Cloud Firewall

Service Overview

Issue 03

Date 2023-03-30

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 Internet and VPC borders on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. CFW employs AI for intelligent defense, and can be elastically scaled to meet changing business needs, helping you easily handle security threats. CFW provides basic network security protection for your workload 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, phishing, and brute-force attacks.

High Scalability

CFW can implement fine-grained traffic control on Internet borders, between VPCs, and between ECSs, preventing intrusions, internal penetration attacks, and unauthorized access from inside your network to the Internet. The CFW cluster is deployed in high availability mode. You can increase your bandwidth, EIPs, and security policies without limit, safeguarding your network even 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 block mode. In block mode, CFW detects and blocks traffic that matches the IPS rules. For details, see **Adding a Protection Rule**.
- ACL access control policies set for IP address groups, blacklists, and whitelists

2 Features

Cloud Firewall (CFW) comes in the standard edition, and professional edition. On the CFW console, you can check CFW status, access control, intrusion prevention, traffic analysis, and log audit statistics.

Table 2-1 Features

Item	Description
Dashboard	You can check enabled and disabled firewalls.
Assets	You can check and manage EIPs.
Access Control	You can control access at Internet and VPC borders.
Intrusion Prevention	You can detect and prevent against intrusions from Internet traffic by selecting a protection mode and determining whether to enable basic protection. Basic protection includes threat detection and vulnerability scanning. • Detects whether traffic contains phishing, Trojan horses, worms, hacker tools, spyware, password attacks, vulnerability attacks, SQL injection attacks, XSS attacks, and web attacks. • Checks whether there are protocol anomalies, buffer overflow, access control, suspicious DNS activities, and other suspicious behaviors in traffic.
Traffic Analysis	You can check the following statistics: • Internet access traffic in the last hour, last 24 hours, and last 7 days • Inter-VPC service traffic statistics in the last hour, last 24 hours, and last 7 days • Intrusion events in the last hour, last 24 hours, and last 7 days

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 Log Tank Service (LTS) on Huawei Cloud to record all CFW logs, including attack event, access control, and traffic logs.
System Management	Alarm notification: You can use CFW to set notifications for attack logs and traffic threshold-crossing warnings. After the alarm notification function is enabled, the CFW sends IPS attack logs and traffic threshold-crossing warnings to users through emails or SMS messages.

Table 2-2 In-path engine

Engine	Function	Protocol	Scenario
In-path engine	The firewall in-path engine completes security detection and protection for user traffic and then sends the traffic to the target ECS. This engine provides various detection functions and flexible blocking policies.	TCP, UDP, ICMP, Any, and ICMPv6	Protection for Internet borders

3 Editions

Cloud Firewall (CFW) comes in the standard edition, and professional edition. On the CFW console, you can check CFW status, access control, intrusion prevention, traffic analysis, and log audit statistics.

For details about their functions, see **Features**.

Table 3-1 lists the differences between these editions.

NOTE

Description:

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

Table 3-1 Editions

Feature	Standard	Professional
Protected EIPs at Internet boundary	20 (expandable)	50 (expandable)
Peak protection traffic at Internet boundary	10 Mbit/s (expandable)	50 Mbit/s (expandable)
Protected VPCs	×	2 (expandable)
Max. peak protection traffic between VPCs	×	200 Mbit/s
Northbound and southbound traffic audit and attack log query	√	√
Northbound and southbound traffic protection and cloud resources (including EIPs) protection against risks on the Internet	√	√
ACL management for public network resources based on IP addresses, domain names, or applications	√	√

Feature	Standard	Professional
Network traffic analysis and abnormal inbound and outbound traffic detection	√	√
Network intrusion prevention system	√	√
Eastbound and westbound traffic protection, resource protection between VPCs, access control, traffic analysis, and intrusion prevention	×	√

4 Scenarios

Constraint

- The CFW ALG tag function is restricted.
- By default, the network-layer defense against DDoS attacks and IP spoofing is disabled on CFW.
- Domain name protection depends on the DNS server you configure. The IP address of a default server may be incorrectly resolved. You are advised to use a custom server.
- To use CFW persistent connections, enable a bidirectional out-of-path policy. If you only enable a unidirectional policy, the client will need to re-initiate connections in certain scenarios, such as enabling or disabling protection, and expanding engine capacities. You are advised to submit a service ticket for risks assessment.

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.

5 Security

5.1 Shared Responsibilities

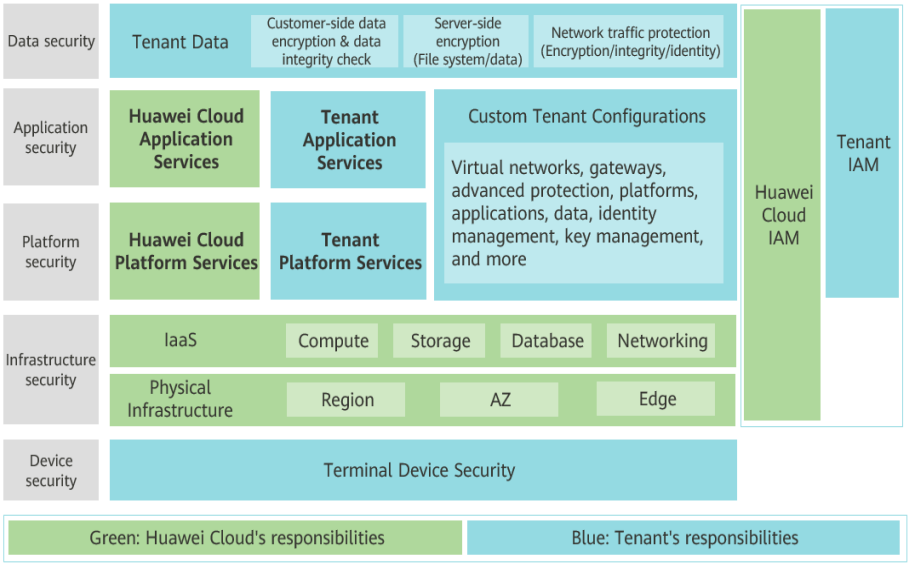
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 5-1 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 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 5-1 Huawei Cloud shared security responsibility model



5.2 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**.

5.3 Data Protection Technologies

CFW takes different measures to keep data secure and reliable.

Table 5-1 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**.

5.4 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.

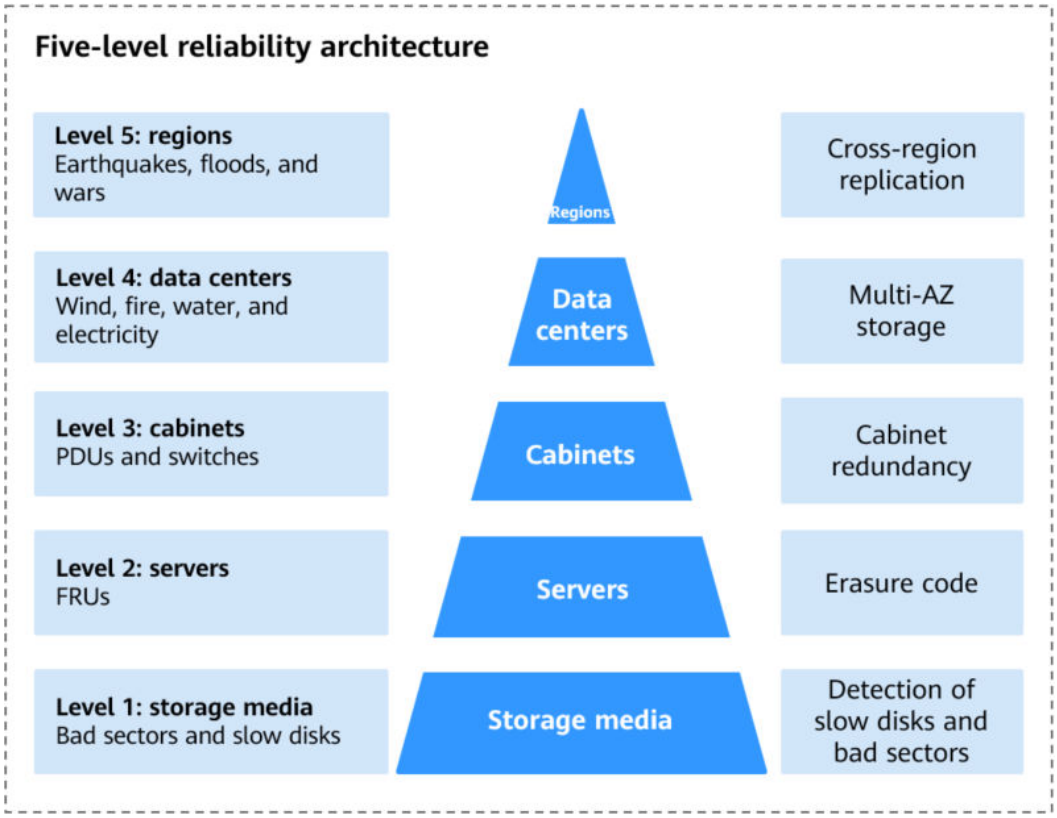
For details, see **What Is Cloud Trace Service?**

5.5 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**.



5.6 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.

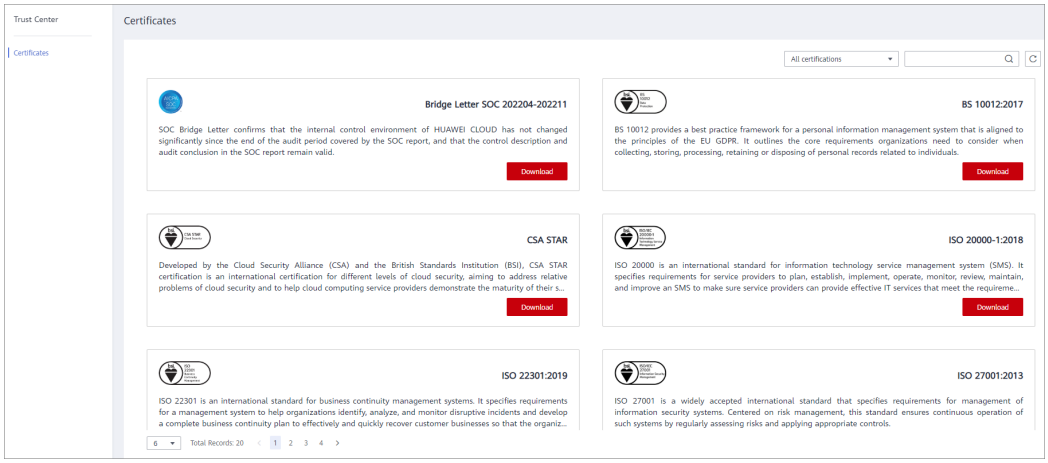
- For details about what is Cloud Eye and how to use it, see **Overview**.
- For details about how to use Cloud Eye to monitor CFW, see **Configuring Alarm Monitoring Rules**.

5.7 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.

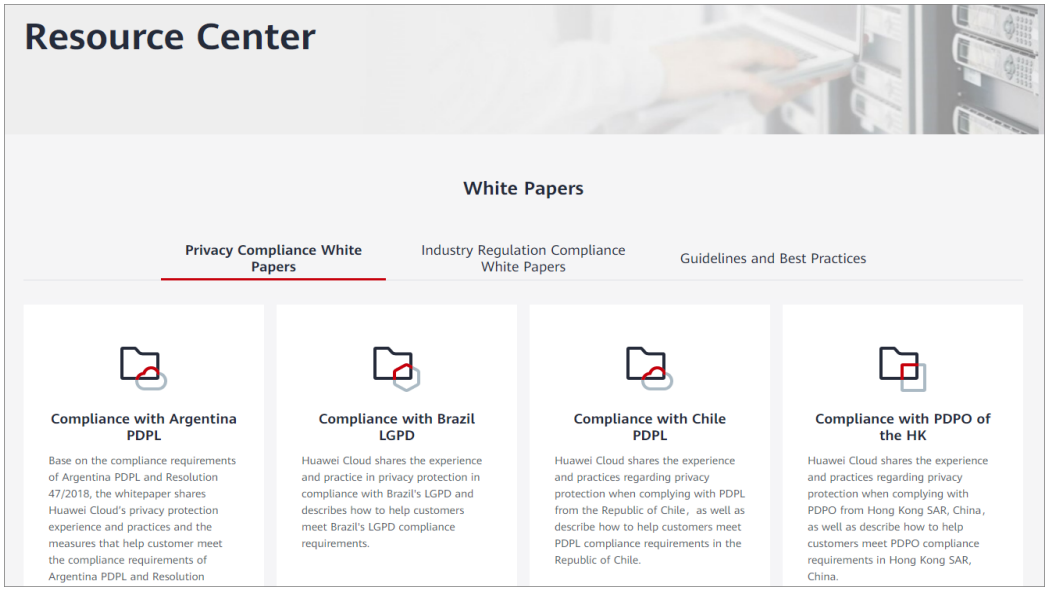
Figure 5-2 Downloading compliance certificates



Resource Center

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

Figure 5-3 Resource center



6 Billing

The CFW **standard** edition and **professional** edition can be purchased in prepaid yearly/monthly mode. For details, see **Pricing**.

Billing Items

CFW is billed based on the edition, service duration, and specifications you purchase.

Table 6-1 CFW billing

Edition	Billing Mode	Billing Item	Billing
Standard	Yearly/ Monthly	Required Duration	Billed on a yearly or monthly basis
		(Optional) Protected EIPs	Billed based on the purchased quantity
		(Optional) Peak Protection Traffic at Internet Boundary	Billed based on the purchased traffic
Professional	Yearly/ Monthly	Required Duration	Billed on a yearly or monthly basis
		(Optional) Protected EIPs	Billed based on the purchased quantity
		(Optional) Peak Protection Traffic at Internet Boundary	Billed based on the purchased traffic
		(Optional) Protected VPCs	Billed based on the purchased quantity

Billing Mode

If you choose the yearly/monthly billing mode, the longer duration you purchase, the more you save. In yearly/monthly mode, you are billed based on the purchase period specified in the order.

Configuration Changes

- Changing the edition
  - In-path engine: You can upgrade the CFW from the standard edition to the professional edition by changing specifications. You can also increase the number of protected EIPs, peak Internet traffic, and protected VPCs based on service requirements.
- Unsubscribing from CFW

  To stop using CFW, go to the Billing Center and **unsubscribe** from it.

Renewal

- After your CFW expires, there is a retention period for you.

  This period varies depending on your account. For details, see **Retention Period**.
- You can go to the management console to renew your subscription. For details, see **Renewal Management**.

Expiration and Overdue Payment

- Expiration

  If you do not renew CFW after it expires, your resources will enter a retention period. The retention period length depends on your account. After this period ends, your resources will be automatically deleted and cannot be restored, and the service cannot be renewed. For details, see **Retention Period**.
- Overdue payment

  If your account is in arrears, you can view the arrears details. You need to pay the arrears within the specified period. To prevent services from being stopped, top up your account in a timely manner. For details, see **Repaying Arrears**.

7 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.

Border Firewall

Edge Firewall (EdgeFW) is a bridge connecting the internal network and the external network. EdgeFW provides border security protection for the north-south traffic between the cloud data center and external networks, and supports intrusion prevention system (IPS) and network antivirus (AV) functions based on elastic IP addresses.

What Is 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.

What Is 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.

8 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 is free. 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 8-1 describes the system roles of CFW.

Table 8-1 System policies supported by CFW

Role Name	Description	Category	Dependency
CFW FullAccess	Full 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": [{
        "Effect": "Allow",
        "Action": [
            "cfw:*:*",
            "vpc:publicIps:list"
        ]
    }]
}
```

CFW ReadOnlyAccess Policy Content

```
{
  "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "cfw:*:list",
            "cfw:*:get",
            "vpc:publicIps:list"
        ]
    }]
}
```


9 Relationship with Other Cloud 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.

Differences Between CFW and WAF

CFW and WAF are two different products launched by Huawei Cloud to protect your Internet borders, VPC borders, and web services.

Differences between CFW and WAF describes the detailed differences.

Table 9-1 Differences between CFW and WAF

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

Item	CFW	WAF
Protection	• EIP and VPC boundary • 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: CFW 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.

A Change History

Date	Description
2023-03-30	This is the third official release. Added information about the CFW professional edition.
2022-11-14	This is the second official release. Added **Security**.
2022-07-30	This is the first official release.

