

Cloud Firewall

Getting Started

Issue 03
Date 2024-12-02



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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.

Contents

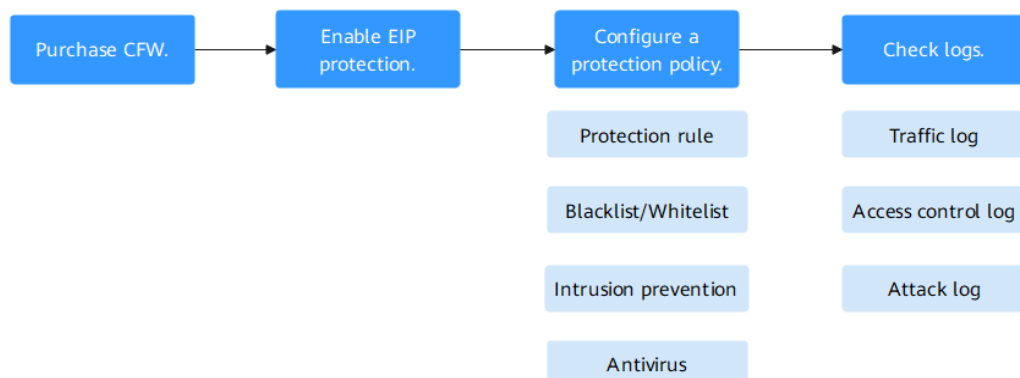
1 Overview.....	1
2 Configuring a Protection Rule to Allow the Inbound Traffic to a Specified EIP.....	6
3 Configuring Intrusion Prevention to Protect EIPs.....	11
4 Getting Started with Common Practices.....	16

1 Overview

Cloud Firewall (CFW) provides traffic protection for cloud services at the Internet border, VPC border, and NAT gateway.

This section describes the configuration processes in different scenarios.

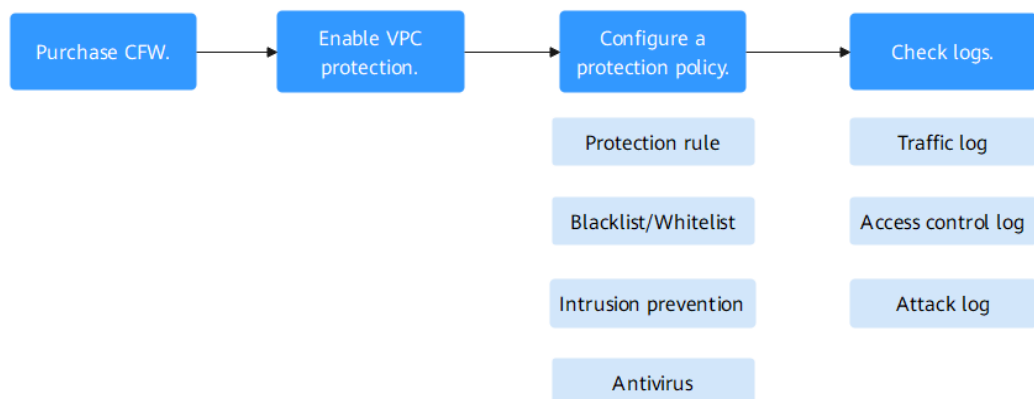
Internet Border Traffic Protection



Procedure	Description	Reference
Purchasing CFW	Purchase a CFW instance in the region where you want to protect traffic.	Purchasing CFW
Enabling EIP protection	Enable protection for one or more EIPs. CFW protects Internet border traffic by protecting EIPs.	Enabling EIP Protection

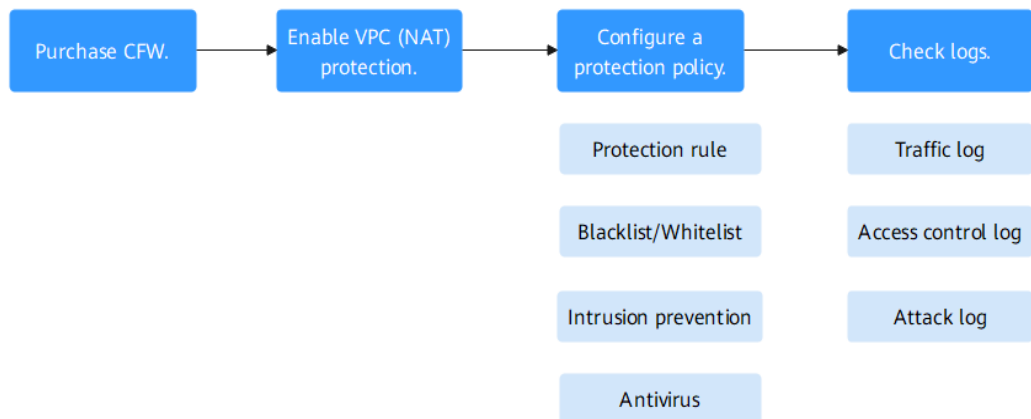
Procedure	Description	Reference
Configuring protection policies	<p>By default, CFW allows all traffic. You need to configure protection policies to protect traffic.</p> <p>The following protection policies are provided:</p> <ul style="list-style-type: none"> • Protection rules: You can set rules to control traffic by IP address, IP address group, region, or domain name. • Blacklist/Whitelist: Traffic is controlled based on specific rules configured for IP addresses and IP address groups. Traffic that matches the whitelist is directly allowed without being checked by other functions. • Intrusion prevention: Network attacks are blocked based on multiple IPS rule databases. • Antivirus: Virus-infected files are blocked based on protocol types. 	<p>Protection rules: Blacklist/Whitelist: Intrusion prevention: Antivirus:</p>
Checking logs	View the traffic protection outcomes in logs.	Viewing Logs
<p>Example scenarios:</p> <ul style="list-style-type: none"> • Implement refined management and control of EIP traffic based on protection rules. For details, see Configuring a Protection Rule to Allow the Inbound Traffic to a Specified EIP. • Use the intrusion prevention function to defend against common attacks. For details, see Configuring Intrusion Prevention to Protect EIPs. 		

VPC Border Traffic Protection



Procedure	Description	Reference
Purchasing CFW	Purchase a CFW instance in the region where you want to protect traffic.	Purchasing CFW
Enabling VPC protection	<p>Enable protection for two or more VPCs.</p> <p>CFW protects VPC border traffic by protecting the VPCs.</p>	
Configuring protection policies	<p>By default, CFW allows all traffic. You need to configure protection policies to protect traffic.</p> <p>The following protection policies are provided:</p> <ul style="list-style-type: none"> ● Protection rules: You can set rules to control traffic by IP address, IP address group, region, or domain name. ● Blacklist/Whitelist: Traffic is controlled based on specific rules configured for IP addresses and IP address groups. Traffic that matches the whitelist is directly allowed without being checked by other functions. ● Intrusion prevention: Network attacks are blocked based on multiple IPS rule databases. ● Antivirus: Virus-infected files are blocked based on protocol types. 	<p>Protection rules:</p> <p>Blacklist/Whitelist:</p> <p>Intrusion prevention:</p> <p>Antivirus:</p>
Checking logs	View the traffic protection outcomes in logs.	Viewing Logs
<p>Example scenarios:</p> <p>Configure CFW protection rules to control inter-VPC traffic. For details, see .</p>		

NAT gateway traffic protection



Procedure	Description	Reference
Purchasing CFW	Purchase a CFW instance in the region where you want to protect traffic.	Purchasing CFW
Enabling VPC (NAT) protection	Enable protection for two or more VPCs. CFW protects the traffic of the NAT gateway by protecting the VPC where the NAT gateway resides.	
Configuring protection policies	By default, CFW allows all traffic. You need to configure protection policies to protect traffic. The following protection policies are provided: <ul style="list-style-type: none"> • Protection rules: You can set rules to control traffic by IP address, IP address group, region, or domain name. • Blacklist/Whitelist: Traffic is controlled based on specific rules configured for IP addresses and IP address groups. Traffic that matches the whitelist is directly allowed without being checked by other functions. • Intrusion prevention: Network attacks are blocked based on multiple IPS rule databases. • Antivirus: Virus-infected files are blocked based on protocol types. 	Protection rules: Blacklist/Whitelist: Intrusion prevention: Antivirus:
Checking logs	View the traffic protection outcomes in logs.	Viewing Logs

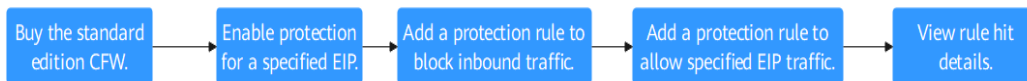
Procedure	Description	Reference
Example scenarios: Configure CFW protection rules to control NAT gateway traffic. For details, see		

2 Configuring a Protection Rule to Allow the Inbound Traffic to a Specified EIP

Proper protection rules can help you manage and control the traffic between cloud assets and the Internet in a refined manner, prevent the spread of internal threats, and enhance the depth of security strategies.

You can configure protection rules on the standard edition firewall to allow the inbound traffic to a specified EIP, easily controlling the traffic to your cloud assets.

Process



Procedure	Description
Making Preparations	Sign up for a HUAWEI ID, enable Huawei Cloud services, top up your account, and assign CFW permissions to the account.
Step 1: Purchase the CFW Standard Edition	Purchase CFW. Select a region and an edition (for example, the standard edition), and configure other parameters.
Step 2: Enable Protection for a Specified EIP	Enable protection for an EIP to divert traffic to CFW.
Step 3: Add a Protection Rule to Block All Inbound Traffic	Configure a protection rule to block all inbound traffic and set its priority to the lowest.
Step 4: Add a Protection Rule to Allow Inbound Traffic to a Specified EIP	Configure a protection rule to allow the inbound traffic of a specified EIP (for example, <code>xx.xx.xx.1</code>) and set its priority to be higher than that of the blocking rule.

Procedure	Description
Step 5: Viewing Rule Hits in Access Control Logs	Check whether protection rule takes effect.

Making Preparations

- Before purchasing CFW, create a Huawei account and subscribe to Huawei Cloud. For details, see [Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services](#) and [Real-Name Authentication](#).
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
- Make sure that your account has sufficient balance, or you may fail to pay to your CFW orders.
- Make sure your account has CFW permissions assigned.


Table 2-1 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

Step 1: Purchase the CFW Standard Edition

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

This section describes how to purchase the CFW standard edition. For details about how to purchase other editions, see [Purchasing CFW](#). For details about the function differences between editions, see [Editions](#).

- [Log in to the management console](#). In the navigation pane, click  in the upper left corner and choose **Security & Compliance > Cloud Firewall**.
- Click **Buy CFW**. On the displayed page, configure the following parameters:
This example only introduces mandatory parameters. Configure other parameters as needed.

Parameter	Example Value	Description
Region	EU-Dublin	Select the region where the EIP is located. 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?
Editions	Standard	Select an edition.

3. Confirm the information and click **Buy Now**.
4. Confirm the order details, select **I have read and agreed to the Huawei Cloud Firewall Service Statement**, and click **Next**.
5. Select a payment method and pay for your order.

Step 2: Enable Protection for a Specified EIP

1. In the navigation pane on the left, choose **Assets > EIPs**.
2. 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 that you want to enable protection and click **Enable Protection** above the list.

NOTICE

- Currently, IPv6 addresses cannot be protected.
- An EIP can only be protected by one firewall.
- Only EIPs in the enterprise project to which the current account belongs can be protected.

3. 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 action of the access control policy is **Allow**.

Step 3: Add a Protection Rule to Block All Inbound Traffic

1. In the navigation pane, choose **Access Control > Access Policies**.
2. Click **Add Rule**. In the **Add Rule** dialog box, configure parameters.
In this example, only necessary parameters are described. For details about other parameters, see [Adding Protection Rules to Block or Allow Traffic](#).

Parameter	Example Value	Description
Direction	Inbound (indicating inbound traffic)	Select the traffic direction. <ul style="list-style-type: none"> • Inbound: Cloud assets (EIPs) are accessed from the Internet. • Outbound: Cloud assets (EIPs) access the Internet.
Source	Any	Source address of access traffic.
Destination	Any	Destination address of access traffic.
Service	Any	Set Protocol, Source Port, and Destination Port.
Application	Any	Configure protection policies for application-layer protocols.
Action	Block	Set the action to be taken when traffic passes through the firewall. <ul style="list-style-type: none"> • Allow: Traffic is forwarded. • Block: Traffic is not forwarded.
Priority	Pin on top (If there are other protection rules, select Lower than the selected rule to set the rule priority to the lowest.)	Set the priority of the rule. Its value can be: <ul style="list-style-type: none"> • Pin on top, indicating that the priority of the policy is set to the highest. • Lower than the selected rule: indicating that the policy priority is lower than a specified rule.

3. Click **OK** to complete the protection rule configuration.

Step 4: Add a Protection Rule to Allow Inbound Traffic to a Specified EIP

1. Choose **Access Policies** and click the **Protection Rules** tab, click **Add**. In the displayed **Add Rule** dialog box, configure the following parameters:

Parameter	Example Value	Description
Direction	Inbound (indicating inbound traffic)	Select the traffic direction. <ul style="list-style-type: none"> • Inbound: Cloud assets (EIPs) are accessed from the Internet. • Outbound: Cloud assets (EIPs) access the Internet.
Source	Any	Source address of access traffic.
Destination	xx.xx.xx.1	Destination address of access traffic.

Parameter	Example Value	Description
Service	Any	Set Protocol , Source Port , and Destination Port .
Application	Any	Configure protection policies for application-layer protocols.
Action	Allow	Set the action to be taken when traffic passes through the firewall. <ul style="list-style-type: none">● Allow: Traffic is forwarded.● Block: Traffic is not forwarded.
Priority	Pin on top (or at least higher than the previous blocking rule)	Set the priority of the rule. Its value can be: <ul style="list-style-type: none">● Pin on top, indicating that the priority of the policy is set to the highest.● Lower than the selected rule: indicating that the policy priority is lower than a specified rule.

2. Click **OK** to complete the protection rule configuration.

Step 5: Viewing Rule Hits in Access Control Logs

In the navigation pane, choose **Log Audit > Log Query**. Click the **Access Control Logs** tab.

The rule has taken effect if access control logs meet the following conditions:

- In the row where **Destination IP** is the allowed EIP (for example, *xx.xx.xx.1*), the corresponding **Action** is **Allow**.
- In the rows where **Destination IP** values are other IP addresses, the corresponding **Action** is **Block**.

References

- For details about protection rule parameters, see [Adding a Protection Rule](#).

3 Configuring Intrusion Prevention to Protect EIPs

CFW provides intrusion prevention 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.

This document describes how to use the standard edition firewall and protect EIPs through intrusion prevention in **Intercept mode - medium** mode, flexibly protecting cloud assets.

Process



Procedure	Description
Making Preparations	Sign up for a HUAWEI ID, enable Huawei Cloud services, top up your account, and assign CFW permissions to the account.
Step 1: Purchase the CFW Standard Edition	Purchase CFW. Select a region and an edition (for example, the standard edition), and configure other parameters.
Step 2: Enable Protection for an EIP	Enable protection for an EIP to divert traffic to CFW.
Step 3: Set the Intrusion Prevention Mode to Observe	In Observe mode, if the firewall detects an attack event, it records the event in the attack event log and does not block traffic. This can prevent traffic interruption caused by incorrect blocking.
Step 4: Periodically View Attack Event Logs to Check for Incorrect Blocking	View attack event logs to check whether there is normal traffic that was incorrectly blocked and record the corresponding rule ID.

Procedure	Description
Step 5: Modify the Improper IPS Rule and Set the Protection Action to Block	Change the protection action of the rule and change the intrusion prevention mode to Intercept (for example, Intercept mode - medium.)
Step 6: View the Protection Effect Through Attack Event Logs	View attack event logs to check whether normal traffic is allowed.

Making Preparations

- Before purchasing CFW, create a Huawei account and subscribe to Huawei Cloud. For details, see [Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services](#) and [Real-Name Authentication](#).
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
- Make sure that your account has sufficient balance, or you may fail to pay to your CFW orders.
- Make sure your account has CFW permissions assigned.


Table 3-1 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

Step 1: Purchase the CFW Standard Edition

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

This section describes how to purchase the CFW standard edition. For details about how to purchase other editions, see [Purchasing CFW](#). For details about the function differences between editions, see [Editions](#).

- [Log in to the management console](#). In the navigation pane, click  in the upper left corner and choose **Security & Compliance > Cloud Firewall**.
- Click **Buy CFW**. On the displayed page, configure the following parameters:

This example only introduces mandatory parameters. Configure other parameters as needed.

Parameter	Example Value	Description
Region	EU-Dublin	Select the region where the EIP is located. 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?
Editions	Standard	Select an edition.

3. Confirm the information and click **Buy Now**.
4. Confirm the order details, select **I have read and agreed to the Huawei Cloud Firewall Service Statement**, and click **Next**.
5. Select a payment method and pay for your order.

Step 2: Enable Protection for an EIP

1. In the navigation pane on the left, choose **Assets > EIPs**.
2. 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 that you want to enable protection and click **Enable Protection** above the list.

NOTICE

- Currently, IPv6 addresses cannot be protected.
- An EIP can only be protected by one firewall.
- Only EIPs in the enterprise project to which the current account belongs can be protected.

3. 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 action of the access control policy is **Allow**.

Step 3: Set the Intrusion Prevention Mode to Observe

1. In the navigation pane, choose **Attack Defense > Intrusion Prevention**.
2. In the **Protection Mode** area, select **Observe**.

NOTE

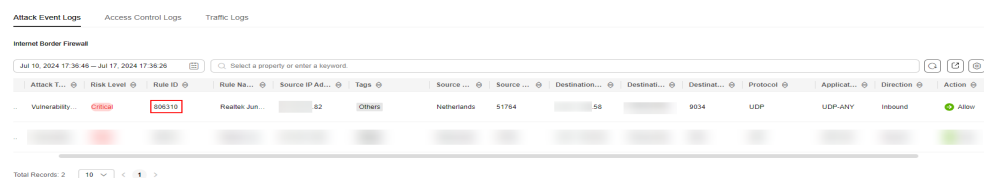
This document uses the **Observe** mode as an example. If your workloads need stronger protection, you can change to the **Intercept** mode. You are advised to select a loose interception mode (for example, **Intercept mode - loose**) and observe its effects for a period of time before using a mode with higher granularity.

Step 4: Periodically View Attack Event Logs to Check for Incorrect Blocking

1. In the navigation pane, choose **Log Audit > Log Query**.
2. On the **Attack Event Logs** tab, check whether any traffic was improperly blocked based on the **Direction, Source IP Address, and Destination IP Address** recorded in logs. If there is improperly blocked traffic, record the corresponding rule ID.

For example, the traffic from an external IP address *xx.xx.xx.82* to an internal IP address *xx.xx.xx.58* is normal, but is blocked by the IPS rule whose ID is 806310. This means such traffic was blocked by rule 806310 in **Intercept** mode. Record the rule ID.

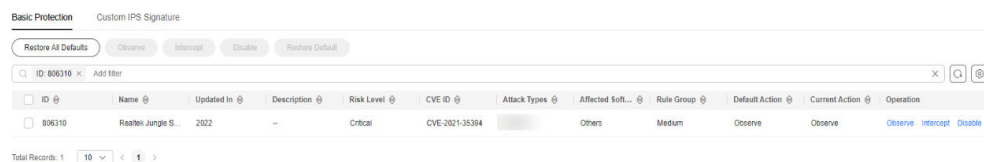
Figure 3-1 Viewing attack event logs



Step 5: Modify the Improper IPS Rule and Set the Protection Action to Block

1. In the navigation pane, choose **Attack Defense > Intrusion Prevention**.
2. Click **Check Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.
3. Filter out the rule whose ID is 806310, click **Observe** in the **Operation** column, and change **Current Action** to **Observe**.

Figure 3-2 Modifying a basic protection action



4. Return to the **Intrusion Prevention** page. In the **Protection Mode** area, select **Intercept mode - medium**.

Step 6: View the Protection Effect Through Attack Event Logs

1. In the navigation pane, choose **Log Audit > Log Query**.
2. On the **Attack Event Logs** tab page, view logs to check whether normal service traffic is identified as an attack event, that is, whether the **Action** for the traffic is **Block**.

References

- For details about intrusion prevention parameters, see [Blocking Network Attacks](#).

4 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 4-1 Common practices

Practice	Description
Allowing Outbound Traffic from Cloud Resources Only to a Specified Domain Name	Quickly allow access traffic from cloud resources to a domain name. This mode applies to scenarios where services only need to access a specified domain name.
Using CFW to Defend Against Network Attacks	Use CFW to defend against diverse network attacks on cloud services.