

Cloud Firewall

Best Practices

Issue 08
Date 2025-01-23



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 CFW Best Practice Summary.....	1
2 Purchasing and Querying CFW via API.....	3
3 Migrating Security Policies to CFW in Batches.....	6
4 Configuration Suggestions for Using CFW with WAF, Advanced Anti-DDoS, and CDN.....	11
5 Allowing Internet Traffic Only to a Specified Port.....	15
6 Allowing Outbound Traffic from Cloud Resources Only to a Specified Domain Name.....	18
7 Using CFW to Defend Against Network Attacks.....	21
7.1 Using CFW to Defend Against Access Control Attacks.....	21
7.2 Using CFW to Defend Against Hacker Tools.....	23
7.3 Using CFW to Defend Against Suspicious DNS Activities.....	24
7.4 Using CFW to Defend Against Trojans.....	26
7.5 Using CFW to Defend Against Vulnerability Exploits.....	28
7.6 Using CFW to Defend Against Worms.....	29
8 Configuring a Protection Rule to Protect Traffic Between Two VPCs.....	32
9 Configuring a Protection Rule to Protect SNAT Traffic.....	43
9.1 SNAT Protection Overview.....	43
9.2 Resource and Cost Planning.....	46
9.3 Connecting VPC1 and VPC-NAT to an Enterprise Router.....	47
9.4 Configuring a NAT Gateway.....	51
9.5 Configuring a Route Table for VPC1.....	53
9.6 Configuring a NAT Protection Rule.....	54
10 Using CFW to Protect Enterprise Resources.....	55
11 Using CFW to Protect EIPs Across Accounts.....	59
12 Using CFW to Protect VPCs Across Accounts.....	64

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 an access control policy	Allowing Internet Traffic Only to a Specified Port
	Allowing Outbound Traffic from Cloud Resources Only to a Specified Domain Name
	Configuring a Protection Rule to Protect Traffic Between Two VPCs
	Configuring a Protection Rule to Protect SNAT Traffic
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

Category	Reference
	Using CFW to Defend Against Vulnerability Exploits
	Using CFW to Defend Against Worms
Enterprise project management	Using CFW to Protect Enterprise Resources
Multi-account management	Using CFW to Protect EIPs Across Accounts
	Using CFW to Protect VPCs Across Accounts

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 \(AK/SK\)?](#)
- **Region:** region ID, for example, **cn-east-3**. For details about how to obtain the value, see [Regions and Endpoints](#).

```
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 = "xxxx";
        String sk = "xxxx";

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

        CfwClient client = CfwClient.newBuilder()
            .withCredential(auth)
            .withRegion(CfwRegion.valueOf("xxxx"))
            .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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the 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](#)

details about how to enable protection for VPCs, see [Adding a Protected VPC](#).

- 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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the 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](#)For details about how to enable protection for VPCs, see [Adding a Protected VPC](#).
 - 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

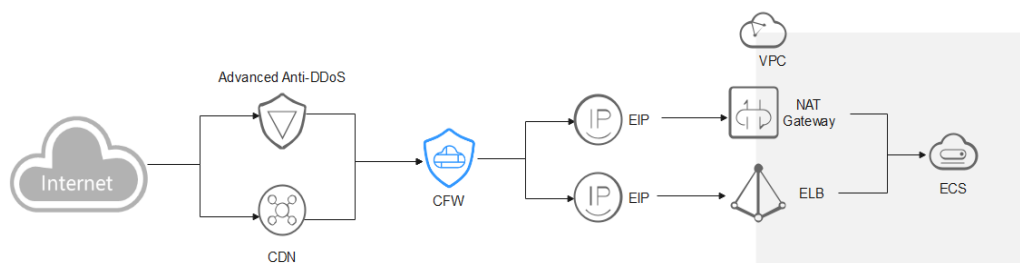
This section describes where CFW is deployed in the network architecture for inbound cloud traffic protection and how to configure CFW when it is used with other Huawei Cloud services.

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.

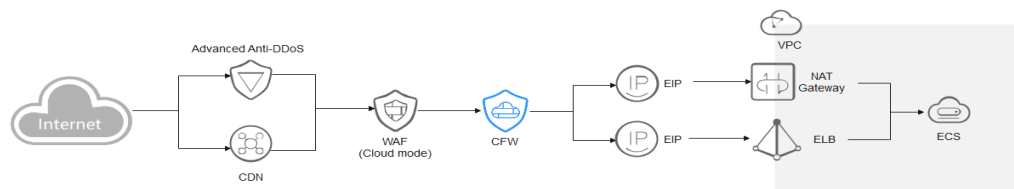
- Adding to whitelist: After back-to-source IP addresses are added to the **whitelist**, the traffic will be directly allowed to pass through, and CFW does not perform any protection.

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 [How Do I Obtain the Real IP Address of an Attacker?](#)

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.

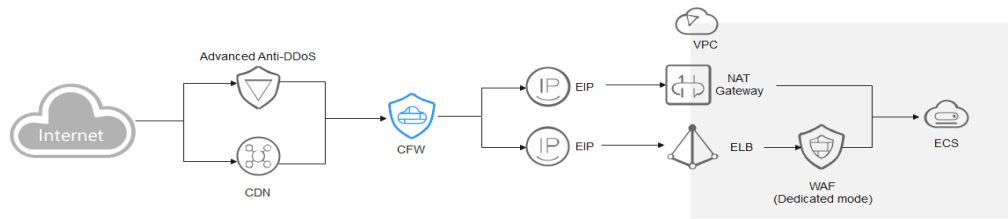
- Creating a rule: Create a policy with the highest priority to allow all back-to-origin IP addresses. In this way, traffic still goes to CFW for check.
- Adding to whitelist: After back-to-source IP addresses are added to the **whitelist**, the traffic will be directly allowed to pass through, and CFW 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 [How Do I Obtain the Real IP Address of an Attacker?](#)

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**.

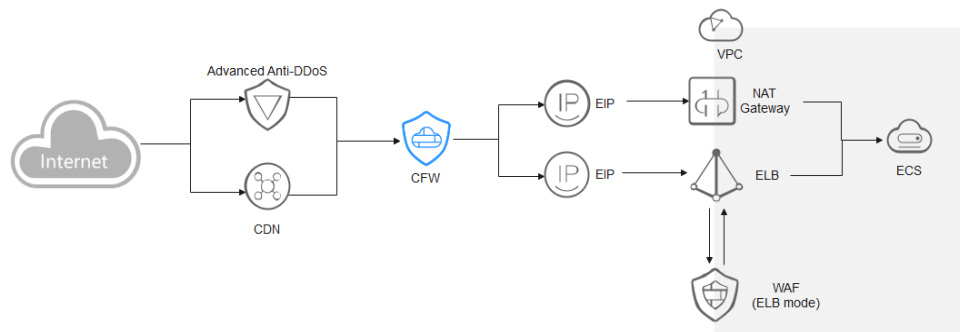
The destination IP address of the event is the EIP bound to the public ELB load balancer, and the source IP address is the IP address of the client.

- 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](#).

- Obtain the back-to-source IP address of Advanced Anti-DDoS. For details, see [How Do I Query the Back-to-Origin IP Address Range?](#)


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*).

Configuring CFW to Allow the Access Traffic from the Internet to a Specified Port

- 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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the 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

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

- 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 Outbound

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

Destination [?](#)
 IP Address IP address group Any [?](#)

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

Protocol	Source Port	Destination Port	Operation
TCP	1-65535	80	Delete

+ Add Add 1 to 5 items.

Application [?](#)
 Application Any

Protection Configuration

Protection Action
 Allowed Blocked

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 a specified domain name. (Wildcard domain name `*.example.com` is used as an example).

Configuring CFW to Allow Cloud Resources to Access a Specified Domain Name

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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the 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, as shown in [Figure 6-1](#). The priority is the lowest.

- **Direction: Outbound**
- **Source: Any**
- **Destination: Any**
- **Service: Any**
- **Application: Any**
- **Protection Action: Block**

Figure 6-1 Blocking all traffic

Matching Condition [View Configuration Guide](#)

Direction

Inbound Outbound

Source [?](#)

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

Destination [?](#)

IP Address IP address group Countries and regions Domain Name/Domain Group Any [?](#)

Service [?](#)

Service Service group Any [?](#)

Application [?](#)

Application Any

Protection Configuration

Protection Action

Allow Block

- The other rule allows the traffic to ***.example.com**, as shown in [Figure 6-2](#). 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/1-65535/1-65535**
- **Application: HTTP and HTTPS**

▪ **Action: Allow**

Figure 6-2 Allowing the access traffic to a domain name

Matching Condition [View Configuration Guide](#)

Direction
 Inbound Outbound

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 [?](#)

Protocol	Source Port ?	Destination Port ?	Operation
TCP	1-65535	1-65535	Delete

+ Add Add 1 to 5 items.

Application [?](#)
 Application
 HTTP × HTTPS ×

Protection Configuration

Protection Action
 Allowed Blocked

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 [Allowing Traffic from a Service to a Platform](#).
- For details about how to add other protection rules, see the parameter description in [Adding a Protection Rule](#).
- For details about how to allow cloud resources to access specified domain names through the NAT gateway, see [Configuring a Protection Rule to Protect SNAT Traffic](#).

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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the page.
- Step 5** 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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 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) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the page.
- Step 5** 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

8 Configuring a Protection Rule to Protect Traffic Between Two VPCs

Application Scenarios

A large amount of data needs to be exchanged between VPCs. CFW can check and collect statistics on inter-VPC traffic, helping you detect abnormal traffic.

This section describes how to configure CFW to protect traffic between VPC1 (172.16.0.0/16) and VPC2 (172.18.0.0/16).

Constraints

- Only the professional edition supports VPC border firewalls.
- Traffic diversion depends on the enterprise router
- Only the VPCs in the enterprise projects of the current account can be protected.
- To use public network CIDR blocks other than 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, or the 100.64.0.0/10 segment reserved for carrier-level NAT as private network CIDR blocks, [submit a service ticket](#) to expand your private IP CIDR blocks, or CFW may fail to forward traffic between your VPCs.

Applicable Version

This section is applicable to the new version of the VPC border firewall. Its configuration GUI is as follows.

Figure 8-1 VPC border firewall (new version)

Create Inter-VPC Firewall ×

i This CIDR block will be used to forward traffic to CFW. It cannot be modified once created. Note that:

- This CIDR block cannot overlap with the private network segment to be protected, or routing conflicts may occur.
- The CIDR block 10.6.0.0/16-10.7.0.0/16 is reserved for CFW.

★ Enterprise Router

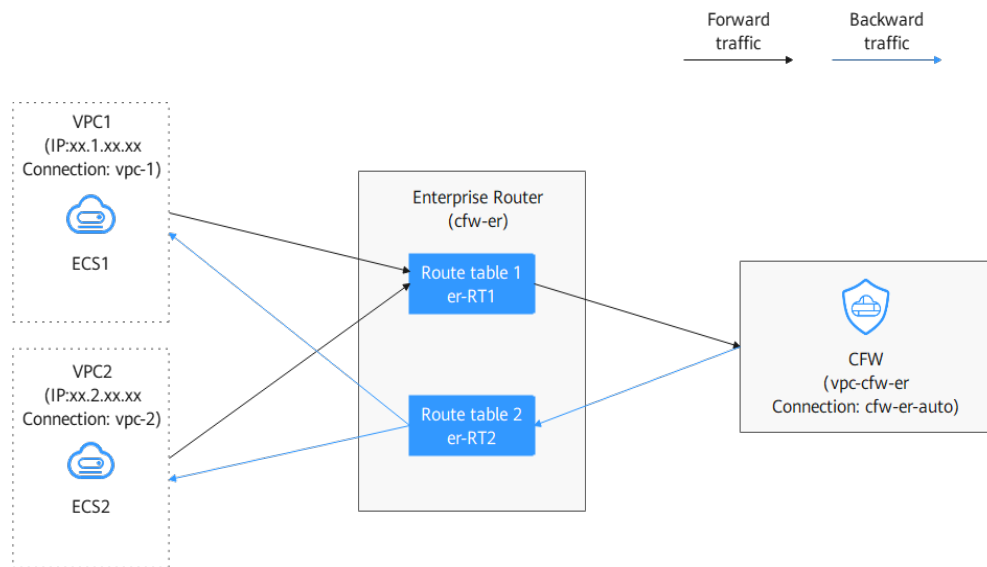
★ CIDR Block · · · /

How to Configure

The process is as follows:


1. Create a firewall (for example, **vpc-cfw-er**) and associate it with subnets. For details, see [Step 1: Create a Firewall](#).
2. Configure an enterprise router.
 - a. Configure all VPCs (including the firewall VPC and the VPC to be connected) to let them route traffic to the enterprise router. For details, see [Diverting Traffic to Enterprise Router](#).
 - b. Create attachments for all VPCs (including the firewall VPC and the VPC to be connected). For details, see [Adding Connections](#).
 - c. Create two route tables (**er-RT1** and **er-RT2**, for example). For details, see [Creating Two Route Tables](#).
 - d. Configure the association route table **er-RT1** to transmit traffic from the VPC to the CFW. For details, see [Configuring Route Table er-RT1](#).
Configure the propagation route table **er-RT2** to transmit traffic from the CFW to the VPC. For details, see [Configuring Route Table er-RT2](#).
 - e. [Modify VPC route tables](#).
3. Enable VPC protection and verify the communication.
4. Configure protection rules and view the outcomes.


Figure 8-2 Traffic flow



Step 1: Create a Firewall

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 In the navigation pane, choose **Assets > Inter-VPC Border Firewalls**.

Step 5 Click **Create Firewall**, select an enterprise router, and configure a CIDR block.

- An enterprise router is used for traffic diversion. It must meet the following requirements:
 - Not associated with other firewall instances.
 - Belongs to the current account and is not shared with other users.
 - **Default Route Table Association, Default Route Table Propagation, and Auto Accept Shared Attachments** must be disabled.
- After a CIDR block is configured, an inspection VPC is created by default to forward traffic to CFW. A CFW-associated subnet is automatically allocated to forward traffic to an enterprise router. Pay attention to the following restrictions:
 - After a firewall is created, its CIDR block cannot be modified.
 - The CIDR block must meet the following requirements:
 - Only private network address segments (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) are supported. Otherwise, route conflicts may occur in public network access scenarios, such as SNAT.
 - The CIDR block 10.6.0.0/16-10.7.0.0/16 is reserved for CFW and cannot be used.


- This CIDR block cannot overlap with the private CIDR block to be protected, or routing conflicts and protection failures may occur.

Step 6 Click **OK**. The firewall will be created in 3 to 5 minutes.

----End

Step 3: Configure an Enterprise Router

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 Configure the route tables of VPCs (**VPC1**, **VPC2**, and **vpc-cfw-er**) to divert traffic to the enterprise router.

In the service list, choose **Networking > Virtual Private Cloud**. In the navigation pane, choose **Route Tables**. In the **Name/ID** column, click the route table name of the VPC to be protected.

Click **Add Route**. The following table describes the parameters.

Table 8-1 Route parameters

Parameter	Description	Example Value
Destination	Destination CIDR block. NOTICE The value cannot conflict with existing routes or subnet CIDR blocks in the VPC.	xx.xx.xx.0/16
Next Hop Type	Select Enterprise Router from the drop-down list.	Enterprise Router
Next Hop	Select a resource for the next hop. The enterprise routers you created are displayed in the drop-down list.	cfw-er
Description	(Optional) Description of a route. NOTE Enter up to 255 characters. Angle brackets (< or >) are not allowed.	-

Step 4 In the service list, Choose **Networking > Enterprise Router**.

Add a VPC connection to the enterprise router. For details, see [Adding VPC Attachments to an Enterprise Router](#).

 **NOTE**

- Add at least three VPC attachments (for CFW and the two protected VPCs). An attachment is required for each protected VPC you add.
For example, the firewall attachment (automatically generated after the firewall is created) is named **cfw-er-auto**, the VPC1 attachment is named **vpc-1**, the VPC2 attachment is named **vpc-2**, and the VPC3 attachment is named **vpc-3**.
- To use the enterprise router of account A to protect VPCs under account B, share the router with account B. For details, see [Creating a Sharing](#).
- In this section, the firewall attachment is named **cfw-er-auto** (automatically created with the firewall), the VPC1 connection is named **vpc-1**, and the VPC2 connection is named **vpc-2**.

Step 5 Create two route tables **er-RT1** and **er-RT2** for connecting to the VPC and the firewall, respectively.

Click the enterprise router name and click the **Route Table** tab. Click **Create Route Table**.

For details about the parameters, see [Table 8-2](#).

Table 8-2 Route table parameters

Parameter	Description	Example Value
Name	Route table name. The name: <ul style="list-style-type: none"> • Must contain 1 to 64 characters. • Can contain letters, digits, underscores (_), hyphens (-), and periods (. 	er-RT1/er-RT2
Tag	During the route table creation, you can tag the route table resources. Tags identify cloud resources for purposes of easy categorization and quick search. For details about tags, see Tag Overview .	Tag key: test Tag value: 01
Description	Route table description	-

Step 6 Configure the association route table **er-RT1**. Set the associations and routing.

1. Select the route table (**er-RT1**) to be connected to the VPC. On the **Route Tables** tab, click the **Associations** tab and click **Create Association**.

For more information, see [Association parameters](#).

Figure 8-3 Creating an association

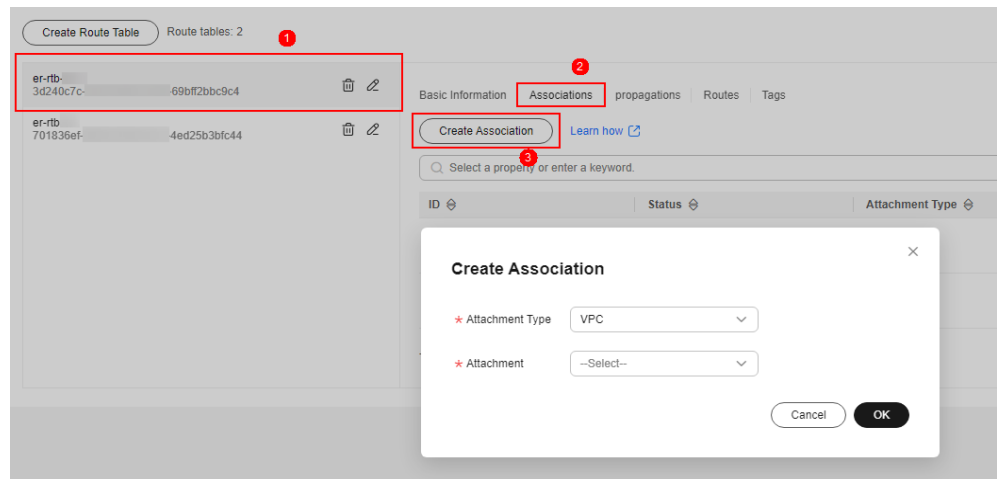


Table 8-3 VPC1 association parameters

Parameter	Description	Example Value
Attachment Type	Select VPC .	VPC
Attachment	Select an item from the Attachment drop-down list.	vpc-1

Table 8-4 VPC2 association parameters

Parameter	Description	Example Value
Attachment Type	Select VPC .	VPC
Attachment	Select an item from the Attachment drop-down list.	vpc-2

2. Create the routing of the route table (**er-RT1**). Click the **Routes** tab and click **Create Route**. You can create one or more routes as needed.

For more information, see [Route parameters](#).

Figure 8-4 Creating a route

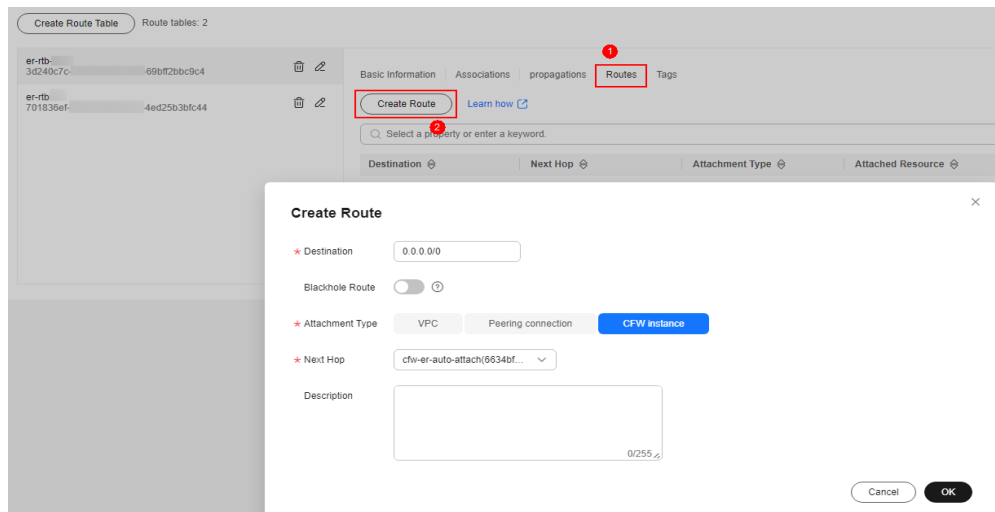


Table 8-5 Route parameters

Parameter	Description
Destination	Set the destination address. – If 0.0.0.0/0 is configured, all the traffic of the VPC is protected by CFW. – If a CIDR block is configured, the traffic of the CIDR block is protected by CFW.
Blackhole Route	You are advised to disable this function. If it is enabled, the packets from a route that matches the destination address of the blackhole route will be discarded.
Attachment Type	Set Attachment Type to CFW instance .
Next Hop	Select the automatically generated firewall attachment cfw-er-auto-attach .
Description	(Optional) Description of a route.

Step 7 Configure the propagation route table **er-RT2**. Set the associations and routing.

1. Select the route table (**er-RT2**) to be connected to the firewall. Click the **Associations** tab and click **Create Association**.

For more information, see [Association parameters](#).

Figure 8-5 Creating an association

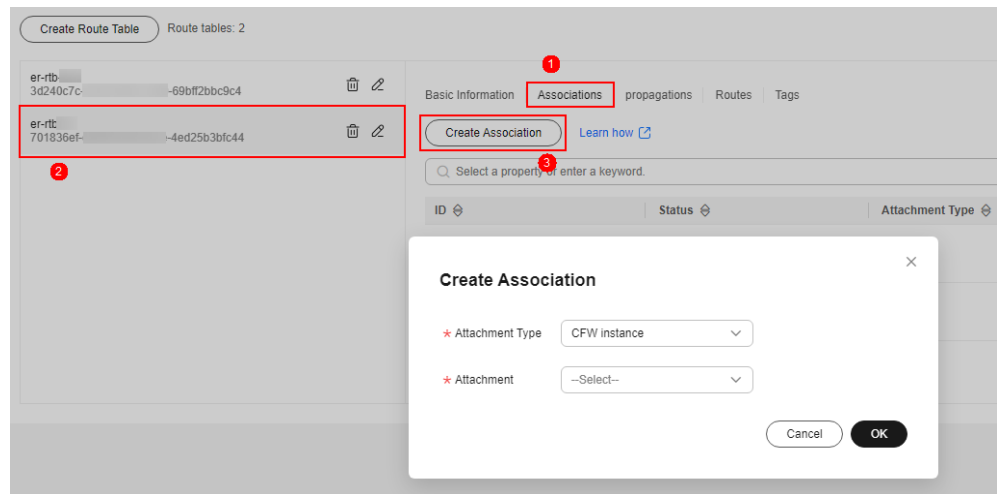


Table 8-6 Association parameters

Parameter	Description
Attachment Type	Set Attachment Type to CFW instance .
Attachment	Select the automatically generated firewall attachment cfw-er-auto-attach .

2. Create propagations for the route table (**er-RT2**). Click the **Propagations** tab and click **Create Propagation**.

For more information, see [Propagation parameters](#).

Figure 8-6 Creating a propagation

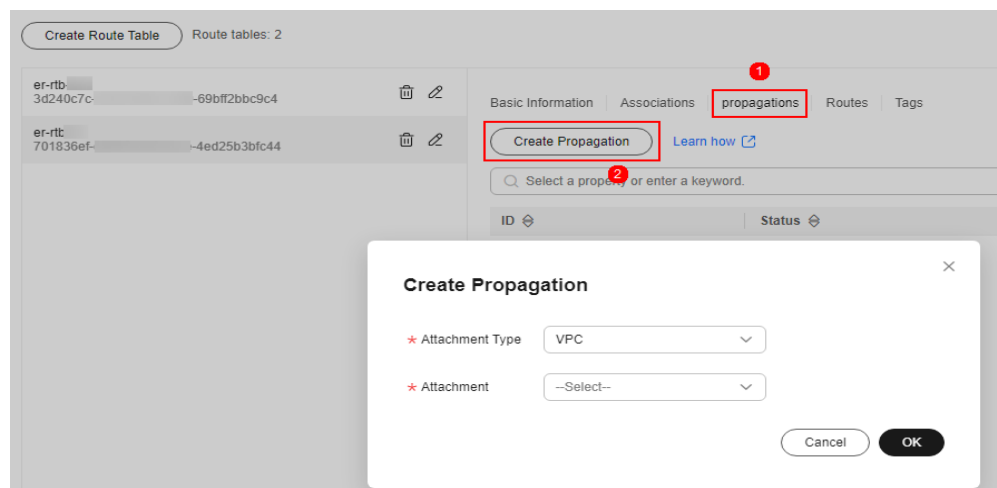


Table 8-7 Propagation parameters

Parameter	Description	Example Value
Attachment Type	Select VPC .	VPC
Attachment	Select an item from the Attachment drop-down list.	vpc-1

Table 8-8 Propagation parameters

Parameter	Description	Example Value
Attachment Type	Select VPC .	VPC
Attachment	Select an item from the Attachment drop-down list.	vpc-2

 **NOTE**

- Add at least two propagations. A propagation is required for each protected VPC you add.
For example, select attachment **vpc-1** for VPC1 and **vpc-2** for VPC2. To add VPC3 for protection, add a propagation and select attachment **vpc-3**.
- After a propagation is created, its route information will be extracted to the route table of the enterprise router, and a propagation route will be generated. In the same route table, the destinations of different propagation routes may be the same, and cannot be modified or deleted.
- You can add static routes for the attachments in a route table. The destinations of static routes in a table must be unique, and can be modified or deleted.
- If a static route and a propagation route in the same route table happen to use the same destination, the static route takes effect first.

Step 8 Modify VPC route tables. Point the route of VPC1 to VPC2 and the route of VPC2 to VPC1.

1. Return to the Enterprise Router page. In the navigation pane on the left, choose **Network > Virtual Private Cloud > Route Tables**.
2. In the **Name/ID** column, click the route table name of a VPC. The **Summary** page is displayed.
3. Click **Add Route** and configure parameters as follows:
 - Add a route to VPC1 (172.16.0.0/16).
 - **Destination Type:** Select **IP address**.
 - **Destination:** **172.18.0.0/16**
 - **Next Hop Type:** **Enterprise Router**
 - Add a route to VPC2 (172.18.0.0/16).

- **Destination Type:** Select **IP address**.
- **Destination:** **172.16.0.0/16**
- **Next Hop Type:** **Enterprise Router**

----End

Step 3: Enable VPC Protection and Verify Communication

Step 1 In the navigation pane, choose **Assets > Inter-VPC Border Firewalls**.

Step 2 Click **Enable Protection** to the right of **Firewall Status**.

Step 3 Click **OK**.

Step 4 Generate traffic. For details, see [Verifying Network Connectivity](#).

Step 5 Viewing logs. In the navigation pane, choose **Log Audit > Log Query**. Click the **Traffic Logs** tab and click **VPC Border Firewall**.

- If a log is generated, CFW is protecting the traffic between VPCs.
- If no logs are recorded, check the configurations of the enterprise router. For details, see [Step 3: Configure an Enterprise Router](#).

----End

Step 4: Configure a Protection Rule and View Outcomes

Step 1 In the navigation pane, choose **Access Control > Access Policies**. Click the **Inter-VPC Borders** tab.

Step 2 Add three protection rules.

Click **Add Rule**. On the **Add Rule** page, configure protection information and set other parameters as needed.

- Add a rule to block all traffic.
 - **Source:** **Any**
 - **Destination:** **Any**
 - **Service:** **Any**
 - **Application:** **Any**
 - **Protection Action:** **Block**
- Add a rule to allow the traffic from VPC1 to VPC2.
 - **Source:** Select **IP address** and enter **172.16.0.0/16**.
 - **Destination:** Select **IP address** and enter **172.18.0.0/16**.
 - **Service:** **Any**
 - **Application:** **Any**
 - **Action:** **Allow**
- Add a rule to allow the traffic from VPC2 to VPC1.
 - **Source:** Select **IP address** and enter **172.18.0.0/16**.
 - **Destination:** Select **IP address** and enter **172.16.0.0/16**.

- **Service: Any**
- **Application: Any**
- **Action: Allow**

Step 3 View the rule hits in access control logs.

In the navigation pane, choose **Log Audit > Log Query**. Click the **Access Control Logs** tab and click **VPC Border Firewall**.

----End

References

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

9 Configuring a Protection Rule to Protect SNAT Traffic

9.1 SNAT Protection Overview

Context

The CFW standard edition protects traffic between EIPs, for example, traffic generated when the Network Address Translation (NAT) gateway is used for multiple VPCs or subnets to use EIPs to initiate external access. The CFW professional edition provides more fine-grained access control, for example, on the traffic generated when private IP addresses are used to initiate access to the public network.

This section describes how to configure the CFW professional edition to protect access from private IP addresses to the public network in the SNAT scenario.

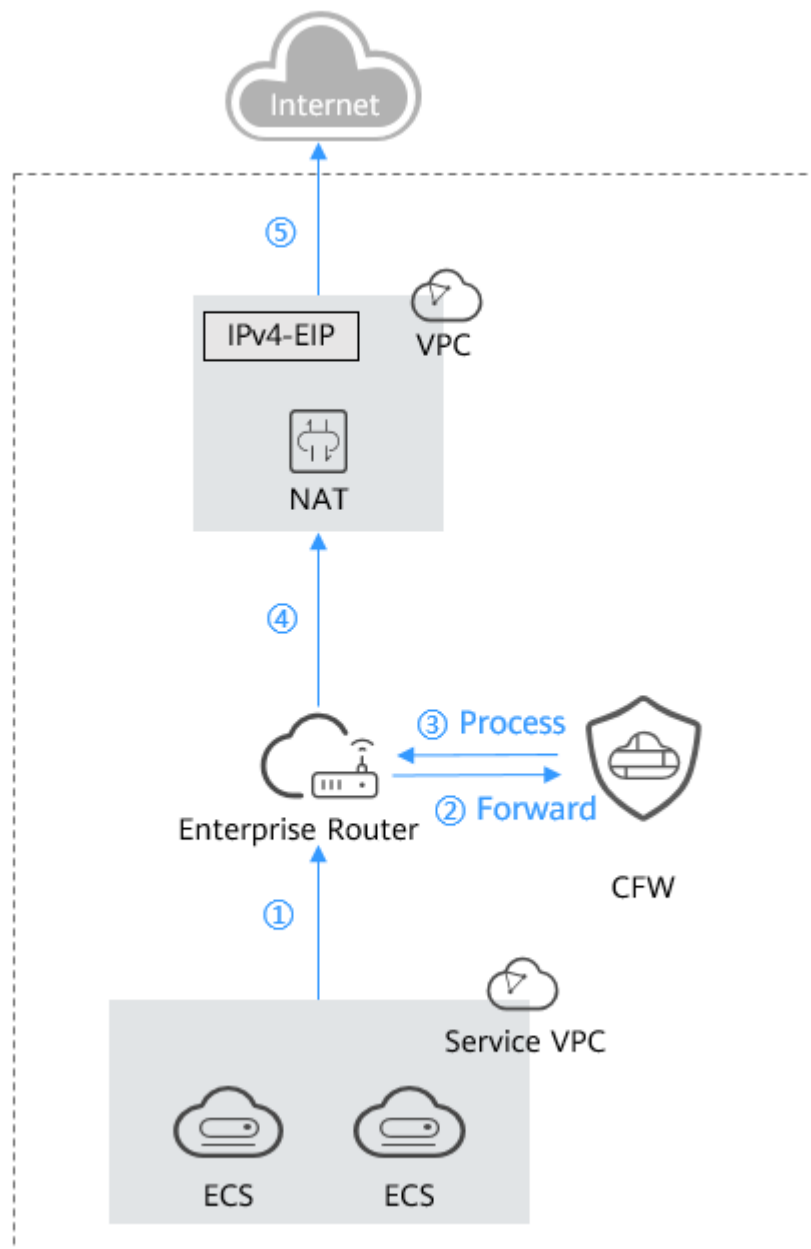
Prerequisites

- An enterprise router has been configured. For more information, see [What's an Enterprise Router?](#)
- A firewall has been created. For more information, see [Creating a Firewall](#).

Constraints

- Only the professional edition supports access control over private IP addresses.
- By default, CFW supports standard private network CIDR blocks. To enable non-standard CIDR block communication, submit a service ticket.

Networking for SNAT Protection



NOTE

The request traffic and response traffic are transmitted along the same path.

Suggestion

- You are advised to create an independent VPC for the NAT gateway. To avoid affecting access control, do not use the VPC in the network configurations of Elastic Cloud Servers (ECSs) or other instances.
- If the existing network is complex or improperly configured (for example, VPC CIDR blocks overlap, the NAT gateway has complex configurations, or east-

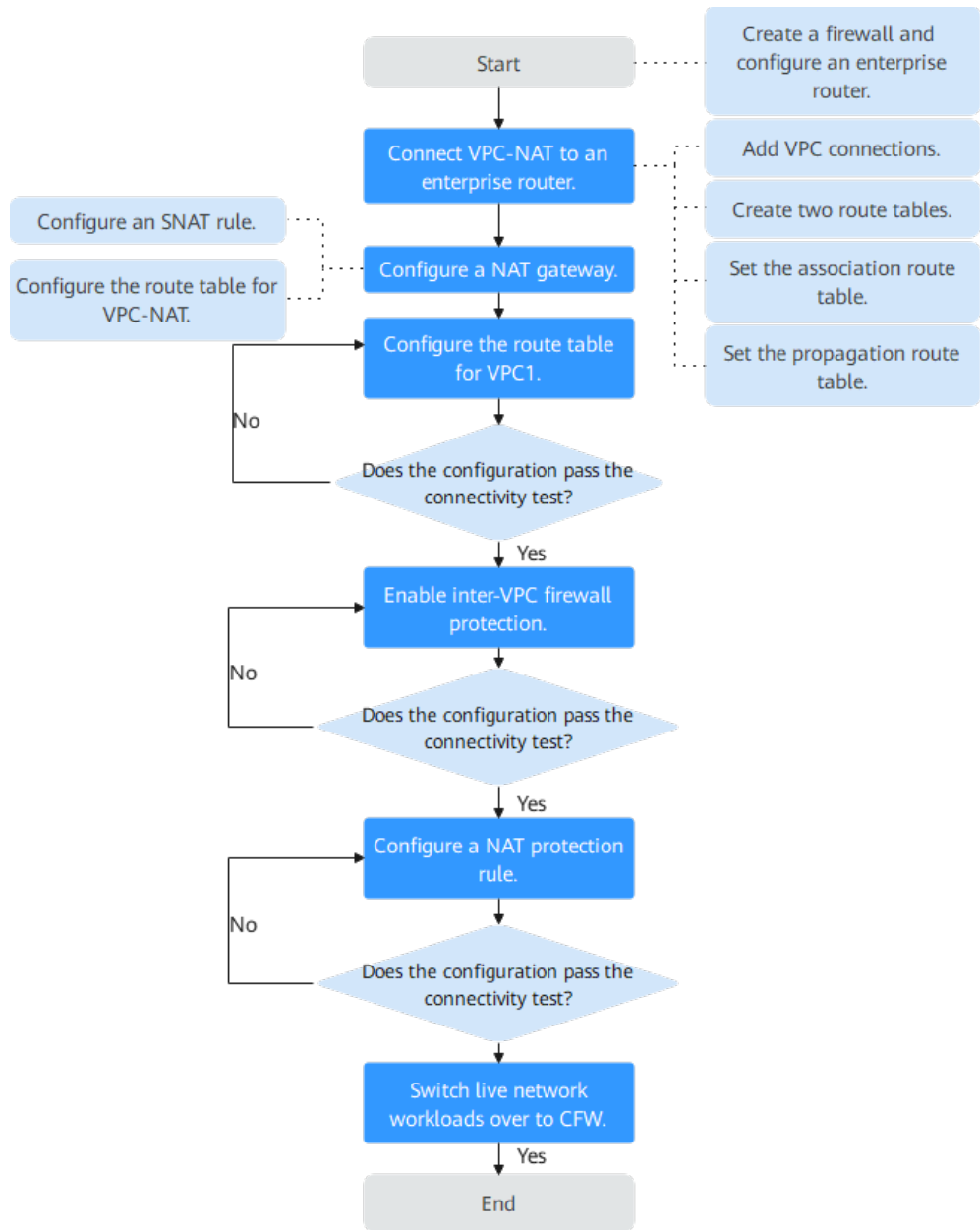
west communication has been configured using VPC Peering), fully evaluate risks in network interconnections, route loops, and route conflicts.

- Test firewall configurations before applying them to a network. You can create a test server, configure the destination address route in the VPC route table, use and the test server in the VPC to check whether the entire service flow runs properly and whether the configured rules are effective. Switch the service flow over to the live network after the configurations pass the test.
- Do not configure interception rules immediately after CFW is enabled. Check whether workloads are normal after traffic passes through the firewall. Gradually add rules and verify them in a timely manner. Once a problem is detected, disable protection in a timely manner to avoid affecting workloads.
- SNAT EIPs do not allow inbound access from the external network. Their outbound access control rules use the Internet border protection capabilities. You are not advised to enable protection for EIPs bound to SNAT on the **EIPs** page, because doing so may interrupt rule implementation and logging.

Configuration Process

1. [Connecting VPC1 and VPC-NAT to an Enterprise Router](#)
2. [Configuring a NAT Gateway](#)
3. [Configuring a Route Table for VPC1](#)
4. (Optional) Test network connectivity. Use the test server in the service VPC to access the external network. If the access is successful, the NAT configuration is proper.
5. Enable firewall protection between VPCs. For details, see [Enabling a VPC Border Firewall](#).
6. (Optional) Use the test server in the service VPC to test the network connectivity again. If the firewall traffic log contains response records, traffic has been successfully diverted to the firewall. For details about how to query traffic logs, see [Traffic Logs](#).
7. Perform the operations described in [Configuring a NAT Protection Rule](#) on the firewall.
8. (Optional) Use the test server to access the IP address or domain name and check whether the access control log contains a log that matches the rule. If it does, the protection rule has taken effect. For more information, see [Access Control Logs](#).
9. After the configurations pass the verification, gradually switch workloads from the production-like or live network environment to CFW.

Figure 9-1 SNAT protection configuration process



9.2 Resource and Cost Planning

This section describes the resource and cost planning for SNAT protection.

Table 9-1 Resource description

Resource	Description	Quantity	Cost
NAT Gateway	Protected resource.	1	For details about the billing modes and standards, see NAT Gateway Billing .
Elastic IP (EIP)	EIP bound to the NAT gateway.	At least 1	For details about billing rules, see EIP Billing .
Virtual Private Cloud (VPC)	VPC that the NAT gateway belongs to. CFW protects the traffic of the NAT gateway through the protected VPC.	1	For details about billing rules, see VPC Billing .
Enterprise Router	An enterprise router routes traffic between VPC and CFW.	1	For details about billing rules, see Enterprise Router Billing .
Cloud Firewall (CFW)	Only the professional edition CFW provides SNAT protection.	1	For details about billing rules, see CFW Billing .

9.3 Connecting VPC1 and VPC-NAT to an Enterprise Router

This section describes how to connect VPC1 and VPC-NAT to an enterprise router.

Connecting VPC1 and VPC-NAT to an Enterprise Router


Step 1 Add VPC connections.

For details, see [Adding VPC Attachments to an Enterprise Router](#).

 **NOTE**

Two connections need to be added. Set their **Attached Resource** to **VPC1** and **VPC-NAT**, respectively.

Step 2 Create two route tables.

1. In the upper left corner, click  and choose **Networking > Enterprise Router**. Click **Manage Route Table**.
2. Create an association route table and a propagation route table, used for connecting to a protected VPC and a firewall, respectively.

Click the **Route Tables** tab. Click **Create Route Table**. For more information, see [Table 9-2](#).

Table 9-2 Route table parameters

Parameter	Description
Name	Route table name. It must meet the following requirements: <ul style="list-style-type: none">– Must contain 1 to 64 characters.– Can contain letters, digits, underscores (_), hyphens (-), and periods (.).
Description	Route table description
Tag	During the route table creation, you can tag the route table resources. Tags identify cloud resources for purposes of easy categorization and quick search. For details about tags, see Tag Overview .

Step 3 Configure the association route table.

1. Create an association between VPC1 and VPC-NAT. On the route table configuration page, click the **Associations** tab and click **Create Association**. For more information, see [Table 9-3](#).

Table 9-3 Association parameters

Parameter	Description
Attachment Type	Select VPC .
Attachment	Select the VPC attachment from the Attachment drop-down list.

 **NOTE**

Two associations need to be added. Set their **Attachment** to VPC1 and VPC-NAT attachments, respectively.

2. Add a static route to the firewall. Click the **Routes** tab and click **Create Route**. For more information, see [Table 9-4](#).

Figure 9-2 Creating a route

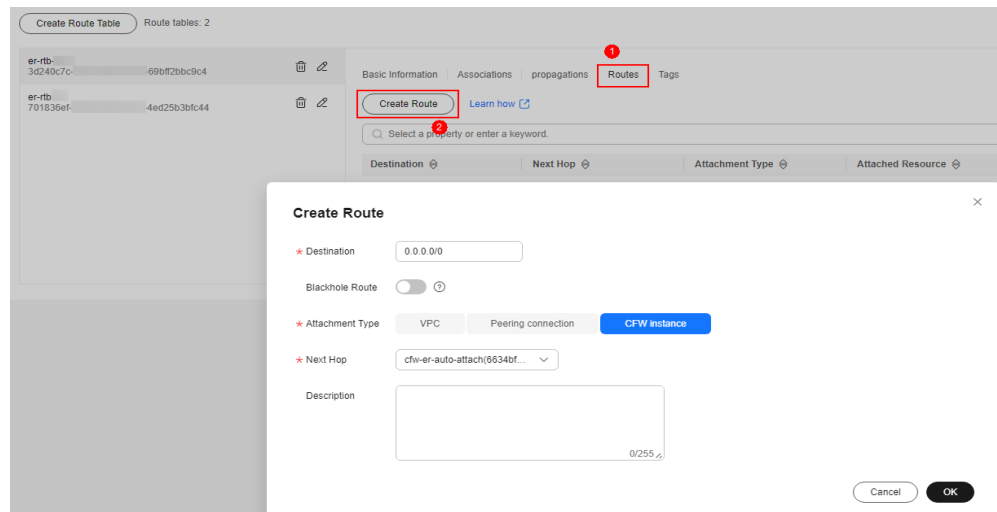


Table 9-4 Route parameters

Parameter	Description
Destination	Set the destination address. – If 0.0.0.0/0 is configured, all the traffic of the VPC is protected by CFW. – If a CIDR block is configured, the traffic of the CIDR block is protected by CFW.
Blackhole Route	You are advised to disable this function. If it is enabled, the packets from a route that matches the destination address of the blackhole route will be discarded.
Attachment Type	Set Attachment Type to CFW instance .
Next Hop	Select the automatically generated firewall attachment cfw-er-auto-attach .
Description	(Optional) Description of a route.

Step 4 Configure the propagation route table.

1. Add an association with the firewall. On the route table configuration page, click the **Associations** tab and click **Create Association**. For more information, see [Table 9-5](#).

Figure 9-3 Creating an association

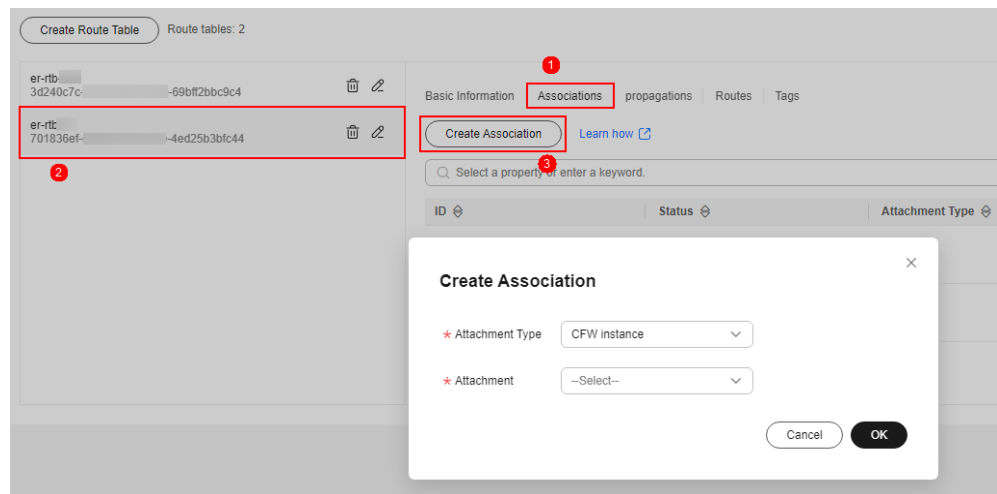


Table 9-5 Association parameters

Parameter	Description
Attachment Type	Set Attachment Type to CFW instance .
Attachment	Select the automatically generated firewall attachment cfw-er-auto-attach .

2. Add a propagation with VPC1. Click the **Propagations** tab, and click **Create Propagation**. For more information, see [Table 9-6](#).

Figure 9-4 Creating a propagation

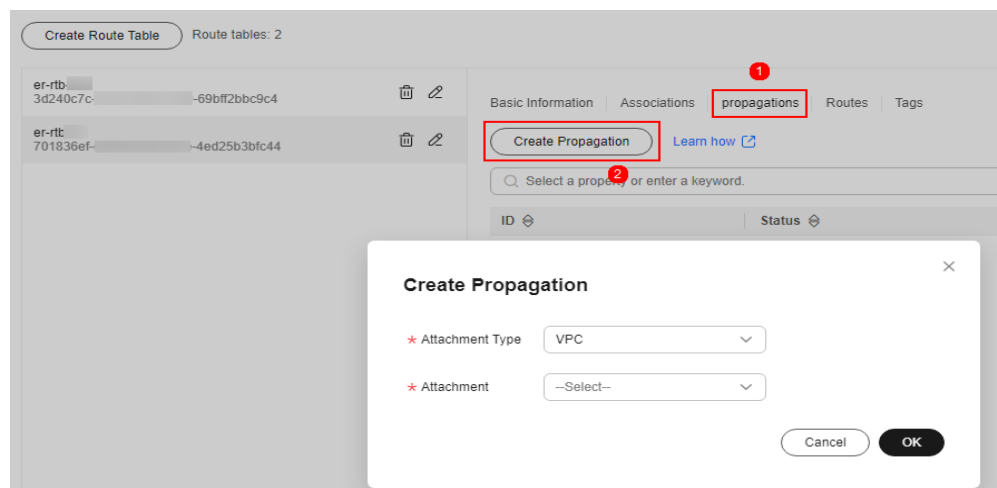


Table 9-6 Propagation parameters

Parameter	Description
Attachment Type	Select VPC .

Parameter	Description
Attachment	Select the VPC1 attachment from the Attachment drop-down list.

3. Add a static route to VPC-NAT. Click the **Routes** tab and click **Create Route**. For more information, see [Table 9-7](#).

Table 9-7 Route parameters

Parameter	Description
Destination	Set it to 0.0.0.0/0 .
Blackhole Route	You are advised to disable this function. If it is enabled, the packets from a route that matches the destination address of the blackhole route will be discarded.
Attachment Type	Select VPC .
Next Hop	Select the VPC-NAT attachment from the drop-down list.

----End

9.4 Configuring a NAT Gateway

Prerequisites

- A NAT gateway has been purchased and its VPC has not been associated with any cloud resources (such as cloud servers).
- If there are no NAT gateways available, [buy a public NAT gateway](#). For details about NAT gateway pricing, see [Billing](#).

CAUTION

If VPC-NAT is associated with the NAT gateway, a route will be added to the default route table by default. (The destination address is 0.0.0.0/0, and the **Next Hop Type** is **NAT gateway**.) This route diverts the traffic destined for VPC-NAT to the NAT gateway. Do not delete it.

Step 1: Configure an SNAT Rule

- Step 1** In the service list, click **NAT Gateway** under **Networking**. The **Public NAT Gateway** page is displayed.
- Step 2** Click the name of a public network NAT gateway. The **Basic Information** tab is displayed. Click the **SNAT Rules** tab.

Step 3 Click **Add SNAT Rule**. For more information, see [Table 9-8](#).

Table 9-8 Adding an SNAT rule

Parameter	Description
Scenario	Scenario where the SNAT rule is used. Select VPC .
CIDR Block	Select Custom to enable servers in this subnet to use the SNAT rule to access the Internet. <ul style="list-style-type: none"> • Custom: Customize a CIDR block or enter the IP address of a VPC. <p>NOTE When you select Custom, you can enter 0.0.0.0/0. Only a 32-bit server IP address is supported.</p>
Public IP Address Type	Select EIP , which is an EIP for Internet access. You can select only an EIP that is not bound to any resource, an EIP that is bound to a DNAT rule whose Port Type is not set to All ports in the current public NAT gateway, or an EIP that is bound to an SNAT rule of the current public NAT gateway. You can select multiple EIPs at once. Up to 20 EIPs can be selected for each SNAT rule. If you have selected multiple EIPs for an SNAT rule, one EIP will be chosen randomly.
Monitoring	Monitoring of the number of SNAT connections. You can set alarm rules to monitor your SNAT connections and keep informed of any changes in a timely manner.
Description	Supplementary information about the SNAT rule. Enter up to 255 characters.

----End

Step 2: Configure a VPC-NAT Route Table

Step 1 In the service list, click **Virtual Private Cloud** under **Networking**. In the navigation pane, choose **Route Tables**.

Step 2 In the **Name** column, click the route table name of a VPC. The **Summary** page is displayed.

Step 3 Click **Add Route**. For more information, see [Table 9-9](#).

Table 9-9 Route parameters

Parameter	Description
Destination Type	Select IP address .

Parameter	Description
Destination	Destination CIDR block. Enter the IP address of VPC1. NOTE The value cannot conflict with existing routes or subnet CIDR blocks in the VPC.
Next Hop Type	Select Enterprise Router from the drop-down list.
Next Hop	Select a resource for the next hop. The enterprise routers you created are displayed in the drop-down list.
Description	(Optional) Supplementary information about the route. NOTE Enter up to 255 characters. Angle brackets (< or >) are not allowed.

----End

9.5 Configuring a Route Table for VPC1

Configuring a Route Table for VPC1

- Step 1** In the service list, click **Virtual Private Cloud** under **Networking**. In the navigation pane, choose **Route Tables**.
- Step 2** In the **Name** column, click the route table name of VPC1. The **Summary** page is displayed.
- Step 3** Click **Add Route**. For more information, see [Table 9-10](#).

Table 9-10 Route parameters

Parameter	Description
Destination Type	Select IP address .
Destination	Destination CIDR block. Set it to 0.0.0.0/0 .
Next Hop Type	Select Enterprise Router from the drop-down list.
Next Hop	Select a resource for the next hop. The enterprise routers you created are displayed in the drop-down list.
Description	(Optional) Supplementary information about the route. NOTE Enter up to 255 characters. Angle brackets (< or >) are not allowed.


----End


9.6 Configuring a NAT Protection Rule

After verifying the traffic flow, configure protection rules so that the CFW can allow or block traffic accordingly.

Configuring a NAT Protection Rule

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

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

Step 3 In the navigation pane 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 **Access Control > Access Policies**.

Step 6 On the **Internet Boundaries** tab, click **Add Rule**. In the **Add Rule** dialog box, configure key parameters as follows:

- **Rule Type:** NAT
- **Direction:** SNAT
- **Source:** Select **IP address**. Enter a private IP address.
- **Destination:** Select **IP address** (and enter a public IP address) or **Domain name/Domain name group**.
- **Application:** Any

Step 7 Click **OK**.

----End

10 Using CFW to Protect Enterprise Resources

Context

Huawei Cloud provides [Enterprise Project Management Service \(EPS\)](#) to help enterprises manage people, funds, resources, permissions, and services on the cloud, standardize enterprise operations on Huawei Cloud, and meet cloud IT governance requirements.

You can create enterprise projects based on your organizational structure to centrally manage resources in different regions. You can also grant different permissions to **users** and **user groups** in enterprise projects.

Application Scenarios

If a large enterprise wants to manage services by branch or department, but finds it difficult to divide bills and allocate resources, the enterprise can use EPS.

- Different services can be put under different enterprise projects. Bills are generated for each enterprise project, facilitating budget management and fee splitting.
- Enterprise projects can be assigned to users and user groups for refined resource management.

This section describes how to plan CFW when an enterprise manages services through EPS.

Resource and Cost Planning

Table 10-1 Resource description

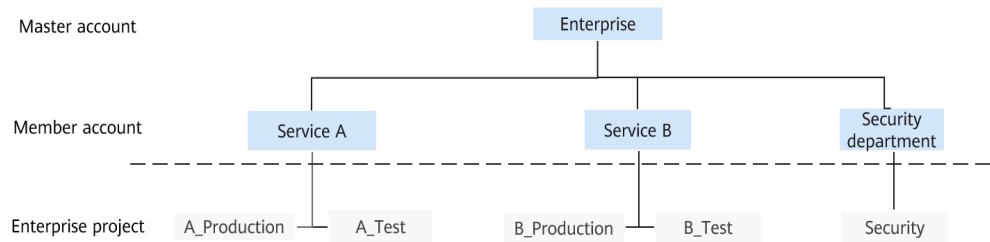
Resource	Description	Quantity	Cost
Enterprise Project Management Service (EPS)	EPS manages enterprise resources.	At least 2	Free of charge
Cloud Firewall (CFW)	CFW protects cloud resources.	At least 2	For details, see CFW Pricing Details .
Elastic IP (EIP)	(Optional) EIP is a type of cloud resource.	Configure based on service demands.	For details, see EIP Pricing Details .
Virtual Private Cloud (VPC)	(Optional) EIP is a VPC of cloud resource.	Configure based on service demands.	For details, see VPC Pricing Details .
Enterprise Router	(Optional) An enterprise router routes traffic between VPC and CFW. When CFW is used to protect VPCs, traffic diversion depends on Enterprise Router.	At least 1	For details, see Enterprise Router Pricing Details .

Example

An enterprise has services A and B on the cloud. Each service has a production team and a test team. The enterprise creates enterprise projects as follows:

- To manage services A and B separately, the enterprise creates enterprise projects **A_Production** and **A_Test** for service A, and **B_Production** and **B_Test** for service B. Cloud resources are bound to the corresponding enterprise projects based on service teams during purchase.
- The enterprise creates an enterprise project named **Security** for the security department. When purchasing security products, the enterprise binds the products to **Security** so that the financial team can distinguish bills and manage security-related budget usage.

Figure 10-1 Accounts and enterprise projects



The enterprise needs to provide isolated production and test environments for member accounts (service A and service B) and use CFW for protection. The security administrator purchases CFW for each environment.

- To protect EIPs and VPCs in the production environment, the security administrator purchases the professional edition firewall.
- To protect EIPs in the test environment, the security administrator purchases the standard edition firewall.

In each environment, the firewall is shared by services A and B, and the bills are paid by the security department, as shown in **Figure 10-2**.

Figure 10-2 Resource allocation and bill split

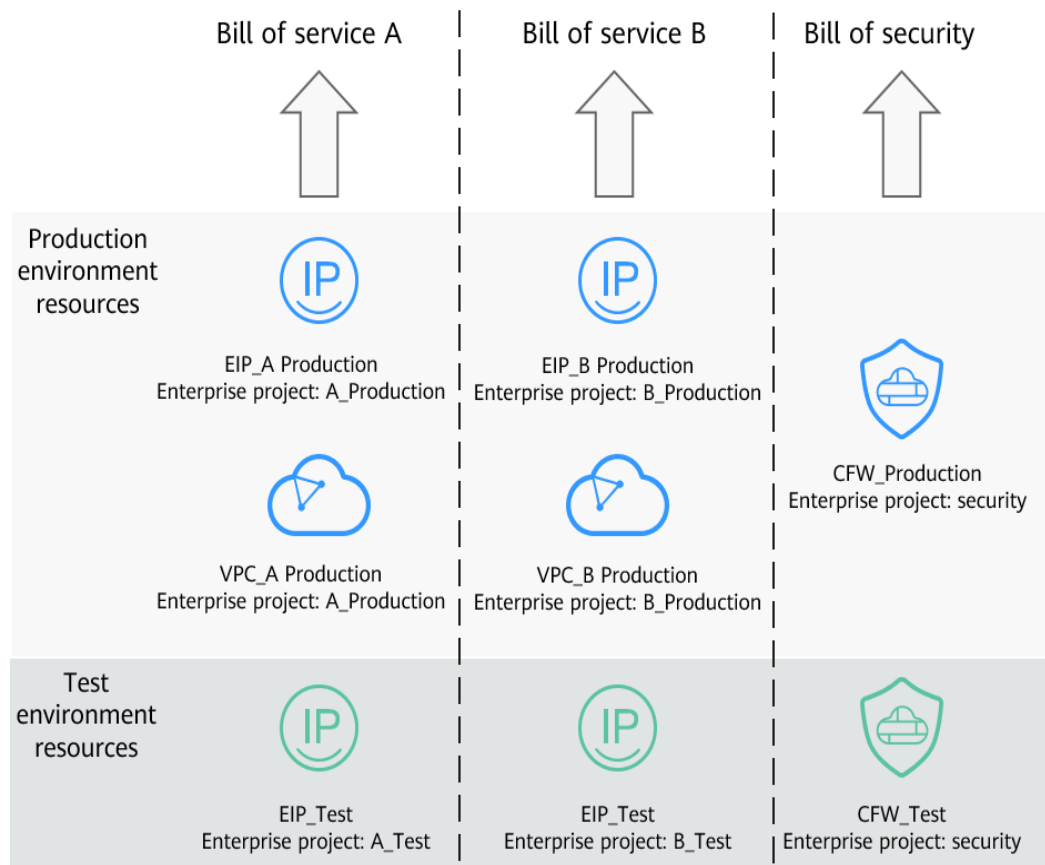


Figure 10-3 Enterprise project management for users

Example user



Enterprises can authorize member accounts by enterprise project in IAM to isolate the resources of different services. Take a security administrator and a test environment administrator as an example:

- The enterprise authorizes the security administrator to access all enterprise projects. The security administrator can view resources on both firewalls, configure different protection policies and security protection modes for the firewalls, and enable protection in different environments.
 - On the CFW in the production environment, protection is enabled for the EIPs and VPCs in enterprise projects **A_Production** and **B_Production**.
 - On the CFW in the test environment, protection is enabled for the EIPs in enterprise projects **A_Test** and **B_Test**.
- The enterprise authorizes the test environment administrator to manage **A_Test**, **B_Test**, and **Security** enterprise projects, but does not authorize the test administrator to manage resources (EIPs and VPCs) in the production environments. The test environment administrator can perform operations on the two firewalls under its account, and can only view the resource information in the test environments.

Related Operations

- For details about how to create an enterprise project, see [Creating an Enterprise Project](#).
- For details about how to purchase a CFW, see [Purchasing a CFW](#).
- For details about how to create and grant permissions to a user group using IAM, see [Creating a User Group and Assigning Permissions](#). For details about how to grant permissions to a user using IAM, see [Assigning Permissions to an IAM User](#).

11 Using CFW to Protect EIPs Across Accounts

Application Scenarios

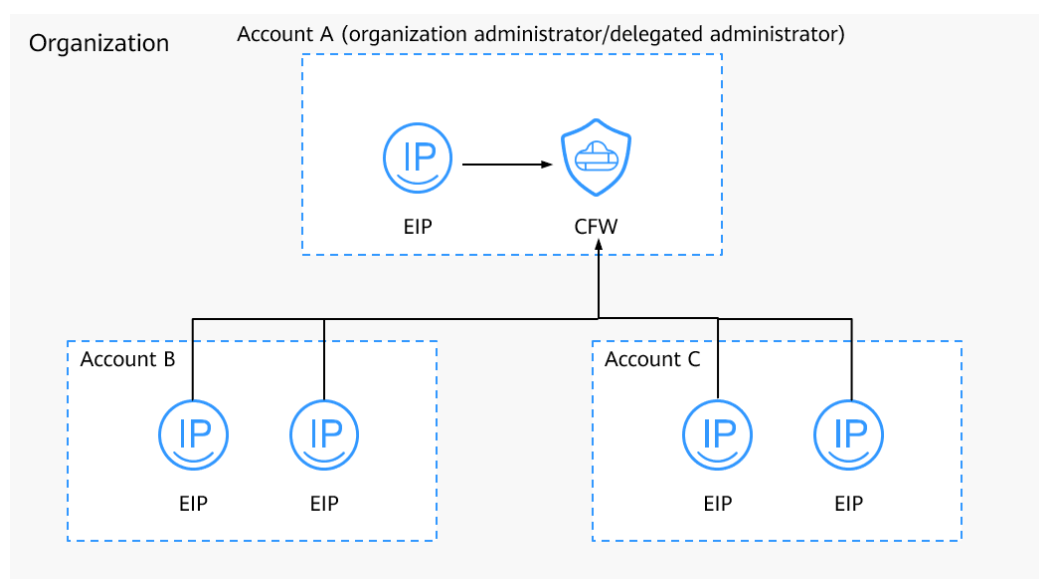
Protect resources across accounts. For example, different departments in an enterprise use different accounts but need to share CFW protection policies.

This section describes how to use CFW to protect the EIPs under multiple accounts.

Solution Overview

The solution for protecting EIPs across accounts is as follows: Account A is an organization administrator or delegated administrator. Accounts B and C are added to the organization. Account A purchases CFW and adds accounts B and C to the organization. Enable EIP protection and configure protection policies.

Figure 11-1 Cross-account protection



Constraints

- EIPs cannot be protected across regions. To use CFW in another region, switch to that region and purchase a firewall. For details, see [Purchasing a CFW](#).
- The number of accounts that can be protected by a single firewall instance is as follows:
 - Yearly/Monthly CFW:
 - Standard edition: 20
 - Professional edition: 50
 - Pay-per-use CFW (professional edition): 20

Resource and Cost Planning

Table 11-1 Resource description

Resource	Description	Quantity	Cost
Enterprise Center	Provides comprehensive management services for enterprise customers to manage organizations and finance on the cloud. To use the Organizations service, you need to enable Enterprise Center.	1	Enterprise Center is free of charge.
Organizations	The Organizations service helps you govern multiple accounts within your organization.	1	The Organizations service is free of charge.
Cloud Firewall (CFW)	CFW protects cloud resources.	1	For details, see CFW Pricing Details .
Elastic IP (EIP)	Protected resource.	Configure based on service demands.	For details, see EIP Pricing Details .

Protecting EIPs Across Accounts

- Step 1** Prepare accounts and permissions. In the following steps, account A is an organization administrator.

 **NOTE**

If account A is not an organization administrator, let the organization administrator add account A as a delegated administrator. For details, see [Adding a Delegated Administrator](#).

1. Perform the following operations using account A:
 - a. Purchase the CFW standard or professional edition. For details, see [Purchasing CFW](#).
 - b. (Optional) Enable the Enterprise Center. For details, see [Enabling Enterprise Center](#).
If the Enterprise Center has been enabled, skip this step.
 - c. (Optional) Enable the Organizations service and create an organization.
If the Organizations service has been enabled, skip this step.

 **NOTE**

If you are already in an organization, leave the organization before creating another organization. For details, see [Removing a Member Account from Your Organization](#).


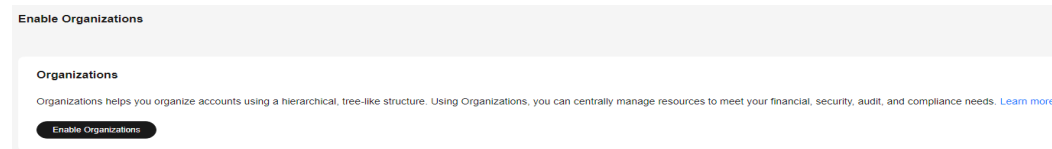
- i. [Log in to the management console](#).
- ii. Click  in the upper left corner and choose **Management & Governance > Organizations**.
- iii. Click **Enable Organizations** to enable the Organizations service.


Figure 11-2 Enabling Organizations



After the Organizations service is enabled, your organization and the root are automatically created, and your login account is defined as the management account.

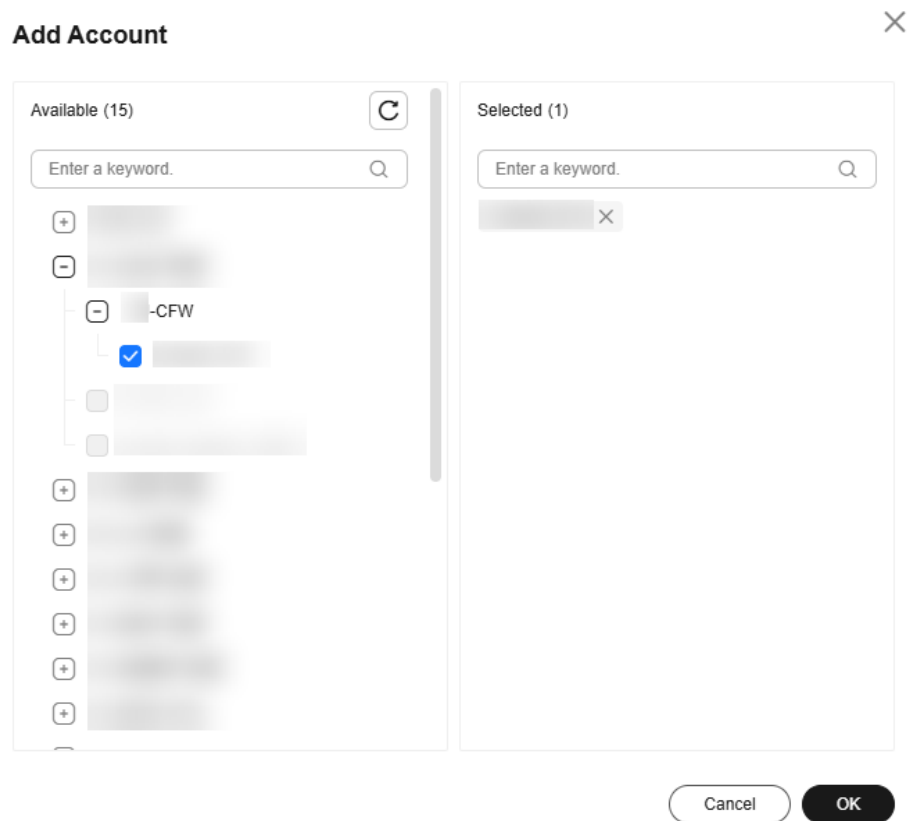
- d. Invite accounts B and C to join the organization. For details, see [Inviting an Account to Join Your Organization](#).
- e. Set CFW as a trusted service. For details, see [Enabling or Disabling a Trusted Service](#).
2. Let accounts B and C join the organization of account A. For details, see [Accepting or Rejecting an Invitation from an Organization](#).

Step 2 Use account A to add accounts B and C to the firewall.

1. In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
2. (Optional) Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the page.
3. In the navigation pane, choose **System Management > Multi-Account Management**.

4. Click **Add Account**. On the page that is displayed, select accounts B and C in the account tree view to add them to the **Selected** area on the right. Click **OK**.

Figure 11-3 Adding an account to an organization



NOTE

- An account to be added must belong to the same organization. For details about organization accounts, see [Overview of an Account](#).
- The account should not be protected by other firewalls.

Step 3 Enable EIP protection.

1. In the navigation pane, choose **Assets > EIPs**.
2. Search for the EIPs under accounts B and C. Select **Owner** from the search box and select accounts B and C.

NOTE

If the EIPs of account B or C cannot be found, click **Synchronize EIP** in the upper right corner of the page to synchronize the EIPs to the list.

3. Select the EIPs to be protected and click **Enable Protection** above the table.

NOTE

The account to which the EIP belongs is displayed in the **Owner** column.

Step 4 Configure protection policies.

- Configure protection rules, blacklists, and whitelists to control traffic. For details, see [Access Control Policy Overview](#).
- Configure attack defense to detect and protect traffic. For details, see [Attack Defense Overview](#).

Step 5 View log information. For details, see [Protection Log Overview](#).

----End

Reference

To protect VPC resources across accounts, see [Using CFW to Protect VPCs Across Accounts](#).

12 Using CFW to Protect VPCs Across Accounts

Application Scenarios

Protect resources across accounts. For example, different departments in an enterprise use different accounts but need to share CFW protection policies.

This section describes how to use CFW to protect the VPC of account A and add the VPC of another account to CFW.

Solution Overview

VPC border protection has been enabled for account A for a period of time, and you need to add the VPCs of accounts B and C for protection. The solution is as follows:

Account A shares an enterprise router with accounts B and C. Accounts B and C add attachments to the enterprise router. Account A accepts the attachments in the enterprise router and adds associations and propagations. Accounts B and C add routes to their VPCs to configure access for protection. In this way, CFW protection policies will protect the VPC resources of accounts B and C as well.

Figure 12-1 Cross-account protection solution

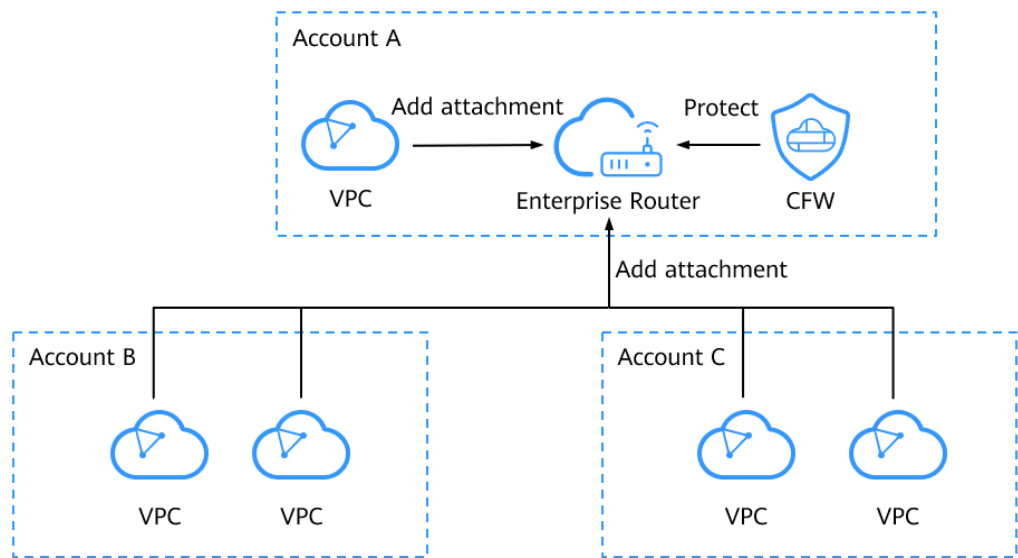
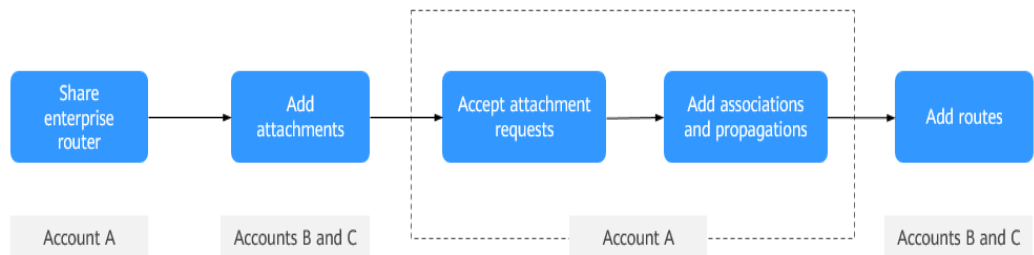


Figure 12-2 Procedure



Resource and Cost Planning

Table 12-1 Resource description

Resource	Description	Quantity	Cost
Enterprise Router	An enterprise router routes traffic between VPC and CFW.	1 (existing)	For details about billing rules, see Enterprise Router Billing .
Cloud Firewall (CFW)	Only the CFW professional edition provides VPC border protection.	1 (existing)	For details about billing rules, see CFW Billing .
Virtual Private Cloud (VPC)	Protected resource.	1	For details about billing rules, see VPC Billing .

Adding VPCs of Another Account to CFW

VPC border protection has been enabled for account A (for details, see [Configuring a Protection Rule to Protect Traffic Between Two VPCs](#)) and has been running for a period of time. To add the VPCs of accounts B and C to protection, perform the following steps:

- Step 1** Use account A to share the enterprise router with accounts B and C. For details, see [Creating a Sharing](#).
- Step 2** Use accounts B and C to add attachments to the enterprise router. For details, see [Creating a VPC Attachment](#).

NOTE

- One attachment needs to be added for each VPC.
- In the following example, account B has a VPC named **VPC1** and an attachment named **VPC_B**. Account C has a VPC named **VPC2** and an attachment named **VPC_C**.

- Step 3** Use account A to configure the route table.

1. Accept the attachment requests. For details, see [Accepting an Attachment Request](#).
2. Add associations.

Click an enterprise router and click the **Route Tables** tab. On the page that is displayed, select the association route table (**er-RT1**), click the **Associations** tab, and click **Create Association**.

NOTE

How to identify the association route table: The association route table is used to transmit traffic from VPC to CFW. The current configurations are as follows:

- **Associations** tab (having multiple attachments):
 - **Attachment Type:** VPC
 - **Attachment:** connections to multiple VPCs under account A
- Key parameters on the **Routes** tab:
 - **Attachment Type:** CFW instance
 - **Next Hop:** firewall connection (**cfw-er-auto-attach**)

This section uses account B as an example to describe how to add VPCs. If you need to add multiple (for example, three) VPCs, you need to add the corresponding number (for example, three) of associations.

- **Attachment Type:** VPC
- **Attachment:** Select the VPC attachment of account B, that is, **VPC_B**.

 NOTE

In this case, the configurations of the association route table are as follows:

- **Associations** tab (having multiple attachments + **VPC_B**):
 - **Attachment Type:** VPC
 - **Attachment:** attachments of VPCs of accounts A and B
- Key parameters on the **Routes** tab:
 - **Attachment Type:** CFW instance
 - **Next Hop:** firewall connection (**cfw-er-auto-attach**)

3. Add propagations.

Select the propagation route table (**er-RT2**), click the **Propagations** tab, and click **Create Propagation**.

 NOTE

How to identify the propagation route table: The propagation route table is used to transmit traffic from CFW to VPC. The current configurations are as follows:

- Key parameters on the **Associations** tab:
 - **Attachment Type:** CFW instance
 - **Attachment:** firewall connection (**cfw-er-auto-attach**)
- **Propagations** tab (having multiple propagations):
 - **Attachment Type:** VPC
 - **Attachment:** connections to multiple VPCs under account A

This section uses account B as an example to describe how to add VPCs. If you need to add multiple (for example, three) VPCs, you need to add the corresponding number (for example, three) of propagations.

- **Attachment Type:** VPC
- **Attachment:** Select the VPC attachment of account B, that is, **VPC_B**.

 NOTE

In this case, the configurations of the propagation route table are as follows:

- Key parameters on the **Associations** tab:
 - **Attachment Type:** CFW instance
 - **Attachment:** firewall connection (**cfw-er-auto-attach**)
- **Propagations** tab (having multiple propagations + **VPC_B**):
 - **Attachment Type:** VPC
 - **Attachment:** attachments of VPCs of accounts A and B

Step 4 Use accounts B and C to configure VPC route tables.

For example, to protect traffic between VPC1 and VPC2, configure the route of VPC1 to point to VPC2 and the route of VPC2 to point to VPC1.

1. Return to the Enterprise Router page. In the navigation pane on the left, choose **Network > Virtual Private Cloud > Route Tables**.
2. In the **Name/ID** column, click the route table name of a VPC. The **Summary** page is displayed.
3. Click **Add Route** and configure parameters as follows:
 - Add a route to VPC1 of account B:
 - **Destination Type:** Select **IP address**.
 - **Destination:** Enter the CIDR block of VPC2.
 - **Next Hop Type:** **Enterprise Router**
 - Add a route to VPC2 of account C:
 - **Destination Type:** Select **IP address**.
 - **Destination:** Enter the CIDR block of VPC1.
 - **Next Hop Type:** **Enterprise Router**

Step 5 Configure a protection policy.

- Configure **protection rules, blacklists, and whitelists** to control traffic. For details, see [Access Control Policy Overview](#) .
- Configure attack defense to detect and protect traffic. For details, see [Attack Defense Overview](#) .

 **NOTE**

By default, VPC resources connected to the same enterprise router use the protection policies of the CFW instance bound to the enterprise router.

Step 6 View log information. For details, see [Protection Log Overview](#).

----End

Reference

To protect EIP resources across accounts, see [Using CFW to Protect EIPs Across Accounts](#).