

Cloud Firewall

Practices

Issue 04
Date 2024-11-04



Copyright © Huawei 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 Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks 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 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 CFW Best Practice Summary.....	1
2 Purchasing and Querying CFW via API.....	2
3 Migrating Security Policies to CFW in Batches.....	5
4 Configuration Suggestions for Using CFW with WAF, Advanced Anti-DDoS, and CDN.....	9
5 Allowing Internet Traffic Only to a Specified Port.....	13
6 Allowing Outbound Traffic from Cloud Resources Only to a Specified Domain Name.....	16
7 Using CFW to Defend Against Network Attacks.....	19
7.1 Using CFW to Defend Against Access Control Attacks.....	19
7.2 Using CFW to Defend Against Hacker Tools.....	21
7.3 Using CFW to Defend Against Suspicious DNS Activities.....	22
7.4 Using CFW to Defend Against Trojans.....	24
7.5 Using CFW to Defend Against Vulnerability Exploits.....	26
7.6 Using CFW to Defend Against Worms.....	27

1 CFW Best Practice Summary

This section summarizes the common application scenarios of Cloud Firewall (CFW) and provides detailed solutions and operation guide to help you easily protect cloud services.

CFW Best Practices

Table 1-1 CFW best practices

Category	Reference
Purchasing CFW via API	Purchasing and Querying CFW via API
Batch migration policy	Migrating Security Policies to CFW in Batches
Using CFW together with other cloud services such as WAF	Configuration Suggestions for Using CFW with WAF, Advanced Anti-DDoS, and CDN
Configuring intrusion prevention	Using CFW to Defend Against Access Control Attacks
	Using CFW to Defend Against Hacker Tools
	Using CFW to Defend Against Suspicious DNS Activities
	Using CFW to Defend Against Trojans
	Use CFW to Defend Against Vulnerability Exploits
	Using CFW to Defend Against Worms

2 Purchasing and Querying CFW via API

Application Scenarios

For professionals, using APIs is more efficient than using the console. CFW provides APIs for diverse functions. For details, see [APIs](#).

You can use APIs to quickly purchase and query standard edition firewall instances.

Prerequisites

The current account has the BSS Administrator and CFW FullAccess permissions.

Purchasing and Querying a Standard Edition Firewall

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

Step 2 Choose **Tools > API Explorer** in the upper right corner.

Step 3 In the navigation pane on the left, click **All Products** and choose **Security & Compliance > Cloud Firewall**.

Step 4 Buy a standard firewall. Select the **Create Firewall** API, set the key parameters as follows, and set other parameters as required.

- **Region**: Select the region where the cloud asset is located.
- **project_id**: project ID, which is automatically obtained.
- **flavor**: Enter flavor information.
 - **version**: firewall edition. In this example, select **Standard**. For details about the differences between editions, see [Editions](#).
- **charge_info**: Enter the billing mode.
 - **charge_mode**: Enter the billing mode information. In this example, the billing mode is yearly/monthly. Set this parameter to **prePaid**.
 - **is_auto_renew**: Whether to automatically renew the subscription. In this example, the subscription period is one month. Select **false**.
 - **is_auto_pay**: Whether automatic payment is enabled. In this example, select **true**.

Step 5 Query a purchased firewall. Select **ListFirewallList** API, set the key parameters as follows, and set other parameters as required.

- **Region:** Select the region where the firewall is located.
- **project_id:** project ID, which is automatically obtained.
- **key_word:** Enter a keyword, for example, a firewall name.
- **limit:** Set the number of records displayed on each page. In this example, set it to 1.
- **offset:** Set the start position of the returned record. Set it to 0.

----End

Code Example

Prepare basic authentication information.

- **ak:** Access key of the Huawei account. For details, see [How Do I Obtain an Access Key \(AK/SK\)?](#)
- **sk:** Secret access key of the Huawei account. For details, see [How Do I Obtain an Access Key \(AK/SK\)?](#)

```
import com.huaweicloud.sdk.cfw.v1.CfwClient;
import com.huaweicloud.sdk.cfw.v1.model.*;
import com.huaweicloud.sdk.cfw.v1.region.CfwRegion;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;

import java.util.ArrayList;
import java.util.List;

public class CreateFirewallSolution {

    public static void main(String[] args) {
        String ak = "xxx";
        String sk = "xxx";

        BasicCredentials auth = new BasicCredentials().withAk(ak).withSk(sk);

        CfwClient client = CfwClient.newBuilder()
            .withCredential(auth)
            .withRegion(CfwRegion.valueOf("xxx"))
            .build();

        //Request body for creating a firewall.
        CreateFirewallRequest request = new CreateFirewallRequest();
        CreateFirewallReq body = new CreateFirewallReq();
        body.setName("cfwtest");
        body.setEnterpriseProjectId("0");
        CreateFirewallReqTags createFirewallReqTags = new CreateFirewallReqTags();
        createFirewallReqTags.setKey("TagKey");
        createFirewallReqTags.setValue("TagValue");
        List<CreateFirewallReqTags> createFirewallReqTagsList = new ArrayList<>();
        createFirewallReqTagsList.add(createFirewallReqTags);
        body.setTags(createFirewallReqTagsList);
        CreateFirewallReqFlavor flavor = new CreateFirewallReqFlavor();
        flavor.setVersion(CreateFirewallReqFlavor.VersionEnum.STANDARD);
        body.setFlavor(flavor);
        CreateFirewallReqChargeInfo createFirewallReqChargeInfo = new CreateFirewallReqChargeInfo();
        createFirewallReqChargeInfo.setChargeMode("prePaid");
        createFirewallReqChargeInfo.setPeriodType("month");
        createFirewallReqChargeInfo.setPeriodNum(1);
        createFirewallReqChargeInfo.setIsAutoPay(true);
        createFirewallReqChargeInfo.setIsAutoRenew(true);
        body.setChargeInfo(createFirewallReqChargeInfo);
        request.setBody(body);
```

```
//Request body for querying a firewall.
ListFireWallListRequest listFireWallListRequest = new ListFireWallListRequest();
QueryFireWallInstanceDto queryFireWallInstanceDto = new QueryFireWallInstanceDto();
queryFireWallInstanceDto.setOffset(0);
queryFireWallInstanceDto.setLimit(1);
queryFireWallInstanceDto.setKeyWord("cfwtest");
listFireWallListRequest.setBody(queryFireWallInstanceDto);
try {
    //Create a firewall.
    CreateFireWallResponse createFireWallResponse = client.createFireWall(request);
    System.out.println(createFireWallResponse.toString());

    ///Query the firewall list.
    ListFireWallListResponse listFireWallListResponse = client.listFireWallList(listFireWallListRequest);
    System.out.println(listFireWallListResponse.toString());
} catch (ConnectionException e) {
    System.out.println(e.getMessage());
} catch (RequestTimeoutException e) {
    System.out.println(e.getMessage());
} catch (ServiceResponseException e) {
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```


3 Migrating Security Policies to CFW in Batches

Application Scenarios

If services need to be migrated to Huawei Cloud, or security policies need to be replaced with CFW, you can quickly add security policies by importing security policies in batches.

Precautions

- If the networking changes during rules migration, you need to rewrite the network information (such as the IP address) in the original policy.
- To reduce the impact of security rules migration on services, you are advised to disable all rules (especially the blocking rules). After the template is imported and the rules are correctly configured, enable the rules.
- The priority of the imported rules is lower than that of the created rules.
If you need to allow specified traffic, allow the rules of CFW, network ACL, and security groups.
- If you need to import and reference an object group (such as an IP address group), enter the group information in the corresponding information table (such as the address information table) and then reference the group in the protection rule table.

Migrating Outbound Blocking Rules in Batches


Step 1 Export the rule configuration file from other firewalls through the API/policy backup function.


For example, export the following rule:

- rule id: 123
- src-zone: trust
- dst-zone: untrust
- src-addr: 0.0.0.0/0
- dst-addr: xx.xx.xx.9

- service: SSH
- action: deny
- name: example123

Step 2 [Log in to the management console.](#)

Step 3 Click  in the upper left corner of the management console and select a region or project.

Step 4 In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.

Step 5 (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 of a firewall to go to its details page.

Step 6 In the navigation pane, choose **Access Control > Access Policies**.

Step 7 Click **Download Center** on the upper right corner of the list.

Step 8 Click **Download Template** to download the rule import template to the local host.

Step 9 Set parameters in the template.

- Order: 1
- Acl Name: example123
- Protection Rule: EIP protection
- Direction: Outbound
- Action Type: Block
- ACL Address Type: IPv4
- Status: Disable
- Description: An example
- Source Address Type: IP address
- Source Address: 0.0.0.0/0
- Destination Address Type: IP address
- Destination Address: xx.xx.xx.9
- Service Type: Service
- Protocol/Source Port/Destination Port: TCP/1-65535/22

Step 10 After filling in the template, click **Import Rule** to import the template.

Step 11 Enable the policy. You are advised to enable the policies that do not affect main services.



Step 12 Check whether there are rule matching records in the logs. For details about how to query access logs, see [Querying Logs](#).

- If there are hit records, the rule has taken effect.
- If there are no hit records, perform the following steps:
 - a. Enable protection on the resources specified in the policy. For details about how to enable protection for EIPs, see [Enabling EIP Protection](#).

- b. Check whether a rule with a higher priority is matched. For details about how to set the priority of rules, see [Configuring a Rule Priority](#).
- c. On the **Access Policies** page, check whether any delivery failure error is reported.

----End

Migrating Address Group Members and Domain Group Members in Batches

- Step 1** Export the rule configuration file from other firewalls through the API/policy backup function.
- Step 2** [Log in to the management console](#).
- Step 3** Click  in the upper left corner of the management console and select a region or project.
- Step 4** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
- Step 5** (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 of a firewall to go to its details page.
- Step 6** In the navigation pane, choose **Access Control > Access Policies**.
- Step 7** Click **Download Center** on the upper right corner of the list.
- Step 8** Click **Download Template** to download the rule import template to the local host.
- Step 9** Set parameters in the template.
 - **Address-Table:**
 - IP Address Group Name: address group 1
 - IP Address Group Description: service A
 - Address Set Address Type: IPv4
 - IP Address Items
 - IP Address: 10.1.1.2; Description: ECS1
 - IP Address: 10.1.1.3; Description: ECS2
 - IP Address: 10.1.1.4; Description: ECS3
 - **Domain-Table:**
 - Domain Set Name: domain group 1
 - Domain Set Type: URL filtering
 - Domain Set Description: external access domain name of service A
 - Domain Items:
 - Domain Address: www.example.test.api; Domain Description: api
 - Domain Address: www.test.example.com; Domain Description: a domain name

- Domain Address: www.example.example.test; Domain Description: XX system
- **Rule-ACL-Table:**
 - Order: 1
 - ACL Name: service A external connection
 - Protection Rule: NAT protection
 - Direction: Outbound
 - Action Type: Allow
 - ACL Address Type: IPv4
 - Status: Disable
 - Source Address Type: IP address group
 - Source Address Group Name: address group 1
 - Destination Address Type: domain group
 - Destination Address Group Name: domain group 1
 - Service Type: Service
 - Protocol/Source Port/Destination Port: TCP/0-65535/8080

Step 10 After filling in the template, click **Import Rule** to import the template.

Step 11 Enable the policy. You are advised to enable the policies that do not affect main services.

Step 12 Check whether there are rule matching records in the logs. For details about how to query access logs, see [Querying Logs](#).

- If there are hit records, the rule has taken effect.
- If there are no hit records, perform the following steps:
 - a. Enable protection on the resources specified in the policy. For details about how to enable protection for EIPs, see [Enabling EIP Protection](#).
 - b. Check whether a rule with a higher priority is matched. For details about how to set the priority of rules, see [Configuring a Rule Priority](#).
 - c. On the **Access Policies** page, check whether any delivery failure error is reported.

----End

References

- Import security policy parameters. For details about the parameters, see [Parameters of Rule Import Template](#).
- Periodically check rule hits on the policy assistant page or in custom security reports.

The policy assistant and security reports display the rule matching trend and top *N* matched rules, helping you locate abnormal rules in a timely manner.

- For details about the policy assistant, visit [Policy Assistant](#).
- For details about security reports, see [Security Reports](#).

4 Configuration Suggestions for Using CFW with WAF, Advanced Anti-DDoS, and CDN

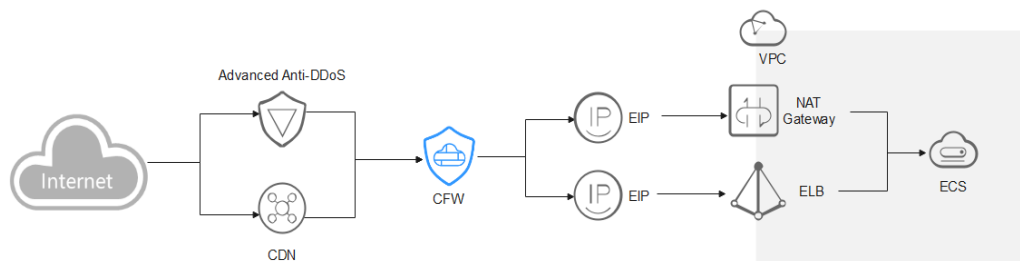
This section describes where CFW is deployed in the network architecture for inbound cloud traffic protection and how to configure CFW when it is used with other Huawei Cloud services.

Overview

Web Application Firewall (WAF), Advanced Anti-DDoS (AAD), and Content Delivery Network (CDN) work as reverse proxies. If these services are deployed, the source IP addresses received by CFW is the back-to-origin IP addresses returned by these services.

If other Huawei Cloud products are configured, traffic will be protected by multiple services. For inbound traffic protection, if a reverse proxy service, such as Content Delivery Network (CDN), Anti-DDoS Service (AAD), or cloud Web Application Firewall (cloud WAF), is deployed before CFW, you need to configure a policy that allows back-to-source IP addresses to avoid misblocking. If a dedicated or load-balancing WAF instance is purchased, configure it as needed.

AAD/CDN



You are advised to create a protection rule to allow access from back-to-source IP addresses, or add these IP addresses to the whitelist.

- Creating a rule: Create a policy with the highest priority to allow all back-to-origin IP addresses. In this way, traffic still goes to CFW for check.

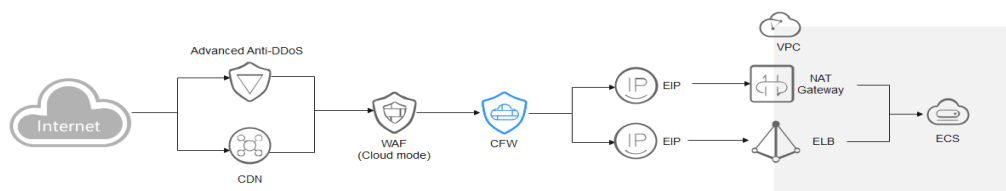
- Adding to whitelist: After back-to-source IP addresses are added to the **whitelist**, the traffic will be directly allowed to pass through, and CFW does not perform any protection.

After traffic passes through the reverse proxy, a source IP address is translated into a back-to-source IP address. If an external attack occurs, CFW cannot obtain the real IP address of an attacker. In this case, you can obtain the real IP address based on the **X-Forwarded-For** field. For details, see

CAUTION

You are not advised to block back-to-origin IP addresses or add them to a blacklist. Otherwise, all traffic from such IP addresses will be blocked and your services may be affected.

Cloud WAF



You are advised to create a protection rule to allow access from back-to-source IP addresses, or add these IP addresses to the whitelist.

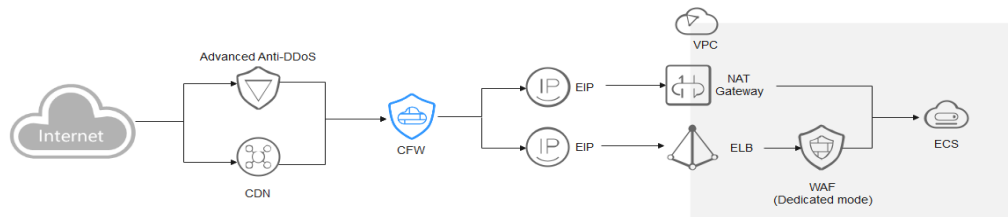
- Creating a rule: Create a policy with the highest priority to allow all back-to-origin IP addresses. In this way, traffic still goes to CFW for check.
- Adding to whitelist: After back-to-source IP addresses are added to the **whitelist**, the traffic will be directly allowed to pass through, and CFW does not perform any protection.

After traffic passes through the reverse proxy, a source IP address is translated into a back-to-source IP address. If an external attack occurs, CFW cannot obtain the real IP address of an attacker. In this case, you can obtain the real IP address based on the **X-Forwarded-For** field. For details, see

CAUTION

You are not advised to block back-to-origin IP addresses or add them to a blacklist. Otherwise, all traffic from such IP addresses will be blocked and your services may be affected.

Dedicated WAF



Traffic passes through CFW and then WAF. The log viewing method varies depending on the protection scenario.

- You have enabled CFW protection for the EIPs bound to public network ELB load balancers.

If there is an attack from the client, CFW prints the attack event on the **Internet Border Firewall** tab under **Attack Event Logs**.

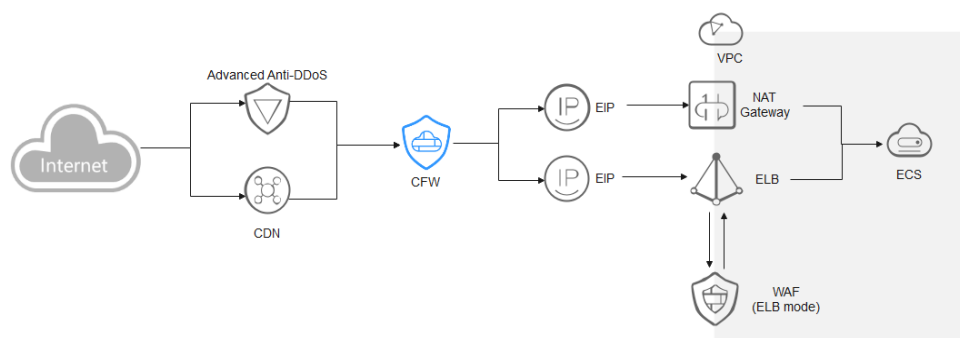
The destination IP address of the event is the EIP bound to the public ELB load balancer, and the source IP address is the IP address of the client.

- You have enabled VPC border firewall and associated with the VPC where the origin server resides. No protection is enabled for EIPs bound to the ELB load balancer.

If there is an attack from the client, CFW prints the attack event on the **VPC Border Firewall** tab under **Attack Event Logs**.

The destination IP address of the event is the private IP address of the origin server, and the source IP address is the private IP address of the traffic ingress (such as the Nginx server).

ELB-mode WAF



The traffic passes through CFW and then WAF. Configure services as needed.

References

- Add a protection rule. For details, see [Adding a Protection Rule](#).
- For details about how to set the whitelist, see [Managing the Blacklist and the Whitelist](#).
- For details about the protection sequence, see [What Are the Priorities of the Protection Settings in CFW?](#)

- Obtain the back-to-source IP address of WAF. For details, see [Step 2: Whitelisting WAF IP Addresses](#).


5 Allowing Internet Traffic Only to a Specified Port

Application Scenarios

For security purposes, you need to allow traffic only from certain ports (such as ports 80 and 443) to access cloud resources.

This section describes how to configure CFW for refined management and control on cloud resources, allowing all EIPs to access port 80 of an EIP (*xx.xx.xx.1*).

Procedure

- Step 1** Purchase the CFW standard or professional edition. For details, see [Purchasing CFW](#).
- Step 2** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
- Step 3** (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 of a firewall to go to its details page.
- Step 4** Enable protection for the EIP (*xx.xx.xx.1*).
1. In the navigation pane, choose **Assets > EIPs**. The EIPs page is displayed. The EIP information is automatically updated to the list.
 2. In the row of the EIP (*xx.xx.xx.1*), click **Enable Protection** in the **Operation** column.
- Step 5** Configure protection rules.
1. In the navigation pane, choose **Access Control > Access Policies**.
 2. Click **Add Rule**. On the **Add Rule** page, configure protection information and set other parameters as needed.
- Configure the following protection rules:
- One of the rule blocks all traffic, as shown in [Figure 5-1](#). The priority is the lowest.

- **Direction: Inbound**
- **Source: Any**
- **Destination: Any**
- **Service: Any**
- **Application: Any**
- **Action: Block**

Figure 5-1 Blocking all traffic

The screenshot shows the configuration for a Cloud Firewall rule. The rule is named "Blocking all traffic". The configuration is as follows:

- Matching Condition:** View Configuration Guide
- Direction:** Inbound (selected), Outbound
- Source:** IP Address (selected), IP address group, Any. Value: .48
- Destination:** IP Address, IP address group, Countries and regions, Domain Name/Domain Group (selected), Any. Value: Application Do..., X_platform
- Service:** Service (selected), Service group. Value: TCP/1-65535/80, TCP/1-65535/443
- Application:** Application (selected). Value: HTTP, HTTPS
- Protection Configuration:** Protection Action: Allow (selected), Block

- The other rule allows the traffic to port 80 of the EIP (*xx.xx.xx.1*), as shown in [Figure 5-2](#). The priority is the highest.
 - **Direction: Inbound**
 - **Source: Any**
 - **Destination: Select IP address** and enter *xx.xx.xx.1*.
 - **Service: TCP/1-65535/80**
 - **Application: Any**
 - **Action: Allow**

Figure 5-2 Allowing access traffic to port 80 of xx.xx.xx.1

Matching Condition [View Configuration Guide](#)

Direction

Inbound
Accessing cloud assets from the Internet

Source: Internet → CFW → Destination: EIP

Outbound
Accessing the Internet from cloud assets

Source: EIP → CFW → Destination: Internet

Source ? IP address IP address group Countries and regions Any ?

Destination ? IP address IP address group Any ?

.1 ×

Service ? Service Service group Any ?

TCP/1-65535/80 ×

Application ? Application Any

Protection Action

Action

Step 6 View the rule hits in access control logs.

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

NOTE

In the rows where **Destination IP** is *xx.xx.xx.1*, the corresponding **Action** is **Block**.

----End

References

For details about how to add other protection rules, see the parameter description in [Adding a Protection Rule](#).

6 Allowing Outbound Traffic from Cloud Resources Only to a Specified Domain Name


Application Scenarios

To prevent sensitive data leakage or external attacks, you need to restrict the Internet domain names that can be accessed by cloud resources.

Use CFW to implement refined management and control on cloud resources and allow access traffic from all EIPs to ports 80 and 443 of a specified domain name. (Wildcard domain name *.example.com is used as an example).

Procedure

Step 1 Purchase the CFW standard or professional edition. For details, see [Purchasing CFW](#).

Step 2 In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.

Step 3 (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 of a firewall to go to its details page.

Step 4 Enable protection for an EIP.

1. In the navigation pane, choose **Assets > EIPs**. The EIPs page is displayed. The EIP information is automatically updated to the list.
2. In the row of the EIP, click **Enable Protection** in the **Operation** column.

Step 5 Configure protection rules.

1. In the navigation pane, choose **Access Control > Access Policies**.
2. Click **Add Rule**. On the **Add Rule** page, configure protection information and set other parameters as needed.

Configure the following protection rules:

- One of the rule blocks all traffic. The priority is the lowest.
 - **Direction: Outbound**

- **Source: Any**
 - **Destination: Any**
 - **Service: Any**
 - **Application: Any**
 - **Protection Action: Block**
- The other rule allows the traffic to ports 80 and 443 of *.example.com, as shown in [Figure 6-1](#). The priority is the highest.
- **Direction: Outbound**
 - **Source: Any**
 - **Destination:** Select **Domain name/domain group** and then **Application**. Select **Domain name** from the drop-down list and enter *.example.com.
 - **Service:** TCP/1-65535/80 and TCP/1-65535/443
 - **Application:** HTTP and HTTPS
 - **Action: Allow**

Figure 6-1 Allowing the access traffic to a domain name

Matching Condition [View Configuration Guide](#)

Direction

Inbound

Accessing cloud assets from the Internet

Source: Internet → CFW → Destination: EIP

Outbound

Accessing the Internet from cloud assets

Source: EIP → CFW → Destination: Internet

Source ? IP address IP address group Any ?

Destination ? IP address IP address group Countries and regions Domain Name/Domain Group Any ?

Application Network

The HOST or SNI field is used for domain name access control. HTTP, HTTPS, TLS1, SMTPS, and POP3S applications are supported.

Domain name ▼

Service ? Service Service group ?

TCP/1-65535/80 × TCP/1-65535/443 ×

Application ? Application

HTTP × HTTPS × ▼

Protection Action

Action Allow Block

Step 6 View the rule hits in access control logs.

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

 NOTE

In the rows where **Destination IP** is a domain name matching **example.com**, the corresponding **Action** is **Allow**. For other traffic, the **Action** is **Block**.

----End

References

- For details about how to configure a domain name group, see .
- For details about how to add other protection rules, see the parameter description in [Adding a Protection Rule](#).

7 Using CFW to Defend Against Network Attacks

7.1 Using CFW to Defend Against Access Control Attacks

You can use CFW to defend against access control attacks.

Application Scenarios

Access control is a key method to protect system resources from unauthorized access. It restricts users' or processes' access to system resources to enhance system security. Attackers may try to bypass or invalidate control measures to implement unauthorized access.

The IPS rule library of CFW provides rules to defend against access control attacks. It can effectively identify and block such behaviors that bypass or damage the system access control mechanism, reducing the risk of such attacks.

What Is an Access Control Attack?

In access control attacks, attackers exploit access control vulnerabilities in systems or applications to illegally obtain or elevate their access permissions in the systems or applications, perform unauthorized operations, or access sensitive resources.

Common access control attacks include:

- **Unauthorized access attack**
 - Vertical privilege escalation: Common users can access or operate resources or functions that require administrator permissions.
 - Horizontal privilege escalation: A user can access or operate resources or functions that only another user has permissions for.
 - Multi-phase privilege escalation: In an operation that requires multiple steps (such as fund transfer), an attacker may skip steps and directly perform the last step.

- **Password attack**
 - Brute-force attack: Attackers crack usernames and passwords by attempting all possible combinations, including pure brute-force attacks (blanket search) and dictionary-based brute-force attacks (using a password dictionary).
 - Rainbow table attack: A batch processing dictionary attack implemented by searching the pre-generated password and hash string mapping table to crack the password.
- **Session hijacking**

An attacker obtains the session ID of a user, uses the session ID to log in to the target account, and performs unauthorized operations. This usually takes place when the user session identifier is leaked or predicted.
- **Access aggregation attack**

A method that is often used in in-depth testing. It collects multiple pieces of non-sensitive information, combines the information to obtain sensitive information, and compares the information to complete an attack.

Harms of Access Control Attacks


Access control attacks severely threaten system security. The major impacts are as follows:


- **Data leakage:** Attackers can bypass the access control mechanism to obtain sensitive data, such as personal information and financial data, without authorization.
- **Data tampering:** Attackers can bypass the access control mechanism to tamper with system data, generating false and unreliable data.
- **System breakdown:** Attackers can bypass the access control mechanism to obtain administrator rights in the system, causing the system to be damaged or crashed.
- **Information security risks:** Access control attacks damage the security mechanism in the system and increase information security risks, such as malware, virus, and Trojan attacks.

How to Defend Against Access Control Attacks

In addition to access control policy design, identity authentication, security audit and monitoring, security configuration and patch management, access control, vulnerability defense, security training and awareness improvement, and security technologies and tools, you can use the CFW intrusion prevention function to block access control attacks.

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) 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 of a firewall to go to its details page.
- Step 5** In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **View Effective Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.
- Step 6** Filter the rules for access control prevention. In the filter above the list, select **Access-Control** from the **Attack Types** drop-down list.
- Step 7** Enable protection in batches. Select multiple rules at a time and click **Intercept**.

 **NOTE**

Intercept: The firewall records the traffic that matches the current rule in attack event logs and blocks the traffic.

----End

7.2 Using CFW to Defend Against Hacker Tools

You can use CFW to defend against hacker tool attacks.

Application Scenarios

Attackers may use hacker tools to intrude computer systems or networks, which may cause computer system or network damage, data leakage, network breakdown, or even serious legal consequences and security risks.

CFW provides intrusion prevention rules to effectively identify and block various hacker tool attacks, such as port scanning, remote control, Trojans, and network listening.

What Is a Hacker Tool?

A hack tool is a malware program used to launch network attacks. It is usually installed by hackers or malicious programs on victims computers to steal sensitive information, damage the system or network, and remotely control computers or networks. Hacker tools can also be legally used by security researchers to test the security of a system or network.

Hacker tools have the following characteristics:

- **Covert:** Hacker tools are usually designed to be very covert. They may disguise as legitimate software or services, or exist in other forms that cannot be easily detected, so that attacks can be launched stealthily.
- **Complex:** There are diverse hacker tools, including but not limited to port scanners, vulnerability scanners, password crackers, remote control software, Trojans, and network listening tools, which can be used in different scenarios.
- **Easy to use:** Hacker tools can be used to implement complex attacks or penetration through simple operations. A large number of hacker tools are shared on the Internet. Most of the tools provide detailed instructions and are easy to use. As a result, the technical threshold for using hacker tools is lowered. Attackers can use these tools to launch attacks even if they have no professional knowledge.

- **Destructive:** Hacker tools are highly destructive. They can be used for diverse attacks, penetration, and cracking; and can quickly detect and exploit vulnerabilities of target systems to efficiently launch attacks.


Harms of Hacker Tools


Abuse of hacker tools may bring huge security risks and economic losses to individuals and the society, including but not limited to the following:

- **Information theft:** Hackers can steal personal and privacy information, such as accounts and passwords, bank account information, and social media accounts, causing property loss and privacy leakage.
- **System damage:** Hackers can attack computer systems and damage system files and data, causing system breakdown or data loss.
- **Malicious attacks:** Hacker tools can be used to launch malicious attacks, such as DDoS attacks and virus attacks, to make websites inaccessible or crash.
- **Cybercrime:** Hacker tools can be used to carry out criminal activities, such as cyber fraud and cyber extortion, causing social security problems.

How to Defend Against Hacker Tools

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) 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 of a firewall to go to its details page.

Step 5 In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **View Effective Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.

Step 6 Filter the rules for hacker tool prevention. In the filter above the list, select **Hacking-Tool** from the **Attack Types** drop-down list.

Step 7 Enable protection in batches. Select multiple rules at a time and click **Intercept**.

NOTE

Intercept: The firewall records the traffic that matches the current rule in attack event logs and blocks the traffic.

----End

7.3 Using CFW to Defend Against Suspicious DNS Activities

You can use CFW to defend against suspicious DNS activities.

Application Scenarios

DNS is a basic and important part of most Internet requests. Once the DNS system is attacked, network services will be severely affected. Therefore, it is important to ensure DNS security. CFW provides intrusion prevention rules for detecting suspicious DNS activities. When CFW detects suspicious DNS activity intrusions, it can block intrusion activities and attack traffic in real time.

What Is a Suspicious DNS Activity?

A domain name system (DNS) is a query and conversion system used to convert domain names into IP addresses for computer connections. When a user enters the domain name of a website in the browser, the browser sends a domain name resolution request to the DNS server. The DNS server returns the IP address corresponding to the domain name. The user can obtain the corresponding website resource based on the IP address.

Suspicious DNS activities refer to abnormal DNS requests or responses over the network. Attackers exploit DNS defects or send excessive requests to attack DNS. As a result, the DNS sends abnormal requests or responses, causing domain name resolution errors, resolution timeout, or DNS breakdown. This affects user experience and may also bring serious consequences such as economic losses and even legal liabilities.


Common Suspicious DNS Activities and Their Harms


Common suspicious DNS activities and their impacts include but are not limited to the following:

- **DNS cache poisoning:** An attacker exploits the vulnerabilities of a DNS server to take over the DNS server. By tampering with the cache of the DNS server, the attacker redirects user access to malicious websites and launches attacks such as phishing and malware download.
- **DNS buffer overflow:** An attacker exploits the vulnerabilities of the DNS server to send a large amount of malicious data to the cache of the server. As a result, the cache overflows and the malicious data overwrites the original valid data, causing attacks such as DNS response tampering, traffic redirection, and man-in-the-middle attacks.

How to Defend Against Suspicious DNS Activities

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) 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 of a firewall to go to its details page.

Step 5 In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **View Effective Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.

Step 6 Filter the rules for defending against suspicious DNS activities. In the filter above the list, select **Suspicious-DNS-Activity** from the **Attack Types** drop-down list.

Step 7 Enable protection in batches. Select multiple rules at a time and click **Intercept**.

 **NOTE**

Intercept: The firewall records the traffic that matches the current rule in attack event logs and blocks the traffic.

----End

7.4 Using CFW to Defend Against Trojans

You can use CFW to defend against Trojan attacks.

Application Scenarios

Trojans are a type of common network attacks. Trojans are implanted in computers to control the computers, steal user information, and damage computer systems. Trojans are highly disguised and latent, making them difficult to detect and remove.

CFW provides intrusion prevention rules for Trojans, helping you effectively identify and defend against Trojan intrusions.

What Is a Trojan?

Trojans are a type of malware program that invades a computer to implement illegal intents. Trojans usually disguise as legitimate software and induce users to download them. Attackers use Trojans to control users' computer systems and steal personal information, passwords, or other sensitive data, or damage the computer systems.

The difference between Trojans and computer viruses is that Trojans do not replicate themselves, are not infectious, and do not proactively initiate attacks. The main characteristics of Trojans are as follows:

- **Disguised:** Trojans usually disguise as programs or files that seem normal to deceive users into installing or opening them. There are many ways Trojans disguise themselves, for example, use a normal file icon, such as a text, image, or HTML icon; or to use the name of a system file.
- **Hidden:** Once a Trojan is implanted in a computer, it can lurk in the computer for a long time and is not easy to detect and remove, waiting for instructions from the attacker. Trojans are hidden in legitimate programs. When a Trojan is running, its icon is not displayed in the taskbar, and it cannot be easily detected by the task manager.
- **Destructive:** After a Trojan is implanted in a computer, attackers can remotely control the Trojan client to perform a series of illegal behaviors that can cause serious consequences, such as stealing user privacy information, controlling system running, and damaging system data.

Types of Trojans and Their Harms

Common Trojans and their harms include but are not limited to the following:

- **Remote control:** Remote control is a basic function of Trojans. Without the victim's knowledge, an attacker can deliver commands to remotely control the victim's computer and complete attack instructions, such as tampering with files and data and downloading malware.
- **Password theft:** This type of Trojan mainly collects all hidden passwords, such as the accounts and passwords of social accounts and online games, and sends out the password information without the victim's knowledge.
- **Keylogger:** This type of Trojans can record keystrokes, through which an attacker can obtain useful information such as passwords. This type of Trojan is automatically loaded when the OS is started. It can be online or offline, which records users' keystrokes in online or offline states, respectively. Generally, a keylogger Trojan can send recorded information to a controller via email.

How to Defend Against Trojans


The key to defending against Trojans is prevention, that is, blocking attacks before Trojans infect a device and cause losses. In addition to improving cybersecurity awareness, you can also use CFW intrusion prevention rules to defend against Trojans. The specific measures are as follows:


Improving cybersecurity awareness

- Install authorized OSs and applications. Do not download applications from non-official websites.
- Do not open emails or install software from unknown sources. Some seemingly normal emails and software may contain Trojans.
- Do not click pop-up advertisements on websites. Trojans often disguise as such advertisements.

Configuring Trojan prevention rules on CFW

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) 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 of a firewall to go to its details page.

Step 5 In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **View Effective Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.

Step 6 Filter the rules for defending against Trojans. In the filter above the list, select **Trojan** from the **Attack Types** drop-down list.

Step 7 Enable protection in batches. Select multiple rules at a time and click **Intercept**.

 **NOTE**

Intercept: The firewall records the traffic that matches the current rule in attack event logs and blocks the traffic.

----End

7.5 Using CFW to Defend Against Vulnerability Exploits

You can use CFW to defend against vulnerability exploits.

Application Scenarios

Vulnerabilities are often the breakthrough point for intruding a system. They provide opportunities for attackers to bypass security control, posing threats to the system.

The IPS rule library of CFW provides defense rules for vulnerability exploits. It can detect malicious behaviors in network traffic in depth and automatically block potential attacks to effectively cope with diverse vulnerability exploits.

What Is a Vulnerability Exploit?

A vulnerability exploits refer to the behavior that attackers exploit security vulnerabilities in a system, software, or hardware to access the target system without authorization or damage it through well-constructed attack methods to achieve malicious purposes. These vulnerabilities are usually caused by defects in the design, implementation, or configuration process. They provide an opportunity for attackers to bypass security mechanisms.

Multiple technologies and methods can be used in vulnerability exploits, including but not limited to:

- **Injection attacks:** Examples of injection attacks include SQL injection and command injection. Attackers insert malicious code into the input fields of applications to perform unexpected operations or access sensitive data.
- **Cross-site scripting (XSS):** Attackers exploit website security vulnerabilities to inject malicious scripts into users' browsers to steal user information and session tokens or perform other malicious activities.
- **Cross-site request forgery (CSRF):** An attacker tricks a user into performing an unexpected operation on a web application that the user has logged in to, such as transfer money or change password, while the user is unaware of the operation.
- **Buffer overflow:** An attacker sends data that is beyond the processing capability of a program, causing the program to crash or execute malicious code.

Harms of Vulnerability Exploits


The harms of vulnerability exploits include but are not limited to:


- **Economic loss:** Vulnerability exploits may cause service interruption and data leakage, resulting in huge economic losses.
- **Information leakage:** Attackers can exploit vulnerabilities to obtain sensitive information such as users' contacts and chat records, infringing on personal privacy.
- **Network damage:** After successfully attacking a server, a hacker may turn the server into a zombie and use the zombie to attack other servers, expanding the attack scope.
- **Malware spread:** Attackers may exploit vulnerabilities to implant malware, such as viruses and Trojans, into a victim's system to further damage system security.

How to Defend Against Vulnerability Exploits

To defend against vulnerability exploits, you can update and fix vulnerabilities in a timely manner, use strong passwords and multi-factor authentication, periodically back up data, use firewalls and protection software, implement access control, and periodically perform security audits and vulnerability scans. You can also use the CFW intrusion prevention function to block vulnerability exploits.

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) 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 of a firewall to go to its details page.

Step 5 In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **View Effective Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.

Step 6 Filter the rules for defending against vulnerability exploits. In the filter above the list, select **Vulnerability-Attack** from the **Attack Types** drop-down list.

Step 7 Enable protection in batches. Select multiple rules at a time and click **Intercept**.

NOTE

Intercept: The firewall records the traffic that matches the current rule in attack event logs and blocks the traffic.

----End

7.6 Using CFW to Defend Against Worms

You can use CFW to defend against worm attacks.

Application Scenarios

Worms exploit network vulnerabilities and weak passwords to attack servers and spread rapidly through network connections, posing great security threats to user assets and services.

The CFW IPS rule library provides rules to effectively block attacks from worms, such as **JS.FortNight.E-2** and the Lovgate worm **netservices.exe**.

What Is a Worm?

A worm is a type of malware that can replicate itself and spread over the network. It scans for vulnerabilities on the network and exploits these vulnerabilities to infect other servers. Worms can exist and run without depending on other programs.

Worms have the following characteristics:

- **Vulnerability exploit:** Worms usually exploit security vulnerabilities in OSs or applications to spread. If a system has vulnerabilities that have not been fixed by installing patches or update, the system may become a target of worms.
- **Self-replication:** Worms can replicate all or part of their own code and spread the replicas to other servers over the network. Self-replication is the basis for the rapid spread of worms.
- **Independent transmission:** Different from traditional viruses that require user interaction (for example, opening attachments) to start an attack, worms can independently search for and infect other vulnerable servers on the network without user intervention. Independent transmission makes worms more difficult to block.

Harms of Worms



Worms pose serious threats to network security, including but not limited to:

- **System damage:** Worms can damage system files and data, causing the system to crash or fail to work properly.
- **Information theft:** Worms can steal sensitive user information, such as passwords and bank account information.
- **Abuse of network resources:** Worms can use infected computers to launch DDoS attacks and send spams, causing network congestion and service unavailability.
- **Malware spread:** Worms can use infected computers to spread other malware, such as Trojans and spyware.

How to Defend Against Worms

To defend against worms, you can establish good security habits, disable or delete unnecessary services, periodically update systems and applications, use strong passwords and multiple authentication mechanisms, and periodically back up data. You can also use the CFW intrusion prevention function to block worm attacks.

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) 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 of a firewall to go to its details page.
- Step 5** In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **View Effective Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.
- Step 6** Filter the rules for defending against worms. In the filter above the list, select **Worm** from the **Attack Types** drop-down list.
- Step 7** Enable protection in batches. Select multiple rules at a time and click **Intercept**.

 **NOTE**

Intercept: The firewall records the traffic that matches the current rule in attack event logs and blocks the traffic.

----End