Cloud Firewall

Getting Started

Issue	02
Date	2023-11-30

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.

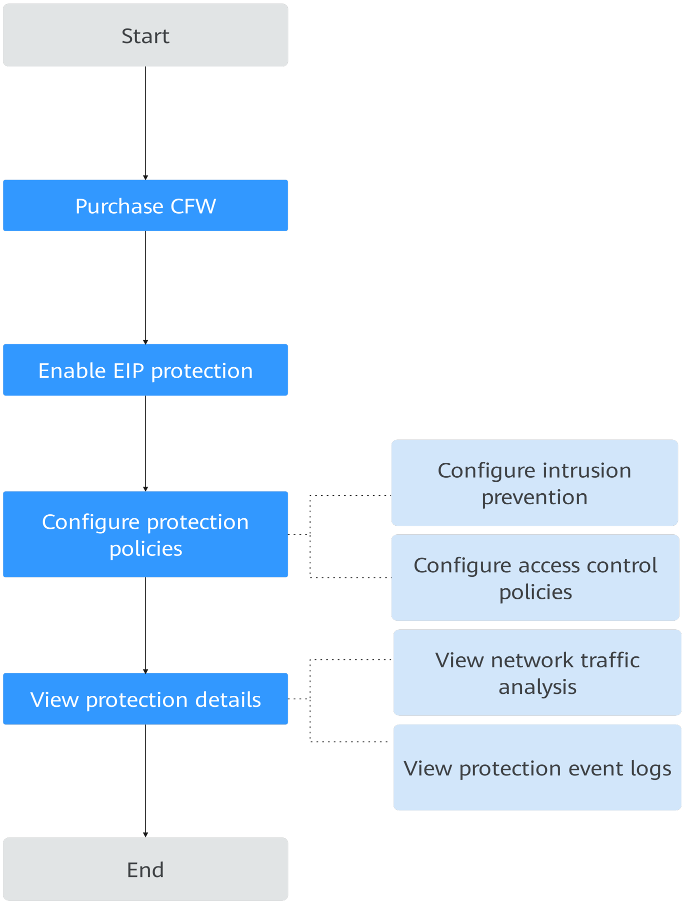
Contents

1 Overview

Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects Internet 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.

This document describes how to use CFW to protect the Internet border. The following figure shows **the process of using CFW**.

Figure 1-1 Process


Start
Purchase CFW
Enable EIP protection
Configure protection policies
Configure intrusion prevention
Configure access control policies
View protection details
View network traffic analysis
View protection event logs
End

2 Step 1: Purchase CFW

You can purchase CFW in yearly/monthly mode.

Edition Description

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

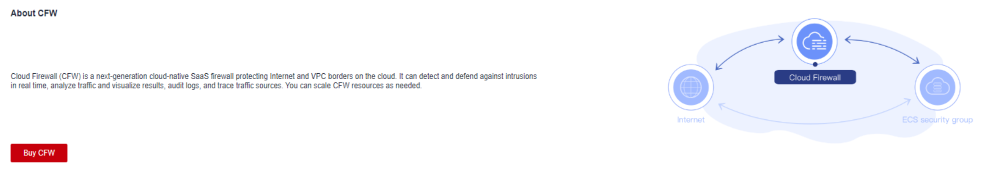
Procedure

Step 1 **Log in to the management console.**

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 2-1**.

Figure 2-1 CFW Dashboard

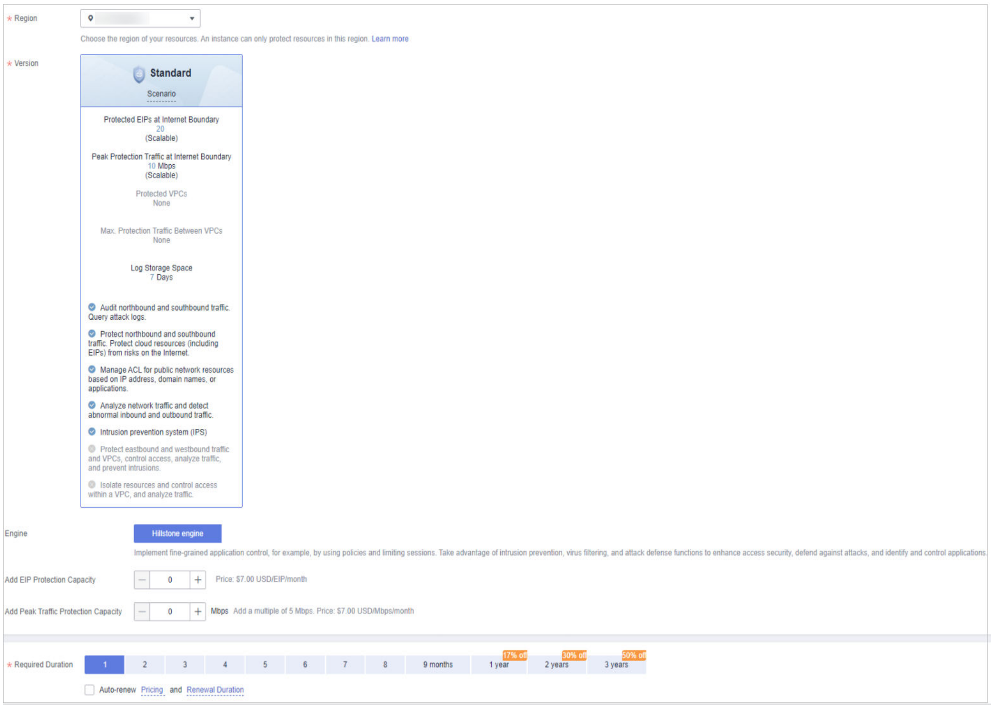


About CFW

Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Step 4 Click **Buy CFW** and configure parameters on the **Buy CFW** page. For more information, see **Table 2-1**.

Figure 2-2 Purchasing an CFW



* Region: [redacted]

Choose the region of your resources. An instance can only protect resources in this region. Learn more

* Version: Standard

Scenario

Protected EIPs at Internet Boundary
20
(Scalable)

Peak Protection Traffic at Internet Boundary
10 Mbps
(Scalable)

Protected VPCs
None

Max. Protection Traffic Between VPCs
None

Log Storage Space
7 Days

- Audit northbound and southbound traffic. Query attack logs.
- Protect northbound and southbound traffic. Protect cloud resources (including EIPs) from risks on the Internet.
- Manage ACL for public network resources based on IP address, domain names, or applications.
- Analyze network traffic and detect abnormal inbound and outbound traffic.
- Intrusion prevention system (IPS)
- Protect eastbound and westbound traffic and VPCs, control access, analyze traffic, and prevent intrusions.
- Isolate resources and control access within a VPC, and analyze traffic.

Engine: Hillstone engine

Implement fine-grained application control, for example, by using policies and limiting sessions. Take advantage of intrusion prevention, virus filtering, and attack defense functions to enhance access security, defend against attacks, and identify and control applications.

Add EIP Protection Capacity: 0 Price: $7.00 USD/EIP/month

Add Peak Traffic Protection Capacity: 0 Mbps Add a multiple of 5 Mbps. Price: $7.00 USD/Mbps/month

* Required Duration: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 months | 1 year (17% off) | 2 years (30% off) | 3 years (50% off)

□ Auto-renew Pricing and Renewal Duration

Table 2-1 CFW parameters

Parameter	Description
Region	Region where the CFW is to be purchased. **NOTICE** CFW can be used in the selected region only. To use CFW in another region, switch to the corresponding region and then purchase it. For details about the regions where CFW is available, see **Can CFW Be Used Across Clouds or Regions?**
Edition	Edition. ● Standard
Engine	Direct engine. You can implement fine-grained application control, for example, by using policies and limiting sessions. You can also take advantage of intrusion prevention, virus filtering, and defense functions to enhance access security, defend against attacks, and identify and control applications.
Add EIP Protection Capacity	(Optional) Number of additional EIPs to be protected. Value range: 0 to 2000 **NOTE** By default, 20 public IP addresses are protected by the standard edition (included in the package fee). If you have 65 public IP addresses, you only need to enter 45.

Parameter	Description
Add Peak Traffic Protection Capacity	(Optional) Additional peak inbound or outbound traffic. The value range is 0 to 2000 Mbit/s per month. (The value must be an integer multiple of 5.) **NOTE** ● By default, up to 10 Mbit/s per month is protected by the standard edition (included in the package fee). If your protection traffic is 200 Mbit/s per month, you only need to enter 190 Mbit/s per month. ● The protection traffic is determined based on the maximum inbound or outbound traffic, whichever is higher.
Enterprise Project	Select an enterprise project from the drop-down list. This option is only available if you have logged in using an enterprise account, or if you have enabled enterprise projects. To use this function, **Enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by project. **NOTE** Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project.
Firewall Name	Firewall name. It must meet the following requirements: ● Only letters (A to Z and a to z), numbers (0 to 9), spaces, and the following characters are allowed: -_ ● The value can contain 1 to 48 characters.
Advanced Settings	**Tag**: You can use a tag for multiple cloud resources. You are advised to predefine tags in TMS. For details, see **Resource Tag Overview**.
Required Duration	Service duration. After selecting a duration, you can select **Auto-renew**. If you select and agree to service auto renewal, the system automatically generates a renewal order based on the subscription period and renews the service before it expires. Note the **Auto-Renewal Rules** when enabling auto-renewal.

Step 5 Confirm the purchase information and click **Buy Now**.

Step 6 Confirm the order details, select **I have read and agreed to the Huawei Cloud Firewall Service Statement**, and click **Next**.

Step 7 Select a payment method and pay for your order.

----End

Effective Conditions

Your CFW instance is purchased when your instance edition and its quota information are shown in the upper right corner of the management console.

3 Step 2: Enable EIP Protection

When you use CFW for the first time, you need to synchronize assets and enable protection for EIP assets so that your service traffic can pass through CFW.

After EIP protection is enabled, the default action of CFW is **Allow**. CFW will block traffic based on your protection policy.

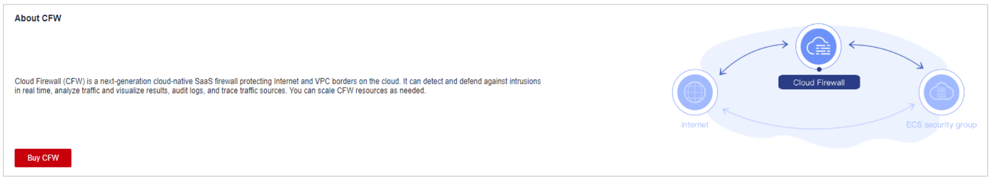
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 3-1**.

Figure 3-1 CFW Dashboard



About CFW

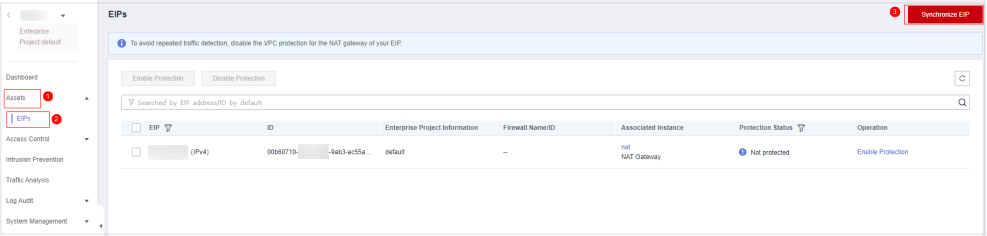
Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Assets** > **EIPs**. The EIP page is displayed. The EIP information is automatically updated to the list. See **Figure 3-2**.

(Optional) Manually refresh the list. Click **Synchronize EIP** in the upper right corner of the page to import your EIP information to the list and refresh the EIP list.

Figure 3-2 EIPs



To avoid repeated traffic detection, disable the VPC protection for the NAT gateway of your EIP.

EIP	ID	Enterprise Project Information	Firewall Name/ID	Associated Instance	Protection Status	Operation
[redacted] (IPv4)	00b60710-[redacted]-9ab3-ac55a...	default	--	nat NAT Gateway	Not protected	Enable Protection

NOTICE

Currently, IPv6 addresses cannot be protected.

Step 6 Enable EIP protection.

- Enable protection for a single EIP. In the row of the EIP, click **Enable Protection** in the **Operation** column.
- Enable protection for multiple EIPs. Select the EIPs to be protected and click **Enable Protection** above the table.

Step 7 On the page that is displayed, check the information and click **Bind and Enable**. Then the **Protection Status** changes to **Protected**.

NOTE

After EIP protection is enabled, the default access control policy is **Allow**.

----End

4 Step 3: Configure a Protection Policy

4.1 Configuring Intrusion Prevention

CFW provides you with basic defense 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.

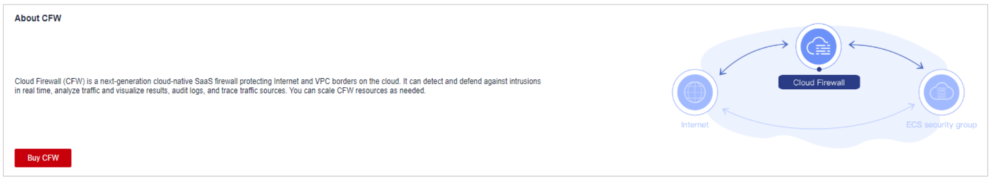
Procedure

Step 1 **Log in to the management console.**

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 4-1**.

Figure 4-1 CFW Dashboard



About CFW

Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Attack Defense** > **Intrusion Prevention**.

Table 4-1 Intrusion prevention functions

Function	Description
Protection Mode	● **Observe**: Attacks are detected and recorded in logs. ● **Intercept**: Attacks and abnormal IP address access are automatically intercepted. – **Intercept mode - loose**: The protection granularity is coarse. In this mode, only attacks with high threat and high certainty are blocked. – **Intercept mode - moderate**: The protection granularity is medium. This mode meets protection requirements in most scenarios. – **Intercept mode - strict**: The protection granularity is fine-grained, and all attack requests are intercepted. You are advised to configure false alarm masking rules after the service has been running for a period of time, then enable the **strict** mode. **NOTE** After selecting a protection mode, you can modify a rule in the basic protection rule library. For details, see "Basic Protection Rule Management" in *Cloud Firewall User Guide*.
Basic Protection	Basic protection on your assets. It is enabled by default. Its functions are as follows: ● Scan for threats and scan vulnerabilities. ● 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.
Virtual Patching	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.

Function		Description
Advanced	Sensitive Directory Scan Defense	Defense against scan attacks on sensitive directories on your servers. **Action**: ● **Observe**: If a sensitive directory scanning attack is detected, CFW records it in logs only. For details about how to view attack logs, see Cloud Firewall User Guide > Log Query. ● **Block session**: If the firewall detects a sensitive directory scan attack, it blocks the current session. ● **Block IP**: If CFW detects a sensitive directory scan attack, it blocks the attack IP address for a period of time. **Duration**: If **Action** is set to **Block IP**, you can set the blocking duration. The value range is 60s to 3,600s. **Threshold**: CFW performs the specified action if the scan frequency of a sensitive directory reaches this threshold.
	Reverse Shell Defense	Defense against reverse shells. **Action**: ● **Observe**: If a reverse shell attack is detected, it is only recorded in attack logs. For details about how to view attack logs, see "Querying Logs" in *Cloud Firewall User Guide*. ● **Block session**: If the firewall detects a reverse shell attack, it blocks the current session. ● **Block IP**: If CFW detects a reverse shell attack, it blocks the attack IP address for a period of time. **Duration**: If **Action** is set to **Block IP**, you can set the blocking duration. The value range is 60s to 3,600s. **Mode**: ● **Conservative**: coarse-grained protection. It observes or blocks frequent attacks, ensuring that no false positives are reported. ● **Sensitive**: fine-grained protection. It ensures that attacks can be detected and handled.

----End

4.2 Configuring an Access Control Policy

The default status of the access control policy is **Allow**. Configure a proper access control policy for fine-grained management and control, preventing the spread of internal threats and enhancing security. For details about how to configure the access control policy, see **Adding an Internet Boundary Protection Rule**. . .

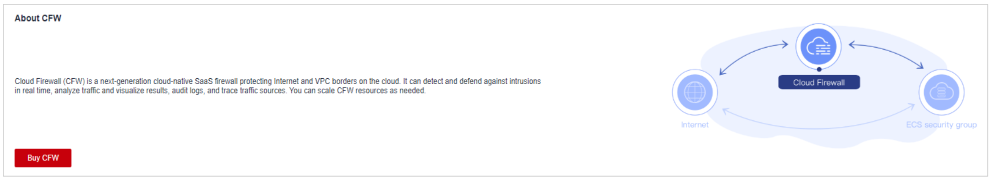
Adding an Internet Boundary Protection Rule

Step 1 **Log in to the management console.**

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 4-2**.

Figure 4-2 CFW Dashboard



About CFW

Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Access Control** > **Access Policies**.

Step 6 Add a protection rule.

Click **Add Rule**. In the displayed dialog box, enter new protection information. For details, see **Table 4-2**.

Table 4-2 Internet boundary rule parameters

Parameter	Description	Example Value
Name	Rule name.	test
Direction	Select a traffic direction. ● **Inbound**: Traffic from external networks to the internal server. ● **Outbound**: Traffic from internal servers to external networks.	Inbound

Parameter	Description	Example Value
Source	Source address of access traffic. ● **IP address** can be configured in the following formats: – A single IP address, for example, **192.168.10.5** – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** – Address segment, for example, **192.168.2.0/24** ● **IP address group**: A collection of IP addresses. For more information, see **Adding an IP Address Group**. ● **Countries and regions**: If **Direction** is set to **Inbound**, you can control access based on continents, countries, and regions. ● **Any**: any source address	**IP address, 192.168.10.5**
Destination	Destination address of access traffic. ● **IP address**: You can set a single IP address, consecutive IP addresses, or an IP address segment. – A single IP address, for example, **192.168.10.5** – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** – Address segment, for example, **192.168.2.0/24** ● **IP address group**: A collection of IP addresses. For details, see **Adding an IP Address Group**. ● **Countries and regions**: If **Direction** is set to **Outbound**, you can control access based on continents, countries, and regions. ● **Domain name**: If **Direction** is set to **Outbound**, you can enter a multi-level single domain name (for example, top-level domain name **example.com** and level-2 domain name **www.example.com**) or a wildcard domain name (***.example.com**). **NOTE** – Click **Test** to check the validity of the domain name and perform DNS resolution. For details, see **Configuring DNS Resolution**. (Currently, up to 600 IP addresses can be resolved from a domain name.) ● **Domain name group**: If **Direction** is set to **Outbound**, a collection of multiple domain names is supported. **NOTE** To protect a domain name, you are advised to configure a domain name group. ● **Any**: any destination address	Any

Parameter	Description	Example Value
Service	Set the protocol type and port number of the access traffic. ● **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol Type**: The value can be TCP, UDP, or ICMP. – **Source/Destination Port**: If **Protocol Type** is set to **TCP** or **UDP**, you need to set the port number. NOTE – To specify all the ports of an IP address, set **Port** to **1-65535**. – You can specify a single port. For example, to manage access on port 22, set **Port** to **22**. – To set a port range, use a hyphen (-) between the starting and ending ports. For example, to manage access on ports 80 to 443, set **Port** to **80-443**. ● **Service group**: A collection of services (protocols, source ports, and destination ports) are supported. For more information, see **Adding a Service Group**. ● **Any**: any protocol type or port number	**Service** **Protocol Type**: **TCP** **Source Port**: **80** **Destination Port**: **80-443**
Action	Set the action to be taken when traffic passes through the firewall. ● **Allow**: Traffic is forwarded. ● **Block**: Traffic is not forwarded.	Allow
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol Type** is set to **TCP** or **UDP**, you can configure the service session aging time. ● **Yes**: Configure the long connection duration. ● **No**: Retain the default durations. The default connection durations for different protocols are as follows: – TCP: 1800s – UDP: 60s NOTE Up to 100 rules can be configured with long connections.	Yes

Parameter	Description	Example Value
Long Connection Duration	This parameter is mandatory if **Allow Long Connection** is set to **Yes**. Configure the long connection duration. Configure the hour, minute, and second. **NOTE** The duration range is 1 second to 1000 days.	60 hours 60 minutes 60 seconds
Tags	(Optional) Tags are used to identify rules. You can use tags to classify and search for security policies.	-
Priority	Priority of the rule. Its value can be: ● **Pin on top**: indicates that the priority of the policy is set to the highest. ● **Lower than the selected rule**: indicates that the policy priority is lower than a specified rule. **NOTE** A smaller value indicates a higher priority.	Pin on top
Status	Whether a policy is enabled. ●: enabled ○: disabled	●
Description	(Optional) Usage and application scenario	-

Step 7 Click **OK**.

NOTE

After EIP protection is enabled, the default status of the access control policy is **Allow**. If you want to allow only several EIPs, you are advised to add a protection rule with the lowest priority to block all traffic.

----End

5 (Optional) Step 4: View Protection Details

5.1 Viewing Network Traffic Analysis

You can view details about the inbound and outbound traffic and attack trend on cloud servers in real time to check for abnormal traffic.

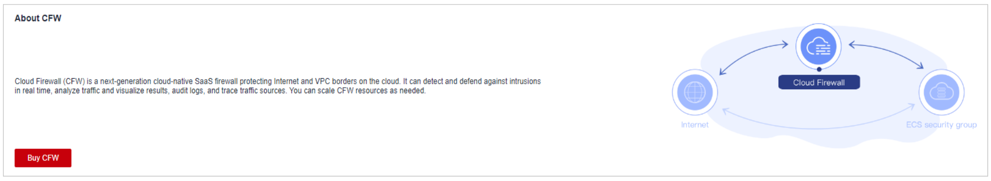
Viewing Inbound Traffic

Step 1 **Log in to the management console.**

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 5-1**.

Figure 5-1 CFW Dashboard



About CFW

Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Traffic Analysis** > **Inbound Traffic**.

Step 6 View the statistics on the traffic passing through the firewall. You can select the query duration from the drop-down list.

- **Traffic Dashboard**: Information about the highest traffic from the Internet to internal servers.

- **Inbound Traffic**: Inbound request and response traffic.
- **Visualizations**: Top 5 items ranked by certain parameters regarding inbound traffic within a specified time range. For more information, see **Table 5-1**. Click a record to view the traffic details.

Table 5-1 Inbound traffic parameters

Parameter	Description
Top Access Source IP Addresses	Source IP addresses of inbound traffic.
Top Access Source Regions	Geographical locations of the source IP addresses of inbound traffic.
Top Destination IP Addresses	Destination IP addresses of inbound traffic.
Top Open Ports	Destination ports of inbound traffic.
Application Distribution	Application information about inbound traffic.

- IP analysis: Top 50 traffic records in a specified period.
  - **EIPs**: Traffic information about destination IP addresses.
  - **Source IP Addresses**: Traffic information about source IP addresses.

----End

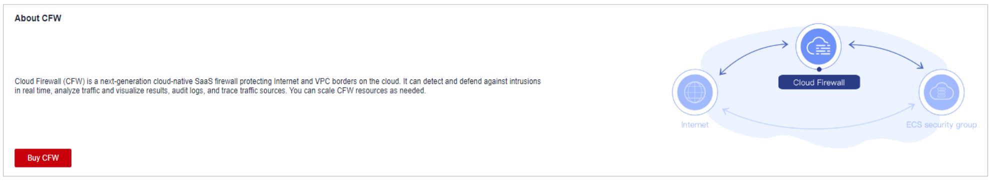
Viewing Outbound Traffic

Step 1 **Log in to the management console.**

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 5-2**.

Figure 5-2 CFW Dashboard



About CFW

Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Traffic Analysis** > **Outbound Traffic**.

Step 6 View the statistics on the traffic passing through the firewall. You can select the query duration from the drop-down list.

- **Traffic Dashboard**: Information about the highest traffic when internal servers access the Internet.
- **Outbound Traffic**: Outbound request and response traffic.
- **Visualizations**: Top 5 items ranked by certain parameters regarding outbound traffic within a specified time range. For more information, see **Table 5-2**. Click a record to view the traffic details.

Table 5-2 Outbound traffic parameters

Parameter	Description
Top Destination IP Addresses	Destination IP addresses of outbound traffic.
Top Destination Regions	Geographical locations of the source IP addresses of outbound traffic.
Top Access Source IP Addresses	Source IP addresses of outbound traffic.
Top Open Ports	Destination ports of outbound traffic.
Application Distribution	Application information about outbound traffic.

- IP analysis: Top 50 traffic records in a specified period.
  - **External IP Address**: Traffic information about the destination IP address.
  - **Assets Initiating Internet Connections**: Traffic information whose source IP addresses are public IP addresses.
  - **Assets Initiating Private Network Connections**: Traffic information whose source IP addresses are private IP addresses.

----End

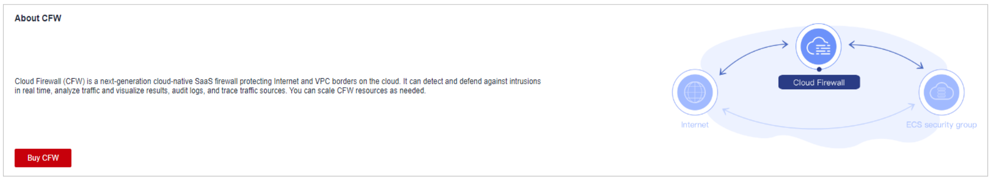
Procedure

Step 1 **Log in to the management console.**

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 5-3**.

Figure 5-3 CFW Dashboard



About CFW

Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Traffic Analysis**. On the displayed page, you can click the following tabs to view details:

- **Internet Access**: the total inbound and outbound Internet traffic, attack trend, and top 10 access IP addresses in different time ranges, as shown in **Internet access**. For more information, see **Internet access parameters**.
- **Server Originated Access**: the inbound and outbound traffic of server originated access and the attack trend in different time ranges, as shown in **Server originated access**. For more information, see **Server originated access parameters**.

Figure 5-4 Internet access

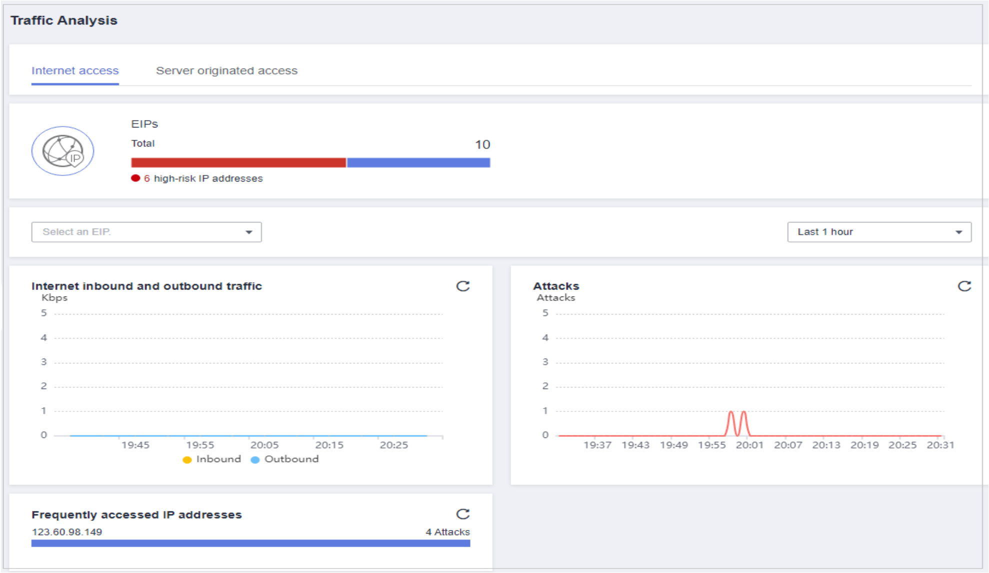


Figure 5-5 Server originated access

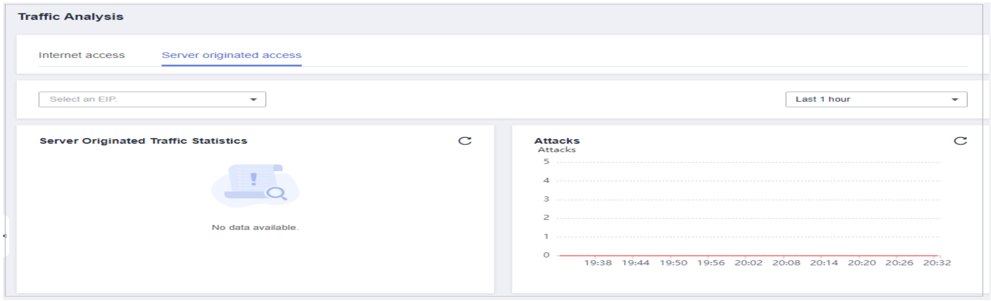


Table 5-3 Internet access parameters

Parameter	Description
EIPs	Total EIPs. They are categorized as follows: ● High-risk IP addresses are not protected and displayed in red. ● Protected IP addresses are displayed in blue.
Internet inbound and outbound traffic	Statistics on Internet inbound and outbound traffic
Attacks	Number of attacks at different time segments.
Frequently accessed IP addresses	Top 10 EIPs with the highest access rates detected by CFW.

Table 5-4 Server originated access parameters

Parameter	Description
Server Originated Traffic Statistics	Statistics on server originated traffic
Attacks	Number of attacks at different time segments.

----End

5.2 Viewing Protection Event Logs

For details about how to view attack traffic detected by the cloud firewall in attack logs, see **Attack Event Logs**.

You can also view all traffic allowed or blocked in access control logs to adjust access control policies. For details, see **Access Control Logs**.

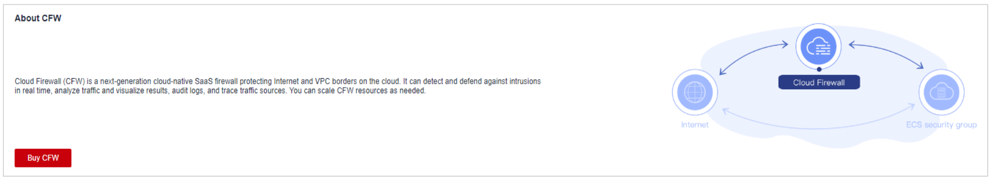
Attack Event Logs

Step 1 **Log in to the management console.**

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 5-6**.

Figure 5-6 CFW Dashboard



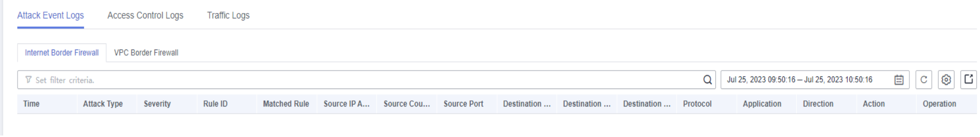
About CFW

Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Log Audit** > **Log Query**. The **Attack Event Logs** tab page is displayed. You can view details about attack events in the past week.

Figure 5-7 Attack event logs



Set filter criteria.

Jul 25, 2023 09:50:16 – Jul 25, 2023 10:50:16

Time	Attack Type	Severity	Rule ID	Matched Rule	Source IP A...	Source Cou...	Source Port	Destination ...	Destination ...	Destination ...	Protocol	Application	Direction	Action	Operation

Table 5-5 Attack event log parameters

Parameter	Description
Time	Time when an attack occurred.
Attack Type	Type of the attack event, including IMAP, DNS, FTP, HTTP, POP3, TCP, and UDP.
Severity	It can be **Critical**, **High**, **Medium**, or **Low**.
Rule ID	Rule ID
Matched Rule	Matched rule in the library.
Source IP Address	Source IP address of an attack event.
Source Country/ Region	Geographical location of the attack source IP address.
Source Port	Source port of an attack.
Destination IP Address	Attacked IP address.
Destination Country/ Region	Geographical location of the attack target IP address.
Destination Port	Destination port of an attack.
Protocol	Protocol type of an attack.
Application	Application type of an attack.
Direction	It can be outbound or inbound.
Action	Action taken on an event. It can be **Observe**, **Block**, or **Allow**.

Parameter	Description
Operation	You can click **Details** to view the basic information and attack payload of an event.

----End

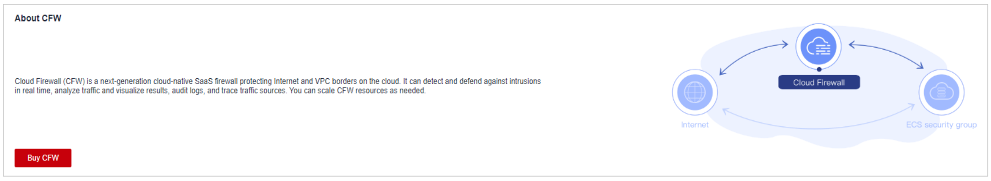
Access Control Logs

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in Figure 5-8.

Figure 5-8 CFW Dashboard



About CFW

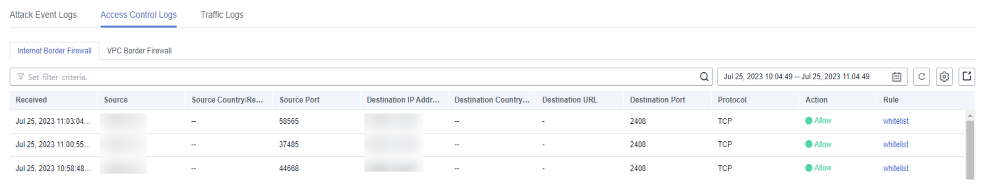
Cloud Firewall (CFW) is a next-generation cloud-native SaaS firewall protecting Internet and VPC borders on the cloud. It can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. You can scale CFW resources as needed.

Buy CFW

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Log Audit** > **Log Query**. Click the **Access Control Logs** tab and check the access control traffic details in the past week.

Figure 5-9 Access control logs



Attack Event Logs | Access Control Logs | Traffic Logs

Internet Border Firewall | VPC Border Firewall

Set filter criteria.

Jul 25, 2023 10:04:49 – Jul 25, 2023 11:04:49

Received	Source	Source Country/Re...	Source Port	Destination IP Addr...	Destination Country...	Destination URL	Destination Port	Protocol	Action	Rule
Jul 25, 2023 11:03:04...	[redacted]	--	58565	[redacted]	--	-	2408	TCP	● Allow	whitelist
Jul 25, 2023 11:00:55...	[redacted]	--	37485	[redacted]	--	-	2408	TCP	● Allow	whitelist
Jul 25, 2023 10:58:48...	[redacted]	--	44668	[redacted]	--	-	2408	TCP	● Allow	whitelist

Table 5-6 Access control log parameters

Parameter	Description
Received	Time of an access.
Source	Source IP address of the access.
Source Country/Region	Geographical location of the source IP address.

Parameter	Description
Source Port	Source port for access control. It can be a single port or consecutive port groups (example: **80-443**).
Destination IP Address	Destination IP address.
Destination Country/ Region	Geographical location of the destination IP address.
Destination URL	Destination domain name.
Destination Port	Destination port for access control. It can be a single port or consecutive port groups (example: **80-443**).
Protocol	Protocol type for access control.
Action	Action taken on an event. It can be **Observe**, **Block**, or **Allow**.
Rule	Type of an access control rule. It can be a blacklist or whitelist.

----End

6 Getting Started with Common Practices

After configuring intrusion prevention and access control policies, you can use a series of common practices provided by CFW for your workloads quickly.

Table 6-1 Common practices

Practice	Description
Configuring Access Policies for IP Address Groups and Service Groups	Configure IP address groups and service groups (ports and protocols) in batches. This policy applies to enterprises or multiple IP addresses or port protocols need to be configured.

A Change History

Released On	Change History
2023-11-30	This issue is the second official release. Optimized: Parameters on **Viewing Network Traffic Analysis**.
2023-07-21	This issue is the first official release.