

Cloud Firewall

FAQs

Issue	13
Date	2025-08-05



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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.

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 About the Product.....	1
1.1 Does CFW Support On-premises Servers?.....	1
1.2 What Traffic Does CFW Protect?.....	1
1.3 Can CFW Protect EIPs of Intelligent EdgeCloud (IEC)?.....	1
1.4 What Are the QPS, New Connections, and Concurrent Connections Supported by CFW?.....	2
1.5 Can CFW Be Shared Across Accounts?.....	2
1.6 What Are the Differences Between CFW and WAF?.....	2
1.7 What Are the Differences Between CFW, Security Groups, and Network ACLs?.....	3
1.8 How Does CFW Control Access?.....	5
1.9 What Are the Priorities of the Protection Settings in CFW?.....	5
1.10 Can WAF, Advanced Anti-DDoS, and CFW Be Deployed Together?.....	6
1.11 Can CFW Protect Resources Across Enterprise Projects?.....	6
1.12 How Long Are CFW Logs Stored by Default?.....	6
2 Regions and AZs.....	8
2.1 What Are Regions and AZs?.....	8
2.2 Can CFW Be Used Across Clouds or Regions?.....	9
3 Troubleshooting.....	11
3.1 Why Are Traffic and Attack Logs Incomplete?.....	11
3.2 Why Does a Protection Rule Not Take Effect?.....	11
3.3 Why Is No Data Displayed on the Access Control Logs Page?.....	13
3.4 What Can I Do If Services Cannot Be Accessed After a Policy Is Configured on CFW?.....	14
3.5 What Do I Do If IPS Blocks Normal Services?.....	19
3.6 Why Is the IP Address Translated Using NAT64 Blocked?.....	20
3.7 Why Some Permissions Become Invalid After a System Policy Is Granted to an Enterprise Project?.....	20
3.8 What Do I Do If a Message Indicating Insufficient Permissions Is Displayed When I Configure LTS Logs?.....	21
3.9 What Can I Do If Automatic EIP Protection Does Not Take Effect?.....	22
4 Network Traffic.....	23
4.1 How Do I Calculate the Number of Protected VPCs and the Peak Protection Traffic at the VPC Border?.....	23
4.2 How Does CFW Collect Traffic Statistics?.....	23
4.3 What Is the Protection Bandwidth Provided by CFW?.....	24
4.4 What Do I Do If My Service Traffic Exceeds the Protection Bandwidth?.....	24

4.5 What Are the Differences Between the Data Displayed in Traffic Trend Module and the Traffic Analysis Page?.....	25
4.6 How Do I Verify the Validity of an Outbound HTTP/HTTPS Domain Protection Rule?.....	25
4.7 How Do I Obtain the Real IP Address of an Attacker?.....	26
4.8 What Do I Do If a High Traffic Warning Is Received?.....	28

1 About the Product

1.1 Does CFW Support On-premises Servers?

No. CFW can protect region-level services on the cloud.

1.2 What Traffic Does CFW Protect?

CFW is a next-generation cloud native firewall. It can protect the following resources:

- Internet border: EIP traffic, including inbound (from the Internet to the firewall) and outbound (from the firewall to the Internet) traffic, can be protected.
- VPC border: The traffic between VPCs, and the traffic between a VPC and an on-premises IDC can be protected. The traffic within a VPC cannot be protected.
- NAT gateway protection comes in the following scenarios:
 - The EIP bound to a NAT gateway can be protected. Only the traffic of the EIP will be audited.
 - The SNAT and DNAT traffic can be protected (depending on the VPC border firewall) and traffic can be traced to private IP addresses.

1.3 Can CFW Protect EIPs of Intelligent EdgeCloud (IEC)?

No. CFW can only protect the resources on Huawei Cloud.

- For details about IEC, see [What Is Intelligent EdgeCloud?](#)

1.4 What Are the QPS, New Connections, and Concurrent Connections Supported by CFW?

Traditional hardware firewalls restrict the number of new connections, number of concurrent connections, and QPS. As a SaaS service, CFW does not have these restrictions. The only standard for measuring CFW performance is the actual protection bandwidth.

The protection bandwidth is defined as follows:

- 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.

1.5 Can CFW Be Shared Across Accounts?

CFW supports cross-account protection. Before protection, perform the following operations:

- For details about cross-account Internet border protection, see [Using CFW to Protect EIPs Across Accounts](#).
- For VPC border cross-account protection, when you add VPC attachments to configure an enterprise router, share the enterprise router of account A with account B, and then add attachments in account B. Subsequent configurations are still performed on account A. For details about an inter-VPC border firewall, see [Using CFW to Protect EIPs Across Accounts](#).

1.6 What Are the Differences Between CFW and WAF?

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

[Table 1-1](#) describes the differences between WAF and CFW.

Table 1-1 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	<ul style="list-style-type: none">• EIP border and VPC border• Basic protection against web attacks• Defense against external intrusions and protection of proactive connections to external systems	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.

1.7 What Are the Differences Between CFW, Security Groups, and Network ACLs?

CFW, security groups, and network ACLs allow you to set access control policies based on IP addresses or IP address groups to protect your Internet borders, VPC borders, ECSs, and subnets.

[Table 1-2](#) describes the differences between them.

Table 1-2 Differences between CFW, security groups, and network ACLs

Item	CFW	Security group	Network ACL
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.	A security group is a collection of access control rules for instances, such as cloud servers, containers, and databases, that have the same security requirements and that are mutually trusted within a VPC. You can define different access control rules for a security group, and these rules are then applied to all the instances added to this security group. For details about security groups, see Security Groups and Security Group Rules .	A network ACL is an optional layer of security for your subnets. After you associate one or more subnets with a network ACL, you can control traffic in and out of the subnets. For details about network ACLs, see Network ACL .
Protected objects	<ul style="list-style-type: none">• Internet boundary• VPC boundary• SNAT scenario	ECS	Subnet
Features	<ul style="list-style-type: none">• Filtering by 5-tuple (source IP address, destination IP address, protocol, source port, and destination port)• Filtering by geographical location, domain name, domain name group, and blacklist/whitelist• Intrusion prevention system (IPS) and antivirus (AV).	Filtering by 3-tuple (protocol, port, and peer IP address)	Filtering by 5-tuple (source IP address, destination IP address, protocol, source port, and destination port)

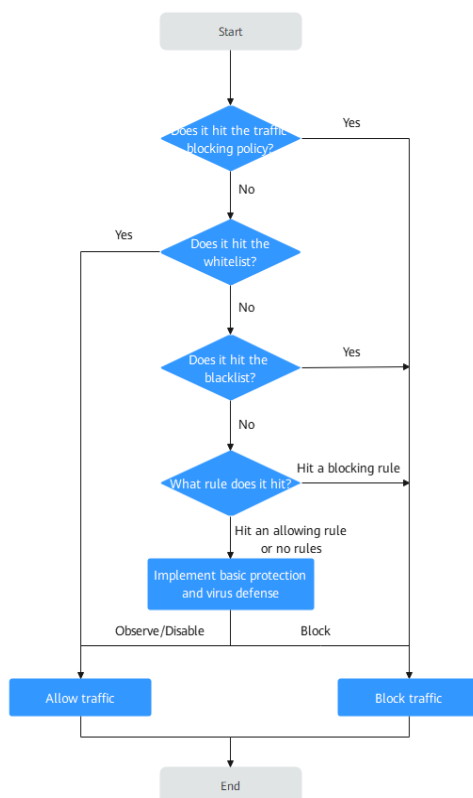
1.8 How Does CFW Control Access?

CFW allows you to configure ACL policies based on a 5-tuple, IP address group, service group, domain name, applications, blacklist, and whitelist. You can also configure ACL policies based on the intrusion prevention system (IPS). The IPS can work in observation or block mode. In block mode, CFW detects and blocks traffic that matches the IPS rules. For details, see [Configuring Access Control Policies](#).

1.9 What Are the Priorities of the Protection Settings in CFW?

The priorities of the protection settings that take effect in CFW in descending order are as follows: Traffic blocking > Whitelist > Blacklist > Protection policy (ACL) > Basic Protection (IPS) = Antivirus.

Figure 1-1 Protection priorities



- For details about how to configure traffic blocking, see [Configuring Traffic Blocking](#).
- For details about how to set the blacklist or whitelist, see [Managing Blacklists and Whitelists](#).
- For details about how to add a protection rule, see [Adding a Protection Rule](#).

- For details about how to set the IPS protection mode, see [Configuring Intrusion Prevention](#). For details about how to customize IPS rules, see [Customizing IPS Signatures](#).
- For details about how to enable virus defense, see [Enabling Antivirus](#).

1.10 Can WAF, Advanced Anti-DDoS, and CFW Be Deployed Together?

Yes. WAF has three modes: exclusive mode, ELB mode, and cloud mode. The traffic trend varies depending on the mode. The details are as follows:

Table 1-3 Traffic flow

WAF Mode	Traffic Flow
Dedicated/ELB mode	Internet -> AAD -> CFW -> WAF (dedicated/ELB mode) -> Origin Server
Cloud mode	Internet -> Advanced Anti-DDoS -> WAF (cloud mode) -> CFW -> Origin server

NOTE

- If you have purchased Advanced Anti-DDoS or WAF in cloud mode, exercise caution when configuring traffic blocking rules. You are advised to configure traffic permitting rules or whitelists.
- If you have purchased WAF in dedicated or ELB mode, configure it based on service requirements.

For details, see [Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN](#).

1.11 Can CFW Protect Resources Across Enterprise Projects?

Yes. CFW can protect all cloud resources (EIPs, VPCs, and NAT gateways) in the current region and under the current account.

[Enable enterprise management](#) , and select an enterprise project when purchasing CFW. In this case, CFW bills belong to this project. It does not affect CFW resource protection.

For details about how to plan CFW when an enterprise uses enterprise project management to manage services, see [Using CFW to Protect Enterprise Resources](#).

1.12 How Long Are CFW Logs Stored by Default?

You can query and export logs generated within the last seven days for free. For details, see [Querying Logs](#).

You can record one or multiple logs in LTS and view logs generated in the past 1 to 365 days. For details, see [Log Management](#).



CAUTION

LTS is billed by traffic and is billed separately from CFW. For details about LTS pricing, see [LTS Pricing](#).

2 Regions and AZs

2.1 What Are Regions and AZs?

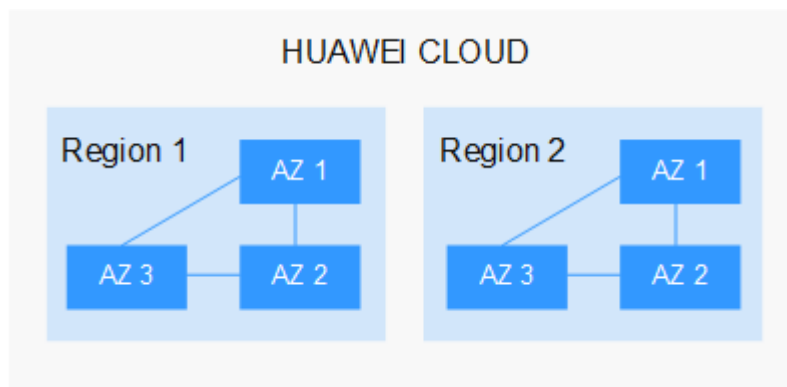
Concepts

A region or an availability zone (AZ) identifies the location of a data center. You can create resources in a specific region or an AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

Figure 2-1 shows the relationship between the regions and AZs.

Figure 2-1 Region and AZ



Huawei Cloud provides services in many regions around the world. You can select a region and AZ as needed.

Selecting a Region

When selecting a region, consider the following factors:

- Location

You are advised to select a region close to you or your target users. This reduces network latency and improves access rate.

- If you or your users are in the Asia Pacific region and outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
- If you or your users are in Africa, select the **AF-Johannesburg** region.
- If you or your users are in Latin America, select the **LA-Santiago** region.

- Resource price

Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

2.2 Can CFW Be Used Across Clouds or Regions?

In Which Regions Is CFW Available?

For details about CFW and the regions supported by each function, see [Function Overview](#).

Can CFW Be Used Across Regions?

- Internet border protection: CFW cannot be used across regions. CFW can be used only in the region selected during purchase.
- VPC border protection: CFW cannot be used across regions, except for the scenarios where cross-region network communication is implemented using Cloud Connect (CC). CFW can be used only in the region selected during purchase.

If a message is displayed indicating that CFW cannot be purchased in the selected region, you can choose: VPC [Network ACLs](#) and [Security Groups](#).

Can CFW Be Used Across Clouds?

No. Currently, CFW only protects services deployed on Huawei Cloud.

3 Troubleshooting

3.1 Why Are Traffic and Attack Logs Incomplete?

Traffic and attack logs are recorded only when CFW is enabled. If it is disabled, no logs are generated for this period until it is enabled again.

To let CFW generate full logs, keep it enabled all along.

3.2 Why Does a Protection Rule Not Take Effect?

All Traffic Is Allowed Even If a Rule Is Configured to Allow Only Several EIPs

After EIP protection is enabled on CFW, the access control policy allows all traffic by default. If you want to allow traffic of only several EIPs, you need to configure a protection rule to block all traffic and set the lowest priority.



- 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 on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
- Step 4** (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.
- Step 5** In the navigation pane on the left, choose **Access Control > Internet Border Protection Rules** or **VPC Border Protection Rules**.
- Step 6** Configure a global blocking rule. Click **Add Rule**. Use the parameter settings shown in [Figure 3-1](#) and configure other parameters as needed.

Figure 3-1 Blocking all traffic

Matching Condition [View Configuration Guide](#)

Direction

☒ Inbound ☐ Outbound

Source [?](#)

☐ IP Address ☐ IP address group ☐ Countries and regions ☒ Any [?](#)

Destination [?](#)

☐ IP Address ☐ IP address group ☒ Any [?](#)

Service [?](#)

☐ Service ☐ Service group ☒ Any [?](#)

Application [?](#)

☐ Application ☒ Any

Protection Configuration

Protection Action

☐ Allow ☒ Block

NOTE

You are advised to enable the rules after adding all required ones.

- Step 7** Configure an allow rule. For details about how to add a protection rule, see [Adding a Protection Rule](#).
- Step 8** Set the priority of the global blocking rule in the [Step 6](#) to the lowest. For details, see [Setting the Priority](#).
- Step 9** Enable all rules. You are advised to enable the allow rules prior to the blocking rules.

----End

Blocked IP Addresses Are Still Allowed Through Even If a Global Blocking Rule Is Configured

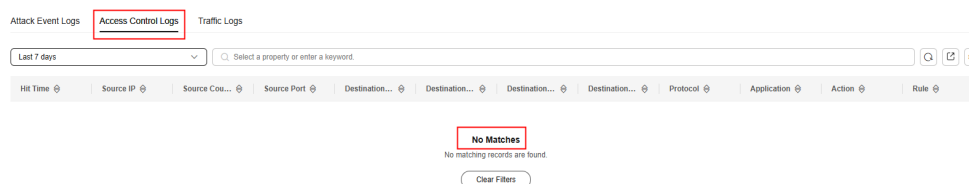
The EIP protection rules configured on CFW are applied based on the EIP management list. If you have enabled global blocking (0.0.0.0/0) but the traffic of EIPs not in an allow rule is allowed through, check whether the EIPs are protected. For more information, see [Enabling EIP Protection](#).

3.3 Why Is No Data Displayed on the Access Control Logs Page?

Symptom

There is traffic, but no data is displayed on the access control log page, as shown in [Figure 3-2](#).

Figure 3-2 Access control logs



Possible Causes

Access control logs display the traffic that hits an ACL protection policy (a protection rule or blacklist/whitelist). If the firewall is not enabled for cloud resources or no ACL policies are configured, no access control logs will be generated.

Solution

1. Enable the firewall to protect cloud resources.
 - For details about how to enable EIP protection, see [Enabling EIP Protection](#).
 - For details about how to enable VPC border protection, see [Enabling VPC Border Traffic Protection](#).
2. Add an ACL policy.
 - For details about how to add a protection rule, see [Adding a Protection Rule](#).
 - For details about how to add a blacklist or whitelist, see [Adding a Blacklist or Whitelist Item](#).

References

Viewing other logs

- For details about the records of all traffic passing through CFW, see [Traffic Logs](#).
- For details about attack event records, see [Attack Event Logs](#).

3.4 What Can I Do If Services Cannot Be Accessed After a Policy Is Configured on CFW?

Symptom

After you configure a protection policy on CFW, the service traffic is abnormal. For example:

- An EIP cannot access the Internet.
- A server cannot be accessed.
- A certain domain name cannot be accessed.

Troubleshooting Methods

Figure 3-3 Procedure of checking traffic exceptions

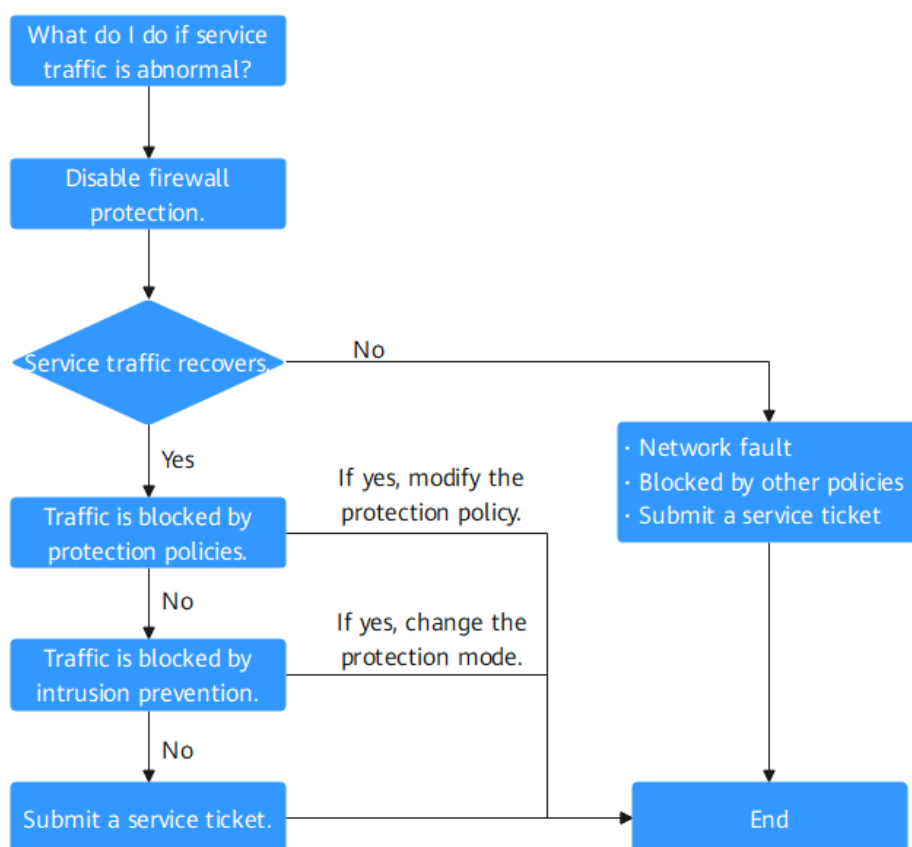


Table 3-1 Procedure of checking traffic exceptions

No.	Possible Cause	Solution
1	Traffic interruption not caused by CFW	See Cause 1: Traffic Interruption Not Caused by CFW .

No.	Possible Cause	Solution
2	Traffic blocked by protection policies	See Cause 2: Traffic Blocked by Protection Policies .
3	Traffic blocked by intrusion prevention	See Cause 3: Traffic Blocked by Intrusion Prevention .

Cause 1: Traffic Interruption Not Caused by CFW

Log in to the [CFW console](#) and perform the following steps:

Step 1 Disable protection.

- EIP traffic fault: Disable the CFW protection in EIPs whose services are interrupted. For details, see [Disabling EIP Protection](#).
- SNAT or inter-VPC access failure: Disable the VPC border firewall. For details, see [Disabling a VPC Border Firewall](#).

Step 2 Observe the service running status.

- If the service is restored, it indicates traffic was blocked by CFW. Rectify the fault by referring to [Cause 2: Traffic Blocked by Protection Policies](#) and [Cause 3: Traffic Blocked by Intrusion Prevention](#).
- If the fault persists, the traffic interruption is not caused by CFW. Possible fault causes include:
 - Network fault: The route configuration is incorrect, or the NE is faulty.
 - Policy-based interception: Interception caused by incorrect configurations of other security services, network ACLs, or security groups.

If you need assistance from Huawei Cloud, you can [create a service ticket](#).

----End

Cause 2: Traffic Blocked by Protection Policies

Traffic is blocked probably because a blocking rule is configured in the access control policy, or the normal services are blacklisted. In this case, CFW blocks related sessions, causing service loss.

You can take the following measures:

In the [Access Control Logs](#) tab, search for logs about the blocked IP address or domain name.

- If no records are found, see cause 3 in [Table 3-1](#).
- If a record is found, click the **Rule** column to go to the matched blocking policy.
 - The blacklist is blocked. You can select either of the following methods:
 - Method 1: Delete the blacklist policy.
 - Method 2: Add a whitelist policy for the IP address/domain name. (The whitelist takes precedence over the blacklist. After the whitelist

policy is added, the blacklist policy will be invalid and the traffic is directly permitted.)

- The protection rule is blocked. You can perform either of the following operations:
 - Method 1: Find the blocking rule of the IP address or domain name in the access control rule list and disable the policy.
 - Method 2: Modify the matching condition of the blocking policy and remove the IP address or domain name information.
 - Method 3: Add a protection rule whose **Action** is **Allow** and **Priority** is **Pin on top**. For details, see [Adding a Protection Rule](#).

Case

Handling process: Detect a fault -> Disable protection -> View logs -> Modify a policy -> Restore protection -> Confirm logs

The network O&M personnel of a company found that an ECS cannot access the Internet through the bound EIP **xx.xx.xx.94**.

The firewall administrator took the following measures:

Step 1 To ensure that the IP address can be used for external communication during fault locating, the firewall administrator logged in to the firewall console, and chose **Assets > EIPs**, and disables protection for the EIP.

During the firewall is disabled, the traffic of the EIP is not processed and related logs are not displayed.

Figure 3-4 EIPs

EIP ID	Protection Status	Firewall Name/ID	Associated Instance	Owner	Tags	Operation
177 a17-414b-980c-4eb75b2e4c01	Not protected	--	NAT Gateway		--	Enable Protection
110-13c-3d5e-a80c0d-1a71 43c-462-0546-c7827c19d942	Not protected	--	Cloud Server		--	Enable Protection
130 679-421f-a258-78e95208038e	Not protected	--	Cloud Server		--	Enable Protection
94 0216401a-4930-4935-e55b-e5b3e28e455a	Protected	Firewall 21689f56-a62c-41d3-9205-4efda5c1e43	Cloud Server		--	Disable Protection

Step 2 The administrator chose **Log Audit > Log Query** and clicked the **Access Control Logs** tab. He searched for the blocking logs of the access source IP address **xx.xx.xx.94**. A blocking rule named **Block-Malicious-Outreach** was found, and this rule blocked the traffic from the attack source IP address to the Internet.

Figure 3-5 Filtering access control logs

Hit Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action	Rule
Mar 20, 2024 10:45:45	94	45093	213	53	UDP	Block	Block_Malicious_Outreach
Mar 20, 2024 11:44:02 GMT+	94	35987	213	53	UDP	Block	Block_Malicious_Outreach
Mar 20, 2024 11:44:01 GMT+	94	39556	213	53	UDP	Block	Block_Malicious_Outreach

Step 3 The administrator searched for "Source: xx.xx.xx.94; Action: Block; Direction: Outbound; Status: Enabled" in the access control policy list. Three available policies that contain the IP address were found.

The policy contained the **Block-Malicious-Outreach** blocking rule. According to the value of the **Hits** column, a large number of sessions have been blocked.

Figure 3-6 Searching for a protection rule

Priority	Name/Rule ID	Direction	Source	Destination	Service	Application	Action	Hits	Status	Tags	Operation
1	Block_Asia 0b29997a-e600-43...	Outbound	94	Antarctica, Europe...	TCP/80/443	--	Block	0	Enabled	--	Edit Configure Priority More
2	Block_*.com 3870056-9009-499...	Outbound	94	*.com	TCP/80/443	--	Block	0	Enabled	--	Edit Configure Priority More
6	Block_Malicious... 2073899-6245-42...	Outbound	0.0.0.0/0	0.0.0.0/0	Any	--	Block	25,497	Enabled	--	Edit Configure Priority More

CAUTION

According to **Figure 3-6**, there were three valid rules whose source IP addresses contain **xx.xx.xx.94**, including **Block-xxx-com** (with the highest priority), **Block-Malicious-Outreach**, and **Allow-Asia** (with the lowest priority). Besides the blocking rule **Block-Malicious-Outreach**, the administrator checked whether the two other two rules may intercept normal services.

Finally, it is found that the EIP accessed suspicious IP addresses so that an administrator configured a blocking rule it, but the configured destination was incorrect. As a result, all external traffic is blocked by mistake (see the second protection rule in **Figure 3-6**).

Step 4 The administrator changed the destination address to a specific IP address that needs to be blocked, and enabled protection for the EIP on the **Assets > EIPs** page of the firewall console. After protection was restored, the traffic of the EIP was normally forwarded by CFW.

Step 5 The administrator viewed the external connection logs related to the IP address in the traffic logs and confirmed that the service was restored.

-----End

Cause 3: Traffic Blocked by Intrusion Prevention

The protection mode of intrusion prevention functions, such as IPS, is too strict, blocking normal traffic.

You can take the following measures:

In the **Attack Event Logs** tab, search for logs about the blocked IP address or domain name.

- If no records are found, [submit a service ticket](#) to troubleshoot the problem.
- If a record is found, perform either of the following operations:

- Copy the rule ID. In the corresponding module (such as IPS), set the protection mode of the rule with that ID to **Observe**. For details about the intrusion prevention module, see [Configuring Intrusion Prevention](#).
- Add the IP addresses that do not need to be protected by CFW to the whitelist. For details about how to configure the whitelist, see [Adding an Item to the Blacklist or Whitelist](#).

Case

Handling process: Detect a fault -> Change the protection status -> View logs -> Confirm services -> Modify the policy -> Restore the protection status -> Confirm logs

The O&M personnel of a company found that a service on the server whose IP address was **xx.xx.xx.90** cannot be accessed. It was suspected that the service was blocked by the firewall.

The firewall administrator took the following measures:

- Step 1** To quickly recover the service, the administrator logged in to the firewall console, choose **Attack Defense > Intrusion Prevention**, and changed the protection mode from **Intercept mode - strict** to **Observe**.

During this period, the firewall did not intercept attack traffic but only logged the attack traffic.

- Step 2** The administrator chose **Log Audit > Log Query** and clicked the **Attack Event Logs** tab. The logs about the access to the destination IP address **xx.xx.xx.90** were displayed. The IPS rule whose ID was 331978 blocked the traffic.

Figure 3-7 Filtering attack event logs

Time	Attack	Severity	Rule ID	Rule Name	Source	Source C...	Source...	Destina...	Destina...	Destina...	Protocol	Applica...	Direction	Action	Operation
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flin...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Black	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flin...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Black	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flin...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Black	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flin...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Black	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flin...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Black	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flin...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Black	View

- Step 3** The administrator clicked **Details** in the **Operation** column, clicked **Payload Content** in the display page, and [created a packet capture task](#) to verify that the service is normal. The administrator searched for the rule whose ID is 331978 from the list on the **Basic Protection** tab page by referring to [Modifying the Action of a Basic Protection Rule](#).

Figure 3-8 Rule 331978

ID	Name	Updated In	Description	Risk Level	CVE ID	Attack Types	Affected Sof...	Rule Group	Default Action	Current Acti...	Operation
331978	Apache Flin...	2021	--	Fatal	CVE-2020-17519	Vulnerability Attack	Apache	Low	Observe	Observe	Observe Intercept Disable

- Step 4** The administrator clicked **Observe** in the **Operation** column. This rule did not block the traffic matching the signature but only logged the traffic.

Step 5 The administrator set the protection mode to **Intercept mode - strict** and went to the **Basic Protection** tab to confirm that the **Current Status** of the rule 331978 was still **Observe**.

Step 6 In the **Attack Event Logs** tab, after the service session matched the rule, the **Action** of the log was **Allow**. The service was restored.

----End

Submitting a Service Ticket

If the preceding methods cannot solve your problem, [submit a service ticket](#).

3.5 What Do I Do If IPS Blocks Normal Services?


IPS detects and defends against access traffic in real time based on the attack defense experience and rules accumulated over the years, blocking common network attacks and effectively protecting your assets.


Check attack event logs. If you can confirm that normal service traffic was blocked, perform either of the following operations:

- Query the ID of the rule that blocks traffic and modify the action of the rule in the IPS rule library. For details, see [Querying Hit Rules and Modifying Protection Actions](#).
- Use a less strict IPS protection mode. For details, see [Configuring Intrusion Prevention](#).

Querying Hit Rules and Modifying Protection Actions

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console. Select a region.

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 In the navigation pane, choose **Log Audit > Log Query**. Click the **Attack Event Logs** query and record the **Rule ID** of the rule that blocks traffic.

Figure 3-9 Rule ID

Attack Type	Severity	Rule ID	Matched Rule
Vulnerability ...	High	336842	Simple HTT...

Step 6 Click **View Effective Rule** under **Basic Protection**. The **Basic Protection** tab is displayed.

Step 7 Search for the rule by its ID. In the **Operation** column, change its action to **Observe** or **Disable**.

- **Observe:** The firewall logs the traffic that matches the current rule and does not block the traffic.
- **Disable:** The firewall does not log or block the traffic that matches the current rule.

----End

References

If traffic was not blocked by IPS but services are still unavailable, rectify the fault by referring to [What Can I Do If Services Cannot Be Accessed After a Policy Is Configured on CFW?](#).

3.6 Why Is the IP Address Translated Using NAT64 Blocked?

A firewall instance cannot protect the real source IP address before NAT64 translation. If you enable IPv6 translation for EIPs, NAT64 will translate a source IP address into a CIDR block of 198.19.0.0/16 for ACL access control.

For IPv6 access, you are advised to allow traffic from the predefined address group **NAT64 Address Set**. Access from all the IP addresses in the 198.19.0.0/16 CIDR block will be allowed. You can configure the blacklist or a blocking policy to block specific IP addresses.

- For details about the IPv6 EIP function, see [Assigning or Releasing an IPv6 EIP](#).
- For details about **NAT64 Address Set**, see [NAT64 Address Set](#).
- For details about how to configure the blacklist, see [Adding an Item to the Blacklist or Whitelist](#).
- For details about how to configure a blocking policy, see [Adding a Protection Rule](#).

3.7 Why Some Permissions Become Invalid After a System Policy Is Granted to an Enterprise Project?

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"
      ]
    }
  ]
}
```

3.8 What Do I Do If a Message Indicating Insufficient Permissions Is Displayed When I Configure LTS Logs?

After you configure logs on the **Log Management** page, if a message indicating insufficient permissions is displayed, you need to add the **LTS FullAccess** permission.

Symptom

On the **Log Management** page, a message indicating insufficient permissions is displayed.

Possible Causes

On the **Log Management** page, you can dump logs to Log Tank Service (LTS). All operations on this page need to call LTS APIs and require LTS permissions.

Solution

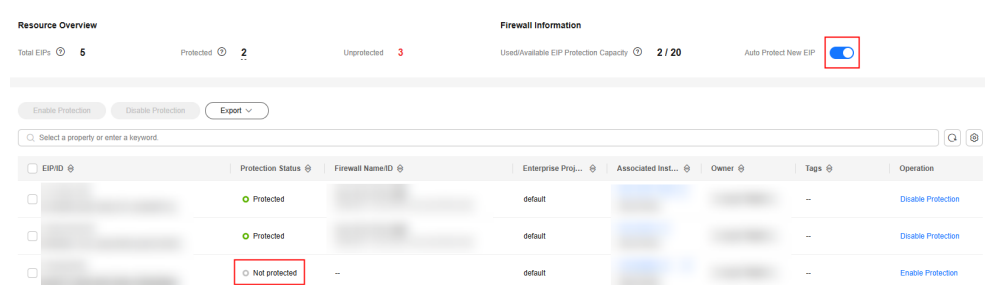
The master account grants the **LTS FullAccess** permission to the member account. For details, see [Granting LTS Permissions](#).

3.9 What Can I Do If Automatic EIP Protection Does Not Take Effect?

Symptom

On the **Assets > EIPs** page, **Auto Protect New EIP** is enabled, but the newly purchased EIP is not protected by CFW. That is, the **Protection Status** of the EIP is **Unprotected**.

Figure 3-10 Auto EIP protection failure



Possible Causes

Protection is not provided immediately after **Auto Protect New EIP** is enabled. CFW synchronizes EIPs on the hour and enable protection for new EIPs only after the synchronization.

Solution

- To enable protection for the EIPs under the same account as the firewall, you can wait for CFW to automatically enable protection or manually enable it. For more information, see [Enabling Internet Border Traffic Protection](#).
- To enable protection for the EIPs under other accounts, perform the following operations:
 - If you have accessed the **Assets > EIPs** page before automatic synchronization, CFW will automatically synchronize EIPs, but will not auto-protect the EIPs under other accounts. In this case, you need to manually enable EIP protection. For details, see [Enabling Internet Border Traffic Protection](#).
 - If you have not accessed the **Assets > EIPs** page, wait for CFW to automatically synchronize EIPs on the hour and enable protection for new EIPs.

4 Network Traffic

4.1 How Do I Calculate the Number of Protected VPCs and the Peak Protection Traffic at the VPC Border?

Pay-per-use firewalls are charged based on the actual protection status. The maximum bandwidth of a pay-per-use firewall (total traffic that can pass through the firewall) is 1 Gbit/s.

Yearly/Monthly CFW: By default, the CFW professional edition protects two VPCs, providing 200 Mbit/s protection for VPC border traffic. To protect more inter-VPC traffic, you can purchase more VPC protection quotas. Each quota provides 200 Mbit/s protection for VPC border traffic.

For example, CFW protects two VPCs (200 Mbit/s in total) by default. To protect 1 Gbit/s VPC border traffic, you need to purchase four more quotas (4 x 200 Mbit/s). The VPC border protection traffic = Default protection traffic (200 Mbit/s) + 4 x VPC protection quotas (200 Mbit/s) = 1 Gbit/s.

4.2 How Does CFW Collect Traffic Statistics?

CFW collects traffic statistics in the following dimensions:

- Traffic
You can view the traffic trend in the **Traffic Trend** area on the **Dashboard** page. Data is updated in real time.
- Session. Traffic statistics are collected at the end of a session.
 - Choose **Log Audit > Log Query** and click the **Traffic Logs** tab. The total traffic from the start to the end of a session is displayed. Data about a session is not reported until the session is terminated.
 - View data on any page under the **Traffic Analysis** menu item. The data displayed is the average bits per second (bps) of sessions that end at the specified time in traffic logs.

4.3 What Is the Protection Bandwidth Provided by CFW?

CFW protects traffic exchanged between the Internet border and VPCs. You can increase the protection bandwidth as required. CFW protection bandwidth varies according to the edition you purchase.

- Internet direction: 10 Mbit/s for the standard edition, and 50 Mbit/s for the professional edition by default
- Inter-VPC protection: No protection bandwidths are provided in the standard edition. The professional edition protects 200 Mbit/s traffic per month by default.

NOTE

- The value of the protection bandwidth in the Internet direction is the maximum value of inbound or outbound traffic. For example, if you purchase a 50 Mbit/s protection bandwidth, 50 Mbit/s inbound or outbound traffic can be protected.
- If your traffic is higher than the current protection bandwidth, purchase more protection capacity. For details, see [Modifying Extension Packages](#).

4.4 What Do I Do If My Service Traffic Exceeds the Protection Bandwidth?

If your actual service traffic exceeds the protection bandwidth you purchased, your traffic may be limited, packets may be discarded randomly, and CFW may be bypassed automatically. Some of your services may be unavailable, frozen, or may respond very slowly.

In this case, purchase more protection capacity as needed to provide sufficient protection bandwidth. If your service traffic fluctuates greatly, determine the protection bandwidth to purchase based on the maximum value of **Outbound 95th Percentile Bandwidth** or **Inbound 95th Percentile Bandwidth** in the **Operations Dashboard** of the **Dashboard** page.

For details about how to purchase an expansion package, see [Adding the EIP Protection Capacity](#).

NOTE

- You can configure high traffic warning in CFW. An alarm will be sent if your service traffic reaches the specified proportion of purchased bandwidth. For more information, see [Alarm Notification](#).
- 95th percentile bandwidth: The system collects bandwidth in every statistical period, and sorts the bandwidth values in descending order, and removes the top 5% bandwidth values. The remaining maximum bandwidth is the 95th percentile bandwidth.

For example, if the 95th percentile bandwidth in the outbound direction is 100 bit/s, that means after the bandwidth values are sorted in descending order and the highest 5% value is removed within a certain period of time (for example, 24 hours), the remaining maximum bandwidth is 100 bit/s.

4.5 What Are the Differences Between the Data Displayed in Traffic Trend Module and the Traffic Analysis Page?

The methods of collecting traffic statistics on the two modules are different.

- The **Traffic Trend** area on the **Dashboard** page displays the inbound, inter-VPC, and outbound traffic based on traffic statistics in real time.
- The **Traffic Analysis** module displays traffic statistics collected from sessions. The statistics of a session is reported only after the session is terminated. The following traffic data is displayed:
 - **Inbound Traffic**
 - **Outbound Traffic**
 - **Inter-VPC Access**

4.6 How Do I Verify the Validity of an Outbound HTTP/HTTPS Domain Protection Rule?

To verify the validity, perform the following steps:

Step 1 Send an HTTP or HTTPS request.

- Method 1: Use the **curl** command. For example:

```
curl -k "https://www.example.com"
```
- Method 2: Use a browser to access the domain name.

CAUTION

Do not run the **telnet** command to test the domain name.

If the **telnet** command is used to test the domain name and port (for example, **telnet www.example.com 80**), only TCP handshake traffic is generated, and no complete HTTP or HTTPS requests will be simulated. In this case, the application type will be identified as unknown and will not hit the HTTP or HTTPS application policy.

Step 2 Log in to the console and view the number of hits and log records of the protection rule. If new hits and records are found, the rule takes effect. If not, modify the protection rule in a timely manner.

1. In the navigation pane on the left, choose **Access Control > Internet Border Protection Rules** or **VPC Border Protection Rules**. On the **Protection Rules** tab page, view the number of rule hits.
2. Choose **Log Audit > Log Query**. On the **Access Control Logs** tab, view the protection records of the rule.

----End

4.7 How Do I Obtain the Real IP Address of an Attacker?

After traffic passes through the reverse proxy, the source IP address is translated into the back-to-origin IP address. In this case, if an external attack occurs, CFW cannot obtain the real IP address of the attacker based on the source IP address. You can obtain the real IP address based on the **X-Forwarded-For** field in attack event logs.

Viewing X-Forwarded-For



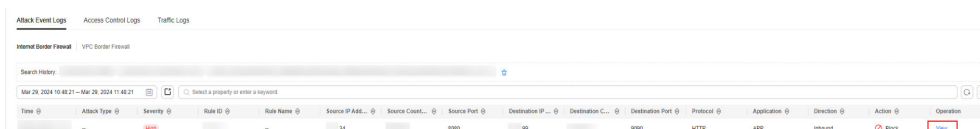
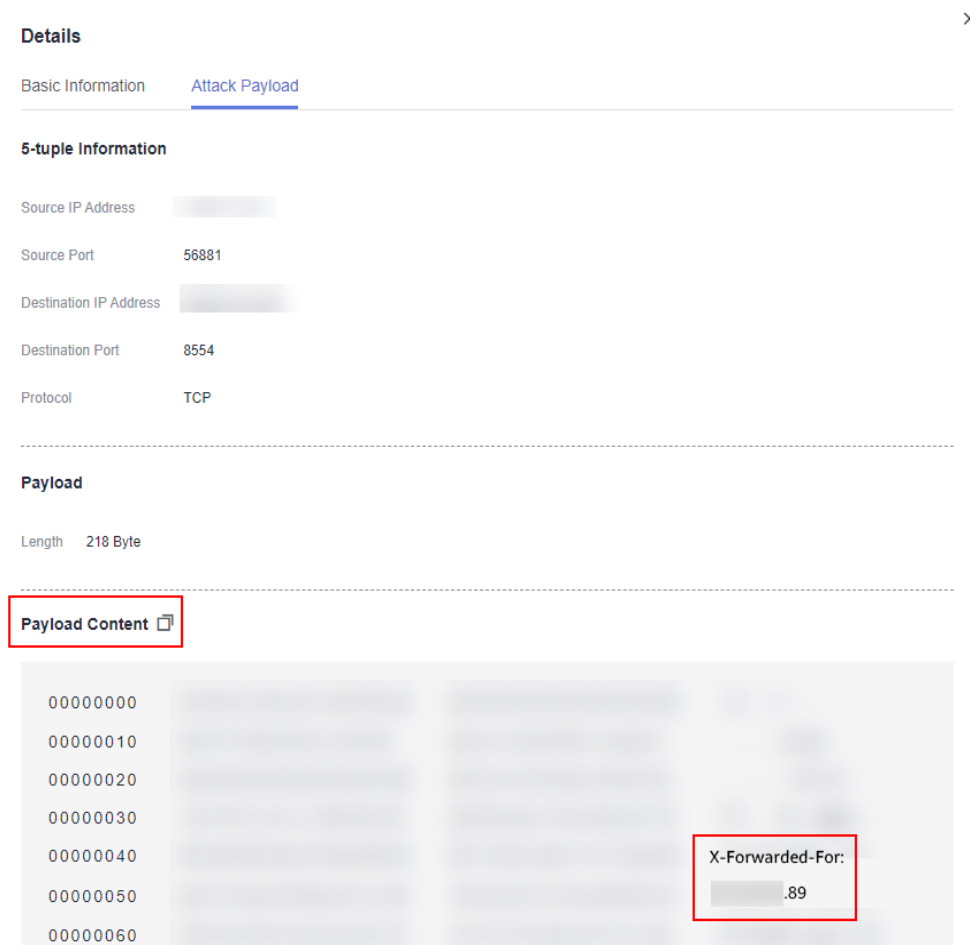
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
- Step 4** (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.
- Step 5** In the navigation pane, choose **Log Audit > Log Query**. Click **Attack Event Logs** tab. In the **Operation** column of the target event, click **View**.

Figure 4-1 Viewing Attack Event Log Details



Time	Attack Type	Severity	Rule ID	Rule Name	Source IP Address	Source Port	Destination IP	Destination Port	Protocol	Application	Direction	Action	Operation
Mar 28, 2024 10:42:21 - Mar 28, 2024 11:42:21	High				14	8080	88	8080	HTTP	APP	Inbound	Block	View

- Step 6** In the **Details** page, click the **Attack Payload** tab, and obtain the value of **X-Forwarded-For** field.
- Method 1: Check **X-Forwarded-For** (all IP addresses from the client to the last proxy server) in the **Payload Content** area.

Figure 4-2 X-Forwarded-For in the payload

- Method 2: Copy the **Payload Content** and use the Base64 tool to obtain the decoding result.
 - **X-Forwarded-For**: all IP addresses from the client to the last proxy server
- For example, the client IP address obtained in [Example of the Base64 decoding result](#) is **xx.xx.xx.89**, and only cloud WAF is used.

Figure 4-3 Example of the Base64 decoding result

```
dGET /api/dbstat/gettablessize HTTP/1.1
X-Real-IP: .89
X-Hwaf-Real-IP: .89
X-Hwaf-Client-IP: .89
X-Forwarded-For: .89
Host: abc.def.gh.net
X-Forwarded-Proto: https
X-CloudWAF-Traffic-Tag: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/ Safari/537.36
Referer: http://c.bookmall.top/api/dbstat/gettablessize
Accept-Encoding: gzip
```

----End

4.8 What Do I Do If a High Traffic Warning Is Received?

Scenario

If you configured the alarm notification function and received the high traffic warning by an email or SMS message, your actual service traffic has reached the threshold and is about to exceed the peak protection traffic.

Handling Method

If your actual service traffic exceeds the peak protection traffic that you have purchased, packet loss may occur. You are advised to:

- Purchase an expansion package. For details about how to purchase an expansion package, see [Modifying Extension Packages](#).
- Reduce protection objects in a timely manner. For details about how to disable EIP protection, see [Disabling EIP Protection](#).