inbound traffic: statistics on the total inbound traffic from the Internet to ECSs • Outbound traffic: statistics on the traffic generated when cloud servers proactively access the Internet • Inter-VPC access: inbound and outbound traffic statistics between VPCs

Item	Description
Log Audit	You can check the following types of logs: • Attack event logs, which contain details about intrusions • Access control logs, which contain details about what access is allowed and what is blocked • Traffic logs, which contain the access traffic of specific services You can use Huawei Cloud Log Tank Service (LTS) to record all CFW logs, including attack event, access control, and traffic logs.
System Management	You can use the following functions: • Alarm notification: You can use CFW to set notifications for attack logs and traffic threshold-crossing warnings. After the alarm notification function is enabled, IPS attack logs and traffic threshold-crossing warnings will be sent through emails or SMS messages. • Network packet capture: Helps you locate network faults and attacks. • Multi-account management: The CFW instance under an account can protect the EIPs under multiple accounts. • DNS configuration: The DNS server resolves and delivers IP addresses. • Security report: Generates log reports to help you learn about the security status of assets in a timely manner.

Table 2-2 Engine

Engine	Function	Protocol	Scenario
Firewall engine	The load balancing component distributes user traffic to the tenant firewall engine for security check and protection, and then sends the traffic to the target ECS. This engine provides various detection functions and flexible blocking policies.	TCP, UDP, ICMP, and Any	Protection for the border of Internet and VPC

3 Application Scenarios

External Intrusion Prevention

You can use CFW to perform security stocktaking on service assets accessible to the public network and enable intrusion detection and prevention in one click.

Control Over Server Originated Traffic

Implement domain-based precise control over server originated traffic.

Inter-VPC Access Control (Available in Professional Edition)

Check inter-VPC traffic and control internal access.

4 Editions

CFW provides the standard edition, and the professional edition. You can use access control, attack defense, traffic analysis, and log audit functions on the console.

For details about the functions, see **Features**. For details about the differences, see **Table 4-2**.

Table 4-1 Editions

Edition	Billing Mode	Protected Object	Description
Basic	Yearly/ Monthly	EIP	• Provides refined access control policy configuration for EIPs. • Meets log query requirements.
Standard	Yearly/ Monthly	EIP	• Meets graded protection requirements. • Provides network security protection to defend against network intrusions and server compromises.
Professional	• Pay-per-use • Yearly/ Monthly	• EIP • VPC	• Meets graded protection or key event assurance requirements. • Provides network security protection to defend against network intrusions and server compromises, and control the accesses between internal networks.

Table 4-2 Editions

Feature		Standard	Professional (Yearly/ Monthly)	Professional (Pay-per-Use)
Protected object	IPv4	√	√	√
	IPv6	×	×	×
Protection specifications	Protected EIPs	20 (can be increased to 2000)	50 (can be increased to 2000)	1000 (upper limit)
	Protected VPCs	×	2 (can be increased to 1,000)	20 (upper limit)
	Internet Border Protection Bandwidth	10 Mbit/s (can be increased to 50,000 Mbit/s)	50 Mbit/s (can be increased to 50,000 Mbit/s)	1 Gbps
	VPC Border Protection Bandwidth	×	200 Mbit/s (can be increased with the number of VPCs)	
Access traffic control	ACL access control for public network assets (based on IP addresses, domain names, domain groups, and geographical locations)	√	√	√
	North-south traffic protection and cloud resource (such as EIP) protection against risks on the Internet	√	√	√
	North-south traffic audit and log query	√	√	√
	East-west traffic protection, asset protection between VPCs, and full traffic analysis	×	√	√

Feature		Standard	Professional (Yearly/ Monthly)	Professional (Pay-per-Use)
	East-west traffic monitoring to obtain inter-VPC traffic data in real time	×	√	√
Protection policies	Intrusion prevention system (IPS)	√	√	√
	Custom IPS signature database	×	√	√
	Virtual patching	√	√	√
	Sensitive directories and reverse shells	√	√	√
	Antivirus	×	√	√
System management	Multi-account management	20	50	20

NOTE

Description:

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

5 Personal Data

Personal Data Use Scenario	Log data	Network packet capture
Collected Personal Data	IP address	Packet capture file
Data Source and Collection Method	The firewall identifies source and destination IP addresses from protected traffic.	Use the packet capture function on the firewall console.
Purpose and Security Measure	• Details about the traffic identified by the firewall are displayed. • The data is uploaded to the alarm management server through HTTP. • The audit logs are stored in plaintext and can be accessed only by administrators.	After a user captures packets on the firewall, the packets are stored in the OBS bucket of the management account. Only administrators can access the OBS bucket.
Retention Period and Policy	The data is automatically deleted after seven days.	The data is automatically deleted after seven days.
Destruction Method	Data is deleted by the system to release the storage space for other data.	Data is deleted by the system to release the storage space for other data.
Export Type	Export logs on the firewall console.	Use access code to download the packet capture file stored in OBS.
Export Guide	Choose **Log Audit** > **Log Query** and export logs.	For details, see **Downloading Packet Capture Results**.

6 Security

6.1 Shared Responsibilities

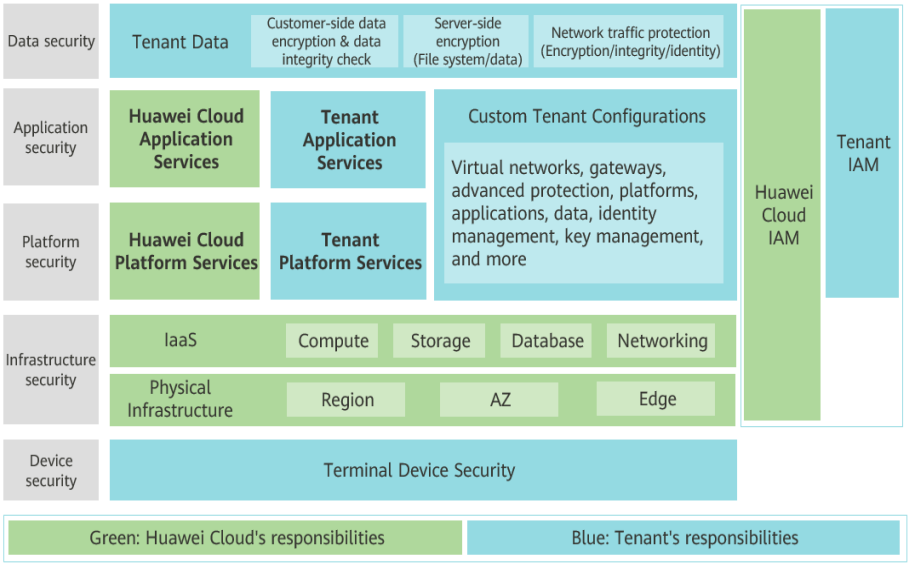
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system 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

CFW works with Identity and Access Management (IAM). IAM permissions define which actions on your cloud resources are allowed and which actions are denied, to control access to your resources. With IAM, you can add users to a user group and configure policies to control their access to Huawei Cloud resources.

For details about CFW resource access permissions, see **Permissions Management**.

6.3 Data Protection Technologies

CFW takes different measures to keep data secure and reliable.

Table 6-1 CFW data protection methods and features

Measure	Description
Static data protection	CFW 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. Your configurations are kept secure when transmitted over HTTPS.
Data integrity verification	When the CFW process is started, the configuration data is obtained from the configuration center instead of local files.

Measure	Description
Data isolation mechanism	CFW isolates its tenant zone from its management plane. Operation permissions for CFW 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. CFW automatically detects cloud service subscription status and releases resources when the retention period expires.

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

6.4 Audit and Logging

Monitoring is key to ensuring the reliability, availability, and performance of CFW. You can summarize operation logs of Huawei Cloud services for analysis, audit, resource monitoring, and fault locating.

CFW interworks with Cloud Trace Service (CTS). Huawei Cloud CTS collects, stores, and queries resource operation records. You can use these records to perform security analysis, track resource changes, audit compliance, and locate faults.

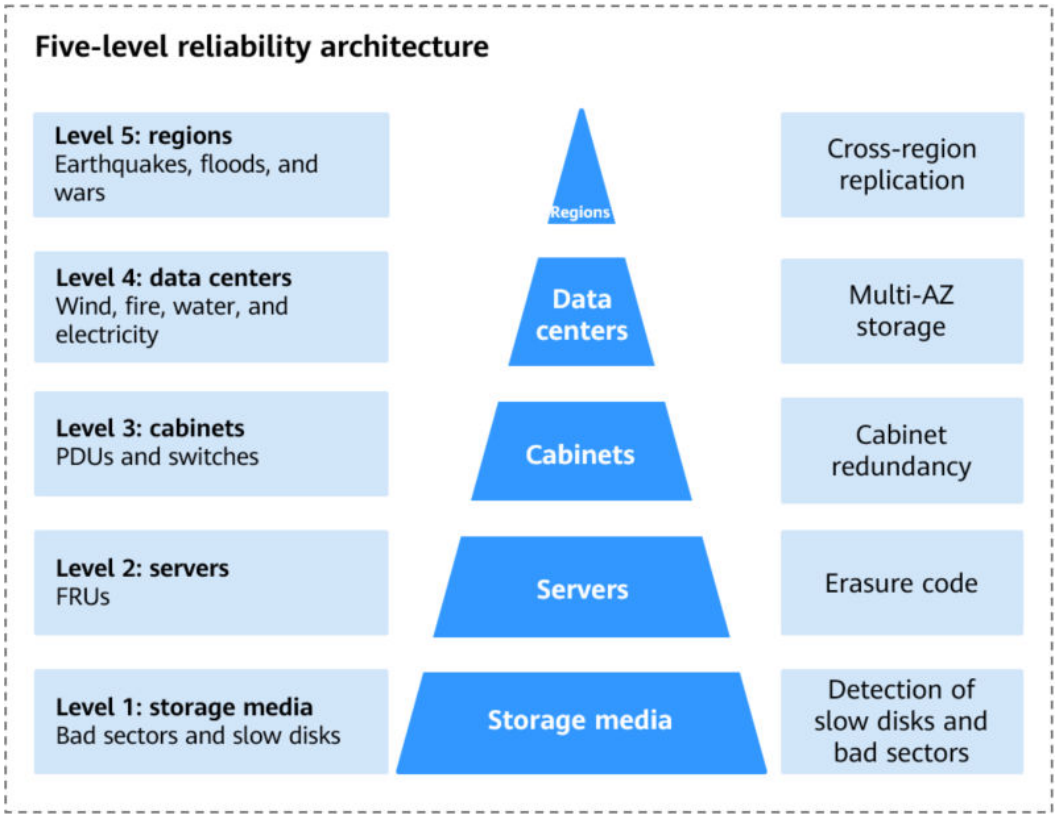
For details, see **What Is Cloud Trace Service?**

6.5 Service Resilience

Huawei Cloud data centers are deployed around the world. All data centers are running properly. 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. In order to minimize the service interruptions caused by hardware failures, natural disasters, or other disastrous events, Huawei Cloud provides a DR plan for all data centers:

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

CFW is available worldwide and is deployed in multiple AZs. With management planes, engines, and other components of CFW deployed in active/standby or cluster mode, CFW itself is stable enough. For details about its deployment, see **Regions and Endpoints**.



6.6 Risk Monitoring

CFW interworks with Cloud Eye. 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 create monitoring metrics in Cloud Eye, and then check the metrics and alarms generated for CFW on the Cloud Eye console.

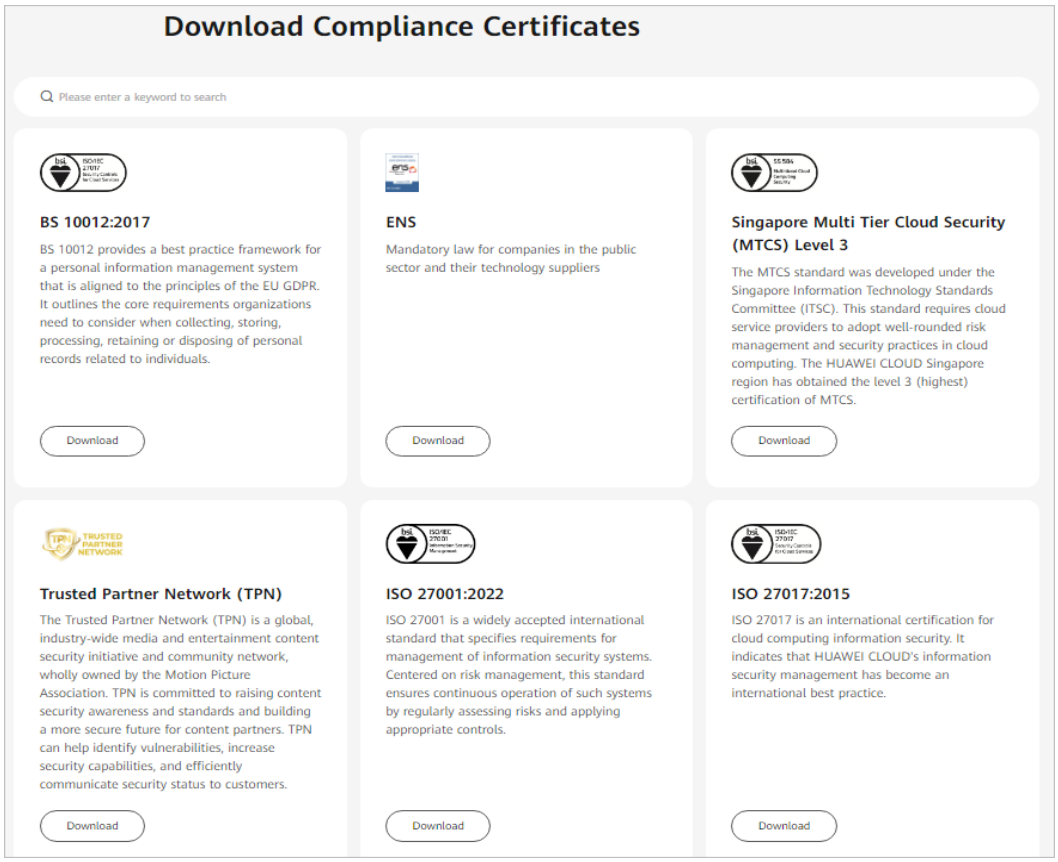
- For details about what is Cloud Eye and how to use it, see **Overview**.
- For details about how to use Cloud Eye to monitor CFW, see **Configuring Alarm Monitoring Rules**.

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.

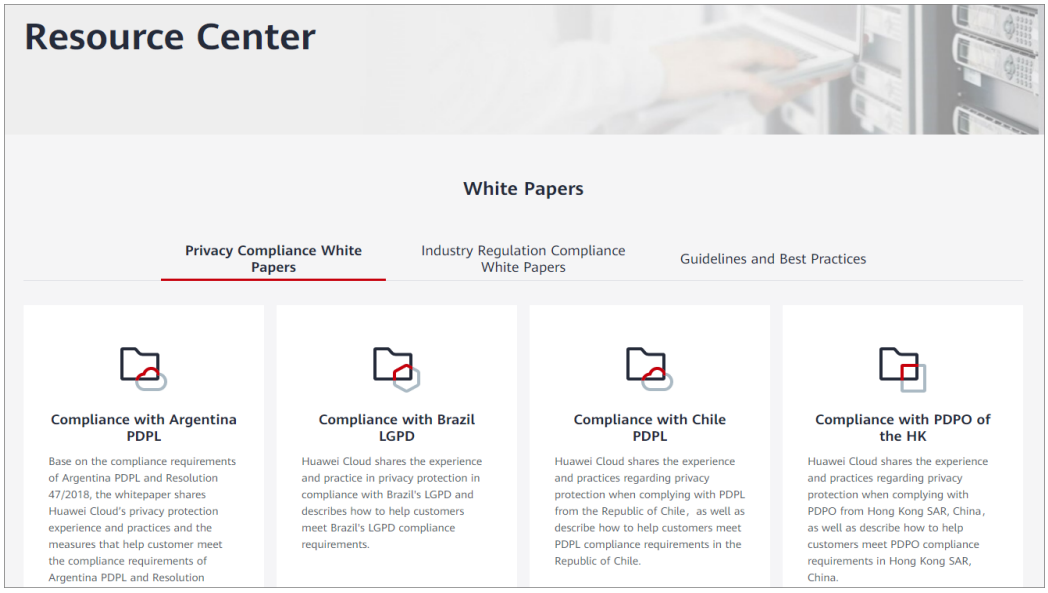
Figure 6-2 Downloading compliance certificates



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 CFW resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your Huawei Cloud resources.

With IAM, you can use your Huawei Cloud account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, if you have software developers and you want to assign them the permission to access CFW but not to delete CFW or its resources, then you can create an IAM policy to assign the developers the permission to access CFW but prevent them from deleting CFW related data.

If your Huawei Cloud account does not require individual IAM users for permissions management, skip this section.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see **What Is IAM?**

CFW Permissions

By default, new IAM users do not have any permissions assigned. To assign permissions to these new users, you need add them to one or more groups, and attach permission 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.

CFW is a project-level service deployed and accessed in specific physical regions. 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 CFW, the users need to switch to a region where they have been authorized to use cloud services.

You can grant users permissions by using roles and policies.

- Roles: a type of coarse-grained authorization mechanism that defines service-level permissions based on user responsibilities. There are only a limited number of roles for granting permissions to users. If one role has a dependency role required for accessing CFW, assign both roles to the users.

Roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: Policy-based permission management is a type of fine-grained authorization mechanism that grants permissions to perform operations on specific cloud resources. This mechanism allows for more flexible policy-based authorization and secure access control. For example, you can grant HSS users only the permissions for managing a certain type of resources.

Table 7-1 describes the system roles of CFW.

Table 7-1 System policies supported by CFW

Role Name	Description	Category	Dependency
CFW FullAccess	All permissions for CFW	System-defined policy	None
CFW ReadOnlyAccess	Read-only permissions for CFW	System-defined policy	None

CFW FullAccess Policy Content

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "cfw:*:*",
            "vpc:publicIps:list",
            "vpc:publicipTags:get",
            "vpc:vpcs:create",
            "vpc:vpcs:list",
            "vpc:vpcs:get",
            "vpc:subnets:get",
            "vpc:subnets:create",
            "vpc:routeTables:list",
            "vpc:routeTables:update",
            "vpc:quotas:list",
            "er:instances:list",
            "er:attachments:list",
            "er:attachments:create",
            "er:routeTables:list",
            "er:routes:list",
            "er:associations:list",
            "er:instances:get",
            "ecs:cloudServers:list",
            "ecs:availabilityZones:list",
            "smn:topic:list",
            "nat:natGateways:list",
            "lts:groups:list",
            "lts:topics:get",
            "dcaas:vgw:list",
            "eps:resources:list",
            "tms:predefineTags:list"
         ],
         "Effect": "Allow"
      }
   ]
}
```


CFW ReadOnlyAccess Policy Content

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "cfw:*:list",
            "cfw:*:get",
            "vpc:publicIps:list",
            "vpc:publicipTags:get",
            "vpc:vpcs:list",
            "vpc:vpcs:get",
            "vpc:subnets:get",
            "vpc:routeTables:list",
            "vpc:quotas:list",
            "er:instances:list",
            "er:attachments:list",
           "er:routeTables:list",
           "er:routeTables:list",
           "er:routes:list",
           "er:associations:list",
           "er:instances:get",
            "ecs:cloudServers:list",
            "ecs:availabilityZones:list",
            "smn:topic:list",
            "nat:natGateways:list",
            "lts:groups:list",
            "lts:topics:get",
            "dcaas:vgw:list",
            "eps:resources:list",
            "tms:predefineTags:list"
         ],
         "Effect": "Allow"
      }
   ]
}
```

Special Permission Policy

Certain CFW functions depend on cloud services such as Elastic Cloud Server (ECS) and Virtual Private Cloud (VPC). Some functions of these cloud services do not support enterprise projects, so some permissions may become invalid after the **CFW FullAccess** and **CFW ReadOnlyAccess** system policies are granted to enterprise projects.

To avoid this problem, log in to your Huawei Cloud account to create two system policies. For details, see **Creating Custom Policies**.

- For the cloud services that CFW depends on, if they do not support enterprise projects, add the following content to grant permissions to them. For Log Tank Service (LTS), grant all permissions to it on the CFW page.

  ```
  {
     "Version": "1.1",
     "Statement": [
        {
           "Effect": "Allow",
           "Action": [
              "vpc:quotas:list",
              "vpc:publicipTags:get"
           ]
        },
        {
           "Effect": "Allow",
  ```



```
            "Action": [
                "ecs:availabilityZones:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lts:groups:list",
                "lts:groups:get",
            ]
        }
    ]
}
```

- CFW depends on the following global service permissions:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "eps:resources:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "tms:predefineTags:list"
            ]
        }
    ]
}
```


8 Constraints and Limitations

This topic describes some limitations and constraints on using CFW.

CFW Usage Restrictions

- Only the services deployed on Huawei Cloud can be protected. Cross-cloud access is not supported.
- Traffic protection supports EIPs, but does not support global EIPs or the EIPs bound to API Gateway.
- CFW can be used only in the region where it was purchased. To use it in another region, switch to that region and purchase it. For details about the regions where CFW is available, see **Function Overview**.
- VPC border protection depends on the enterprise router for traffic diversion. To use this function, ensure your account has at least one enterprise router.
- CFW does not support Chinese domain names.

Protection Policy Quota Limit

- Protection rules

  A maximum of 20,000 protection rules can be added to a firewall instance.
- Blacklist/Whitelist
  - A maximum of 2000 blacklist items can be added to a firewall instance.
  - A maximum of 2000 whitelist items can be added to a firewall instance.
- Groups
  - IP address groups
    - A firewall instance can have up to 3800 IP address groups.
    - An IP address group can contain up to 640 IP addresses.
    - A firewall instance can contain up to 30,000 IP addresses.
  - Service groups
    - A firewall instance can have up to 900 services.
    - A firewall instance can have up to 512 service groups.

    - A service group can have up to 64 services.
  - Domain name groups
    - The domain names in a domain name group can be referenced by protection rules for up to 40,000 times, and wildcard domain names can be referenced for up to 200 times.
    - **Application domain name group (layer 7 protocol parsing)**
      - A firewall instance can have up to 500 domain name groups.
      - A firewall instance can have up to 2,500 domain names.
      - A domain name group can have up to 1,500 domain names.
    - **Network domain name group (layer 4 protocol parsing)**
      - A firewall instance can have up to 1,000 domain names.
      - A network domain name group can have up to 15 domain names.
      - Each domain name group can resolve up to 1,500 IP addresses.
      - Each domain name can resolve up to 1,000 IP addresses.

Restrictions on Basic IPS

- Modifying the action of a basic protection rule
  - The actions of up to 3000 rules can be manually changed to observation.
  - The actions of up to 3000 rules can be manually changed to interception.
  - The actions of up to 128 rules can be manually changed to disabling.
- Custom IPS signature
  - Only the professional edition supports custom IPS signatures.
  - A maximum of 500 features can be added.

Restrictions on Logs

- CFW allows you to view log data of the last seven days. One or multiple types of logs can be recorded in LTS. You can view log data in the past 1 to 365 days.
- Up to 100,000 records can be exported for a single log at a time.

9 Related Services

IAM

Identity and Access Management (IAM) provides the permission management function for CFW. Only users who have Tenant Administrator permissions can perform operations such as authorizing, managing, and detect cloud assets using CFW. To obtain the permissions, contact the users who have the Security Administrator permissions.

EIP

Elastic IP (EIP) provides independent public IP addresses and bandwidth for Internet access.

CFW protects Internet border traffic by protecting EIPs.

VPC

Virtual Private Cloud (VPC) enables you to provision an isolated, private virtual network for cloud resources, such as cloud servers, containers, and databases.

CFW can protect traffic at VPC borders, such as between VPCs, or between a VPC on the cloud and an on-premises data center.

NAT Gateway

NAT Gateway provides public and private NAT gateways. A public NAT gateway provides SNAT and DNAT to let cloud servers in a VPC use an EIP to communicate with the Internet.

CFW protects the NAT gateway traffic by protecting the VPC where the NAT gateway resides.

Enterprise Router

Enterprise Router provides inter-VPC traffic diversion for CFW. If you purchase the professional edition to protect inter-VPC traffic or Direct Connect traffic, you need to use Enterprise Router to divert traffic.

CTS

Cloud Trace Service (CTS) generates traces to enable you to get a history of operations performed on CFW, 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 CFW, facilitating your further queries, audits, and retrievals.

Cloud Eye

Cloud Eye provides a comprehensive monitoring platform for resources such as the ECS and bandwidth. Cloud Eye monitors the metrics of CFW, so that you can understand the protection status of the service in a timely manner, and set protection policies accordingly.

LTS

Log Tank Service (LTS) collects log data from servers and cloud services. CFW can record attack event logs, access control logs, and traffic logs to LTS, enabling real-time, efficient, and secure log processing.

SMN

Simple Message Notification (SMN) provides the message notification function. After you enable notification on CFW, you will receive alarms based on the notification mode you configured if your resources are attacked or the protection traffic exceeds your quota.

Enterprise Management

You can manage multiple projects in an enterprise, separately settle their costs, and assign them to different personnel. 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.

CFW can be interconnected with Enterprise Management. You can manage CFW resources by enterprise project and grant different permissions to users.

Differences from WAF

CFW and WAF are two different Huawei Cloud products that can be used to protect your Internet borders, VPC borders, and web services.

The following table describes the differences between CFW and WAF.

Table 9-1 Differences between CFW and WAF

Item	CFW	WAF
Definition	Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects the Internet border and VPC border on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. It employs AI for intelligent defense, and can be elastically scaled to meet changing business needs, helping you easily handle security threats. CFW is a basic service that provides network security protection for user services on the cloud.	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). For details about WAF, see **What Is Web Application Firewall?**
Protection	• EIP border and VPC border • Basic protection against web attacks • Defense against external intrusions and protection of proactive connections to external systems	• WAF protects web applications on Huawei Cloud and other clouds and on-premises applications through domain names or IP addresses. • Comprehensive protection against web attacks
Features	• Asset management and intrusion defense: It detects and defends against intrusions into cloud assets that are accessible over the Internet in real time. • Access control: You can control access at Internet borders. • Traffic Analysis and log audit: CFW controls, analyzes, and visualizes VPC traffic, audits logs, and traces traffic sources.	WAF identifies and blocks a wide range of suspicious attacks, such as SQL injections, XSS attacks, web shell upload, command or code injections, file inclusion, unauthorized sensitive file access, third-party vulnerability exploits, CC attacks, malicious crawlers, and CSRF.

10 Basic Concepts

5-tuple

A 5-tuple (or quintuple) consists of a source IP address, a destination IP address, a protocol, a source port, and a destination port.

Protected Traffic

Inbound traffic is the traffic transferred from the Internet to CFW. For example, the traffic for downloading resources from the public network to servers in the cloud is the inbound traffic.

Outbound traffic is the traffic transferred from CFW to the Internet. For example, servers on the cloud provide services for external users, the traffic used by external users for downloading resources from the cloud is outbound traffic.

Protection bandwidth: bandwidth of all services protected by CFW.

Protected bandwidth at the Internet border: the maximum inbound or outbound traffic of all EIPs protected by CFW.

Protected bandwidth at the VPC border: the maximum total traffic of all VPCs protected by CFW.

Internet Border Firewall

Internet border firewalls check communication traffic (north-south traffic) between cloud assets and the Internet. They support intrusion prevention system (IPS) and antivirus functions by protecting EIPs. For details, see **Enabling Internet Border Traffic Protection**.

VPC Border Firewall

A VPC border firewall checks east-west traffic between two VPCs, visualizing and protecting internal service access. For details, see **Enabling VPC Border Traffic Protection**.

IPS

An intrusion prevention system (IPS) is located between a firewall and a network device. If an attack is detected, the IPS blocks malicious traffic before the attack

spreads to other parts of the network. For details about IPS, see **Attack Defense Overview**.

Antivirus

Anti-virus uses virus signature detection to identify and handle malware files, preventing data damages, permission changes, and system breakdown caused by malware files. For details, see **Blocking Virus-Infected Files**.

Internet Access

Internet access refers to the access from Internet IP addresses to cloud servers. Internet access protection helps you defend against intrusions from the outside in a timely manner.

Server Originated Access

Server originated access refers to the behavior that a cloud server proactively accesses an external IP address. Server originated access protection helps you manage and control outbound access behaviors.

Enterprise Router

An enterprise router is a central router that interconnects all of your VPCs and on-premises networks.

CFW-associated Subnet

This is a parameter that can be configured for a VPC border firewall. After a CIDR block is configured, a CFW-associated subnet is automatically allocated to forward traffic from the firewall to an enterprise router.

CVE ID

A Common Vulnerabilities and Exposures (CVE) ID is the unique identifier of a vulnerability.

CVE is a list of security vulnerabilities. Each entry in the list has a unique CVE ID.

Inspection VPC

An inspection VPC is used for a VPC border firewall to divert traffic. After a CIDR block is configured, CFW creates an inspection VPC by default. In enterprise router mode, the inspection VPC diverts traffic between the enterprise router and the firewall.

