

Cloud Firewall

Best Practices

Issue 06
Date 2024-04-09



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

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

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 Configuring Inbound and Outbound Access Policies.....	1
2 Configuring Access Policies for IP Address Groups and Service Groups.....	6
3 Configuring the VPC Border Firewall.....	7
4 Using CFW to Protect SNAT.....	23
4.1 SNAT Protection Overview.....	23
4.2 Connecting VPC1 and VPC-NAT to an Enterprise Router.....	26
4.3 Configuring a NAT Gateway.....	31
4.4 Configuring a Route Table for VPC1.....	33
4.5 Configuring a NAT Protection Rule.....	33
5 Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN.....	35
6 Migrating Security Rules.....	39
A Change History.....	43

1 Configuring Inbound and Outbound Access Policies

Selecting a CFW Edition


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


For details about their functions, see [Features](#).

For details about service edition differences, see [Service Edition Differences](#).

Enabling EIP Protection

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

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

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

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

Step 5 In the navigation pane, choose **Assets > EIPs**.

Step 6 Enable EIP protection.

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

NOTICE

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

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


 **NOTE**


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

----End

Enabling Intrusion Prevention

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 **Attack Defense > Intrusion Prevention**.


Step 5 On the **Intrusion Prevention** page, select the **Protection Mode**.

- **Observe**: Attacks are detected and recorded in logs.
- **Intercept**: Attacks and abnormal IP address access are automatically intercepted.
 - **Intercept mode-loose**: The protection granularity is coarse. In this mode, only attacks with high threat and high certainty are blocked.
 - **Intercept mode-moderate**: The protection granularity is medium. This mode meets protection requirements in most scenarios.
 - **Intercept mode-strict**: The protection granularity is fine-grained, and all attack requests are intercepted. Configure false alarm masking rules after the service has been running for a period of time, and then enable strict mode.

----End

Configuring an Inbound Access Policy

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 **Access Control > Access Policies**.
- Step 5** Click **Add Rule**. Configure parameters in the **Add Rule** dialog box.
 - Add a protection rule to allow certain traffic. In the **Add Rule** dialog box, configure the source IP address. Set **Destination** and **Service** to **Any** and **Action** to **Allow**.

Figure 1-1 Allowing a specified IP address

Matching Condition

Direction Inbound Outbound

Source

Destination

Service

Protection Action

Action Allow Block

- Add a rule to block all traffic. In the **Add Rule** dialog box, set the addresses to **Any** and **Action** to **Block**. Ensure that the rule has the lowest priority.

Figure 1-2 Blocking all traffic

Matching Condition

Direction Inbound Outbound

Source

Destination

Service


Protection Action


Action Allow Block

----End

Configuring an Outbound Access Policy

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.

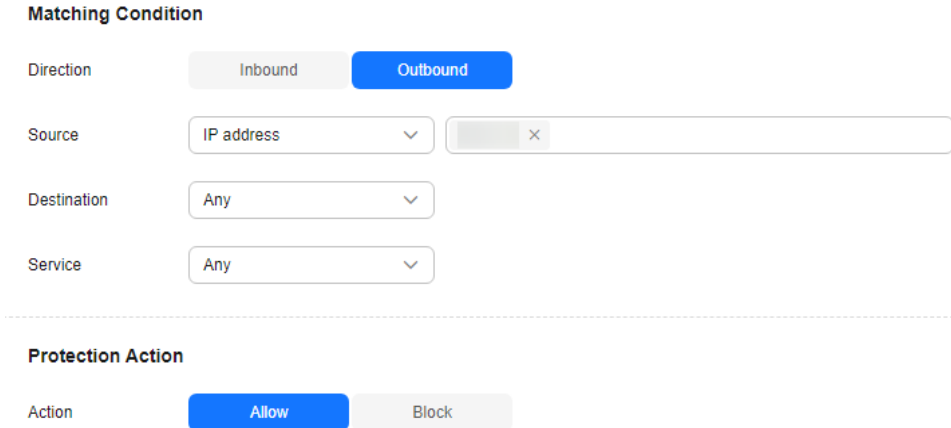
Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.

Step 4 In the navigation pane, choose **Access Control > Access Policies**.

Step 5 Click **Add Rule**. Configure parameters in the **Add Rule** dialog box.

- Add a protection rule to allow certain traffic. In the **Add Rule** dialog box, configure the source IP address. Set **Destination** and **Service** to **Any** and **Action** to **Allow**.

Figure 1-3 Allowing a specific IP address (outbound)



The screenshot shows the 'Add Rule' dialog box with the following configuration:

- Matching Condition:**
 - Direction:** Outbound (selected)
 - Source:** IP address (selected), with an input field containing a greyed-out IP address and a clear button (X).
 - Destination:** Any (selected)
 - Service:** Any (selected)
- Protection Action:**
 - Action:** Allow (selected)

- In the **Add Rule** dialog box, set **Source** to **Any**, **Destination** to **Domain name**, **Service** to **Any**, and **Action** to **Allow**.

Figure 1-4 Configuring a policy to allow outbound traffic (domain name specified)

Matching Condition

Direction: Inbound Outbound

Source:

Destination: Application Network

Support all protocols.

Domain name:

Test: The domain name is valid.

Resolved IP address:

Service:

Protection Action

Action: Allow Block

- Add a rule to block all traffic. In the **Add Rule** dialog box, set **Source**, **Destination**, and **Service** to **Any** and set **Action** to **Block**. Ensure that the rule has the lowest priority.

Figure 1-5 Blocking all traffic (outbound)

Matching Condition

Direction: Inbound Outbound

Source:

Destination:

Service:

Application:

Protection Action

Action: Allow Block

----End

Viewing Protection Details

For details, see [Viewing Protection Details](#).

2 Configuring Access Policies for IP Address Groups and Service Groups

After a protected object is connected to CFW, you can configure access control policies for IP address groups and service groups, and verify the effect of the policies. This section uses the configuration of IP address and service groups as an example to describe how to configure IP address and service access control policies in batches.

Scenario

If your service is deployed in an enterprise that has many IP addresses and services, you need to configure access control policies for users' IP address groups and service groups to permit or block certain access requests.

Prerequisites

- A website to be protected has been connected to CFW.
- Intrusion prevention has been enabled and **Action** has been set to **Block**.

Configuring an Access Control Policy

- For details about how to add an IP address group, see [Adding an IP Address Group](#).
- For details about how to add a service group, see [Adding a Service Group](#).
- For details about how to add a protection rule, see [Adding a Protection Rule](#).

Verifying a Rule

For details, see [Viewing Protection Details](#).

3 Configuring the VPC Border Firewall

Application Scenarios

A VPC border firewall can collect statistics on communication traffic between VPCs, helping you detect abnormal traffic.

Constraints

- Only the professional edition supports VPC border firewalls.
- Traffic diversion depends on the enterprise router
- Only VPCs in the enterprise project to which the current account belongs 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, and 100.64.0.0/10 as private network CIDR blocks, [submit a service ticket](#), or CFW may fail to forward traffic between your VPCs.

Applicable Version

New VPC border firewall version.

NOTE

You can check the GUI to determine your version.

The pages for creating a VPC border firewall differ, as shown in [VPC border firewall \(new version\)](#) and [VPC border firewall \(old version\)](#).

Figure 3-1 VPC border firewall (new version)

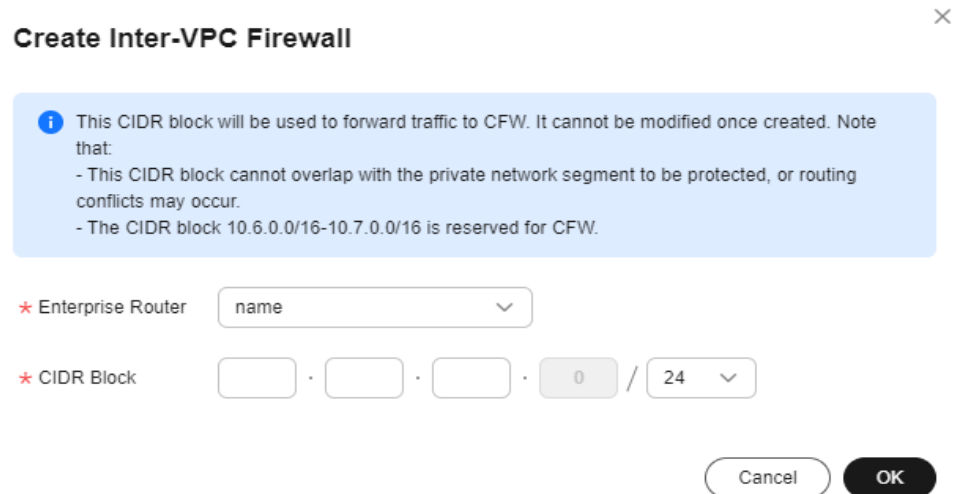
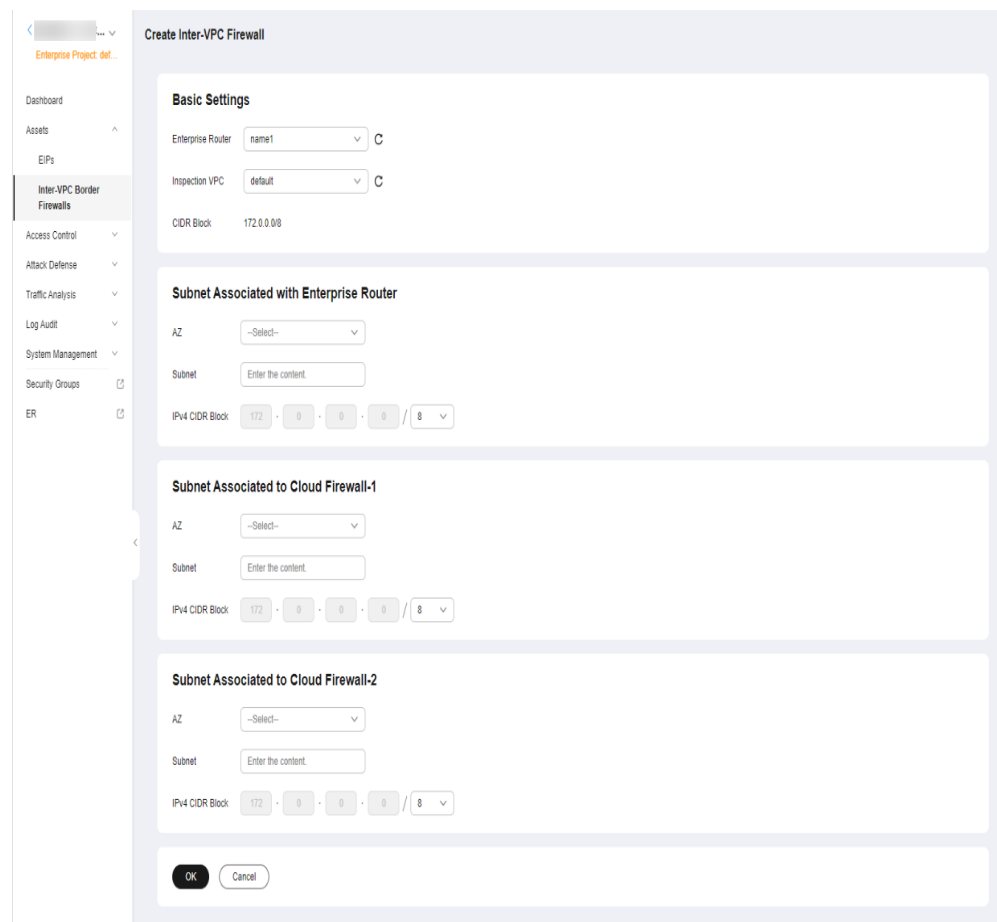


Figure 3-2 Creating a VPC border firewall (old version)

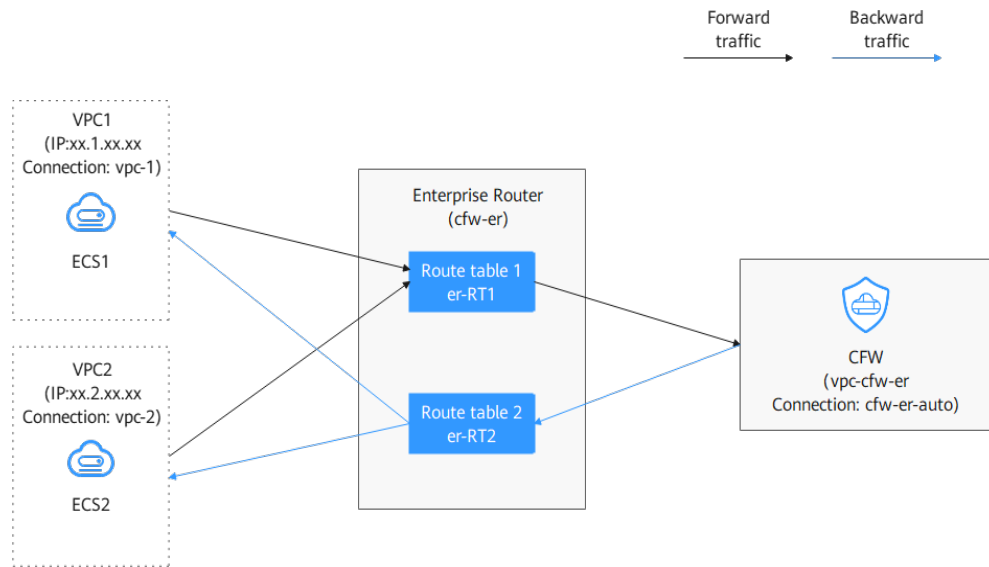


How to Configure

The process is as follows:


1. Create a firewall (for example, **vpc-cfw-er**) and associate it with subnets. For details, see [Creating a Firewall](#).
2. If you have just created a new enterprise router, [configure](#) it.
 - 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 [step 3](#).
 - b. Create attachments for all VPCs (including the firewall VPC and the VPC to be connected). For details, see [step 5](#).
 - c. Create two route tables (**er-RT1** and **er-RT2**, for example). For details, see [step 6](#).
 - d. Configure the association route table **er-RT1** to transmit traffic from the VPC to the CFW. For details, see [step 7](#).
Configure the propagation route table **er-RT2** to transmit traffic from the CFW to the VPC. For details, see [step 8](#).
 - e. Verify that the communication is normal when the traffic passes only through the enterprise router. For details, see [Verifying Configurations](#).
3. If your enterprise router has generated traffic, perform the following operations. For details, see [Configuring a Used Enterprise Router](#).
 - a. Create a connection named **vpc-cfw-er** to the firewall VPC. For details, see [step 4](#).
 - b. Delete the associations and propagations of the automatically generated firewall VPC (**vpc-cfw-er**) from the default route table (**er-RT1**). For details, see [step 5](#).
 - c. Create a route table (**er-RT2**) and configure the associations and propagations. For details, see [step 6](#) and [step 7](#).
 - d. Configure static routes in the default route table (**er-RT1**) and delete all propagations in the table. For details, see [step 8](#).
 - e. (Optional) Set the propagation route table. After setting the propagation route table to **er-RT2**, if you add new VPCs, you only need to configure attachments. For more information, see [step 9](#).


Figure 3-3 Traffic flow



Creating 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

Configuring a New 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 3-1 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) Supplementary information about the 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 3-2](#).

Table 3-2 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
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 .	Tag key: test Tag value: 01

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 3-4 Creating an association

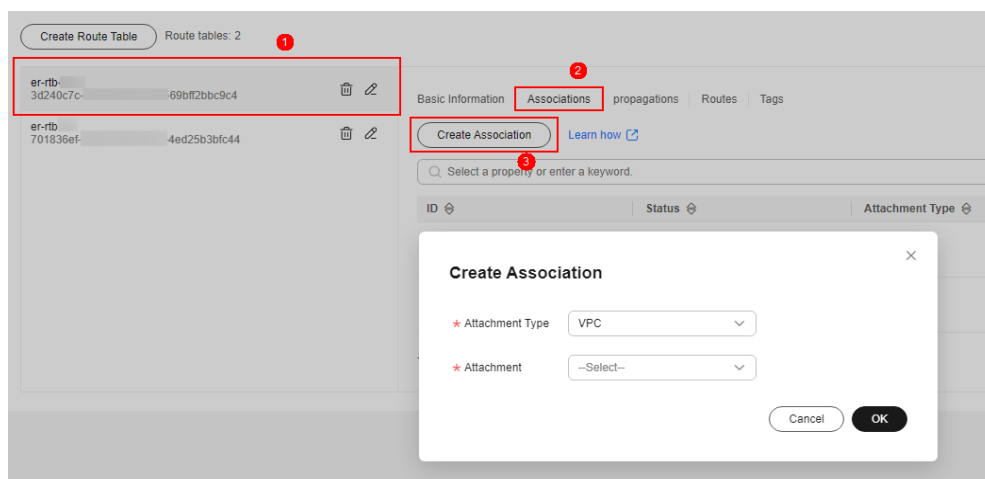


Table 3-3 VPC1 association parameters

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

Table 3-4 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 3-5 Creating a route

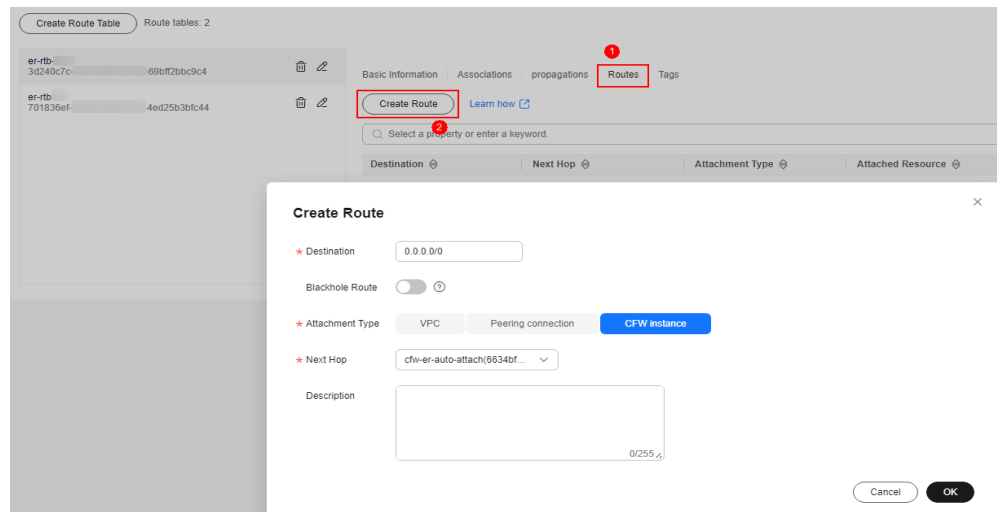


Table 3-5 Route parameters

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

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 3-6 Creating an association

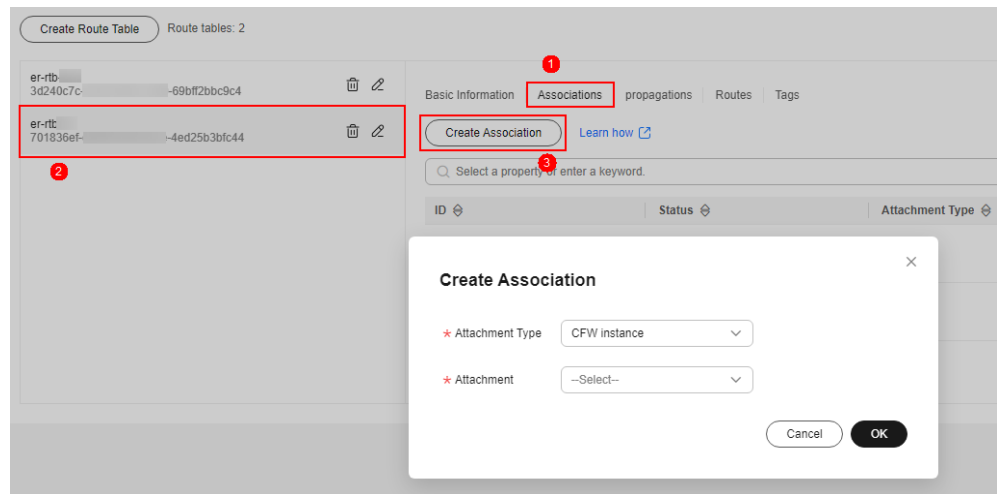


Table 3-6 Association parameters

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 3-7 Creating a propagation

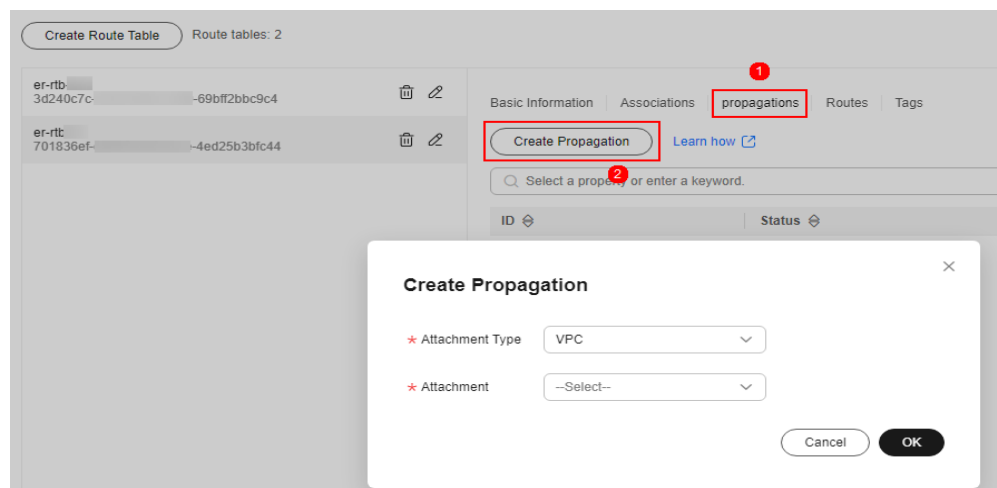


Table 3-7 Propagation parameters

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

Table 3-8 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.

----End

Verifying Configurations

Prerequisites

- You have completed configuration.
- Each of the two VPCs has an ECS.

Method

Ping ECSs in the VPC from each other to check whether they can properly communicate if there is no traffic passing through the firewall.

Troubleshooting

- Step 1** Check whether the two route tables of the enterprise router are correctly configured. For details, see [step 7](#) and [step 8](#).

Step 2 Check whether the default route tables of VPC1 and VPC2 direct routes to the enterprise router. For details, see [step 3](#).

----End


Configuring a Used Enterprise Router

Applicable Scenario

An enterprise router (for example, **vpc-cfw-er**) has been deployed and generated traffic, and the associations and propagations of its default route table (**er-RT1**) have been enabled.

Procedure

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

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

Step 3 In the service list, Choose **Networking > Enterprise Router**.

Step 4 Add a firewall attachment.

Click **Manage Attachment** to go to the **Attachments** tab. Click **Create Attachment** and configure parameters. The following table describes the parameters. After the attachment is created, the associations and propagations of the firewall VPC will be generated too.

Table 3-9 Attachment parameters

Parameter	Description	Example Value
Name	Attachment name The name: <ul style="list-style-type: none"> • Must contain 1 to 64 characters. • Can contain letters, digits, underscores (_), hyphens (-), and periods (. 	cfw-er-auto
Attachment Type	<ul style="list-style-type: none"> • Attachment Type: VPC • VPC: Select a firewall from the drop-down list. • Subnet: Select the subnet associated with CFW. 	<ul style="list-style-type: none"> • Attachment Type: VPC • VPC: vpc-cfw-er • Subnet: cfw-er-1 (xx.xx.1.0/24)

Parameter	Description	Example Value
Auto Add Routes	<ul style="list-style-type: none"> Enable this option if you want to automatically add routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the selected VPC. Do not enable this option if an existing route in the VPC route tables has a destination set to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 because the routes will fail to be added. After the attachment is created, manually add routes to the VPC route tables. 	Enable
Description	Route table description	-
Tag	<p>During the route table creation, you can tag the route table resources. Tags identify cloud resources for purposes of easy categorization and quick search.</p> <p>For details about tags, see Tag Overview.</p>	<p>Tag key: test</p> <p>Tag value: 01</p>

Step 5 Delete the associations and propagations of the firewall VPC (**vpc-cfw-er**) from the default route table **er-RT1**.

Click the route table and click the **Associations** tab. In the **Operation** column of the firewall VPC, click **Delete**. In the confirmation dialog box, click **Yes**.

Click the **Propagations** tab. In the **Operation** column of the firewall VPC, click **Delete**. In the confirmation dialog box, click **Yes**.

Step 6 Create route table **er-RT2**.

Click **Create Route Table**.

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

Table 3-10 Route table parameters

Parameter	Description	Example Value
Name	<p>Route table name. The name:</p> <ul style="list-style-type: none"> Must contain 1 to 64 characters. Can contain letters, digits, underscores (_), hyphens (-), and periods (.). 	er-RT2

Parameter	Description	Example Value
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 .	Tag key: test Tag value: 01

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

1. Select the route table **er-RT2**, click the **Associations** tab, and click **Create Association**.

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

Figure 3-8 Creating an association

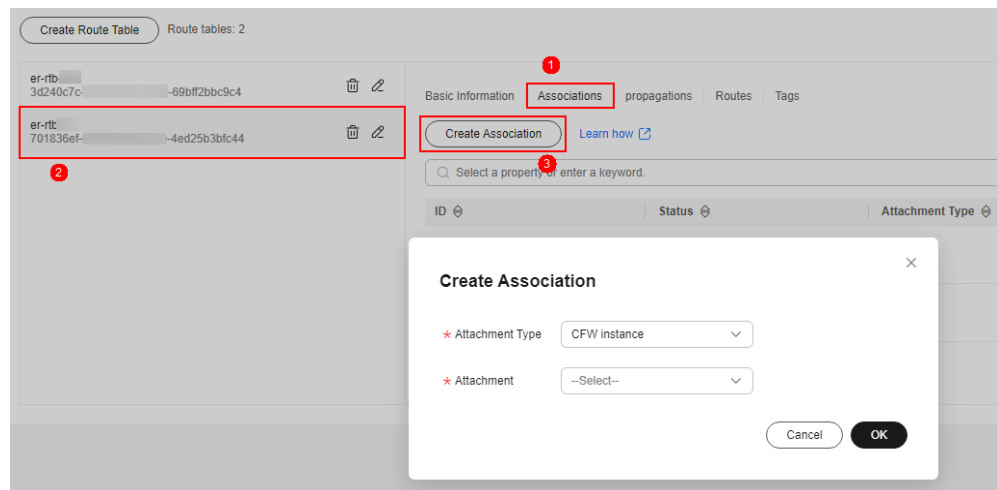


Table 3-11 Association parameters

Parameter	Description	Example Value
Attachment Type	Set Attachment Type to CFW instance .	VPC
Attachment	Select an item from the Attachment drop-down list.	cfw-er-auto

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

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

Figure 3-9 Creating a propagation

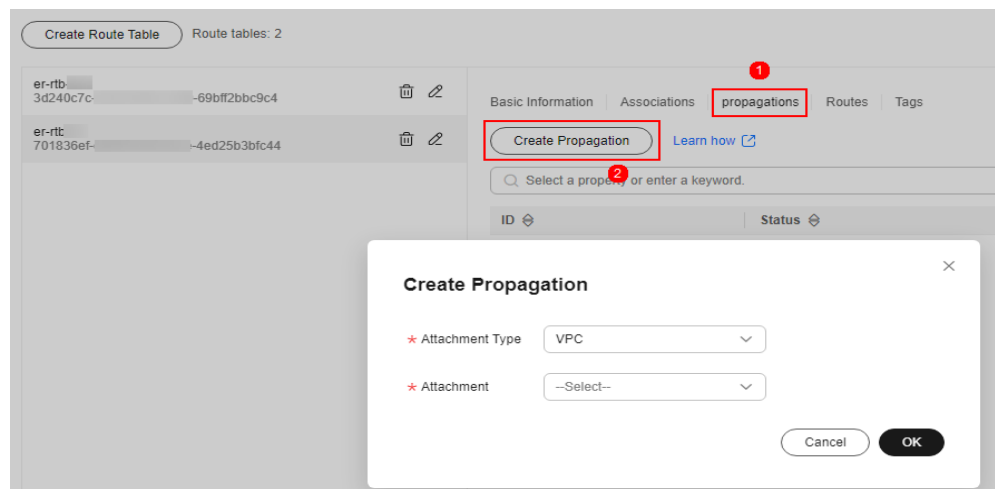


Table 3-12 Propagation parameters

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

Table 3-13 Propagation parameters

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

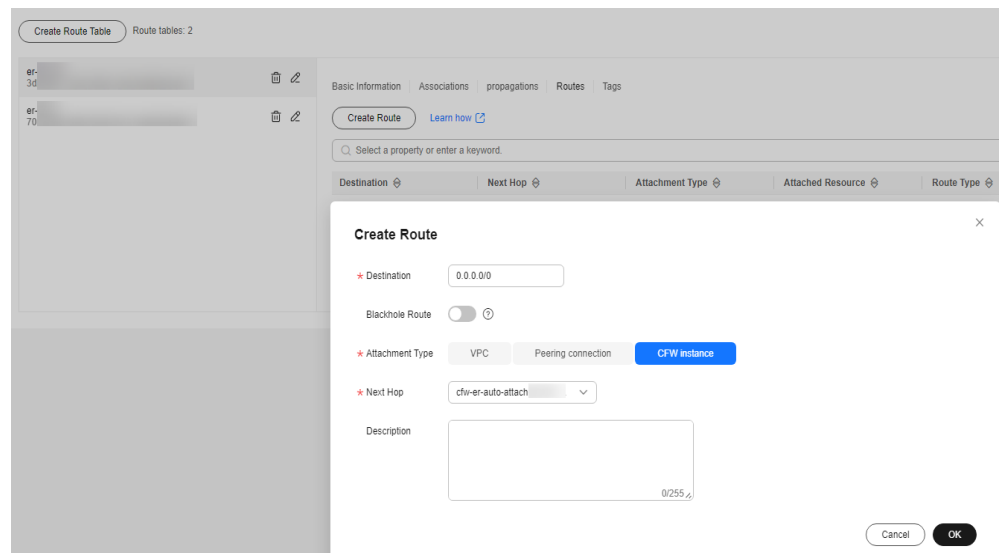
NOTE

- 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 Configure the default route table **er-RT1**.

1. Add a static route. Select the route table **er-RT1**, click the **Routes** tab, click **Create Route**, and configure the following parameters:
 - **Destination: 0.0.0.0/0**
 - **Attachment Type: CFW instance.**
 - **Next Hop: cfw-er-auto** (attachment of the firewall VPC)

Figure 3-10 Adding a static route



2. Delete the propagation in the route table **er-RT1**.
Click the **Propagations** tab. In the **Operation** column, click **Delete**. In the confirmation dialog box, click **Yes**.

NOTE

Delete all the propagations in the route table **er-RT1**.

Step 9 (Optional) You are advised to change the propagation route table of the enterprise router to the new route table (**er-RT2**), so that you simply need to configure an attachment when adding a VPC.

Go to the **Enterprise Router** page, choose **More > Modify Settings**, and set the propagation route table to **er-RT2**.

Figure 3-11 Modifying configurations

Modify Settings ✕

* Name

Default Route Table Association Enable ?

Association Route Table

Default Route Table Propagation Enable ?

Propagation Route Table

Auto Accept Shared Attachments Enable ?

NOTE

To use the enterprise router of account A to protect VPCs under account B, share the router with account B, and add an attachment in account B. For details, see [Creating a Sharing](#).

----End

4 Using CFW to Protect SNAT

4.1 SNAT Protection Overview

Scenario

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.

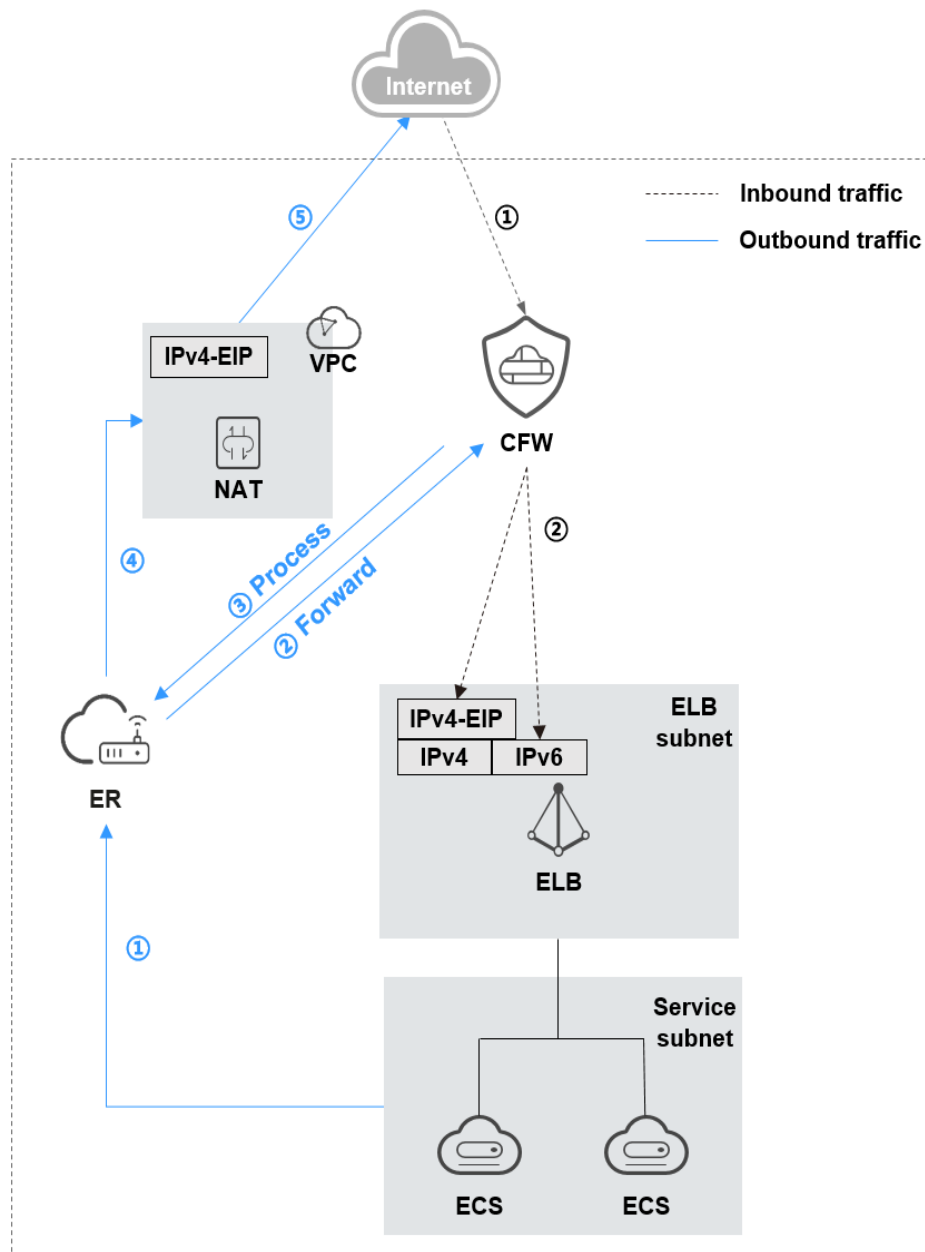
Prerequisites

- 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

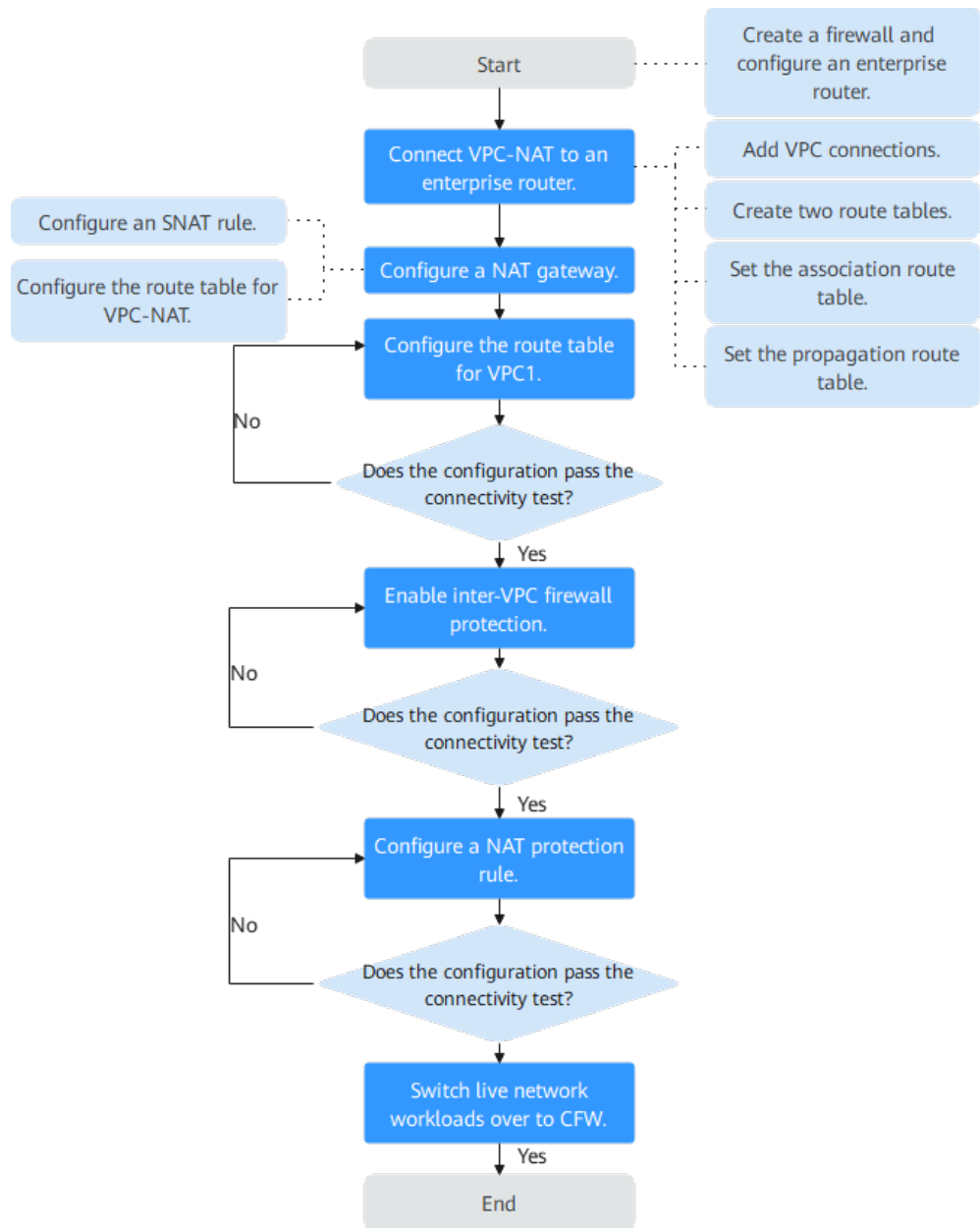
- You are advised to create an independent VPC for the NAT gateway. To avoid affecting access control, do not use the VPC in the network configurations of Elastic Cloud Servers (ECSs) or other instances.
- If the existing network is complex or improperly configured (for example, VPC CIDR blocks overlap, 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 4-1 SNAT protection configuration process



4.2 Connecting VPC1 and VPC-NAT to an Enterprise Router

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

Step 1: Add a VPC Connection


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

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 service list, click **Enterprise Router** under **Networking**. Click **Manage Route Table**.

Step 4 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 4-1](#).

Table 4-1 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 .

 **NOTE**

Create two route tables, to be used as an association route table and a propagation route table, respectively.

----End

Step 3: Set an Association Route Table

Step 1 In the service list, click **Enterprise Router** under **Networking**. Click **Manage Route Table**.

Step 2 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 4-2](#).

Figure 4-2 Creating an association

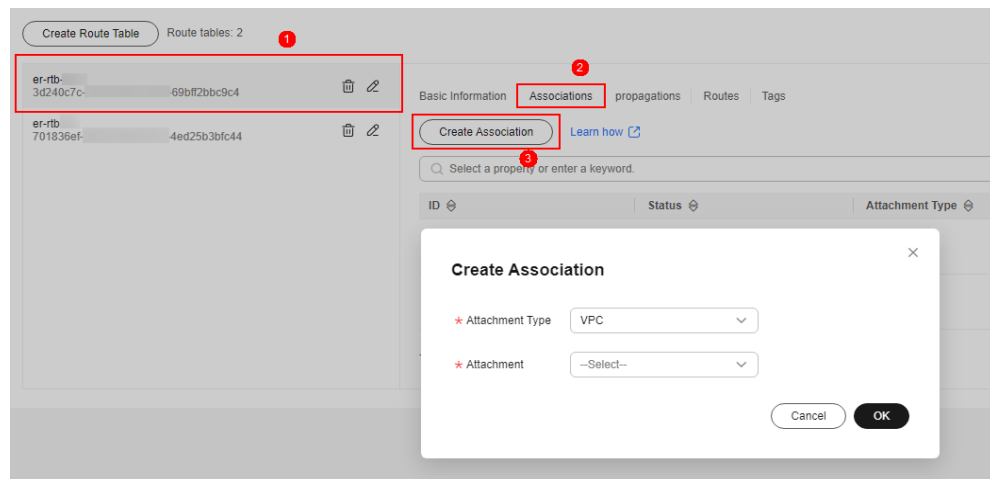


Table 4-2 Association parameters

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.

Step 3 Add a static route to the firewall. Click the **Routes** tab and click **Create Route**. For more information, see [Table 4-3](#).

Figure 4-3 Creating a route

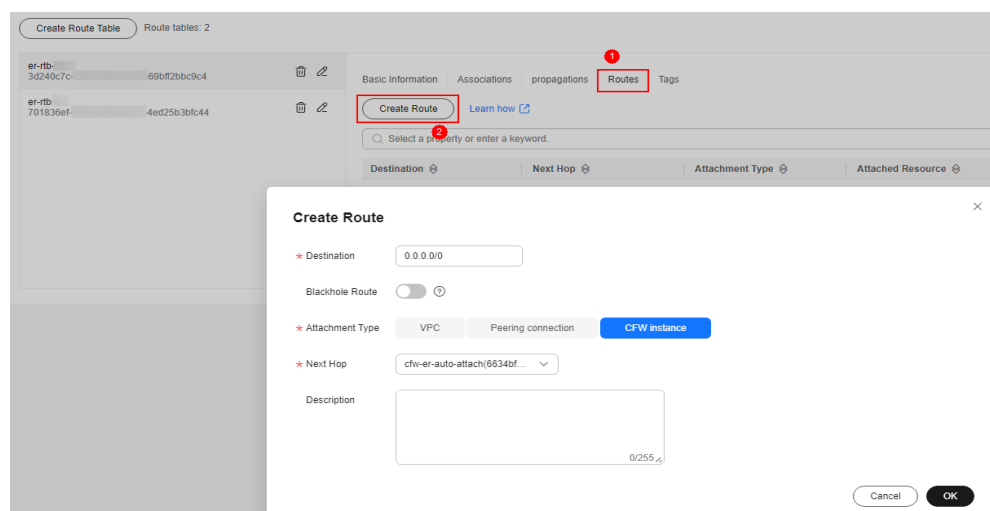


Table 4-3 Route parameters

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

----End

Step 4: Set a Propagation Route Table

- Step 1** In the service list, click **Enterprise Router** under **Networking**. Click **Manage Route Table**.
- Step 2** Configure associations. On the route table configuration page, select the propagation table, click the **Associations** tab, and click **Create Association**. For more information, see [Table 4-4](#).

Figure 4-4 Creating an association

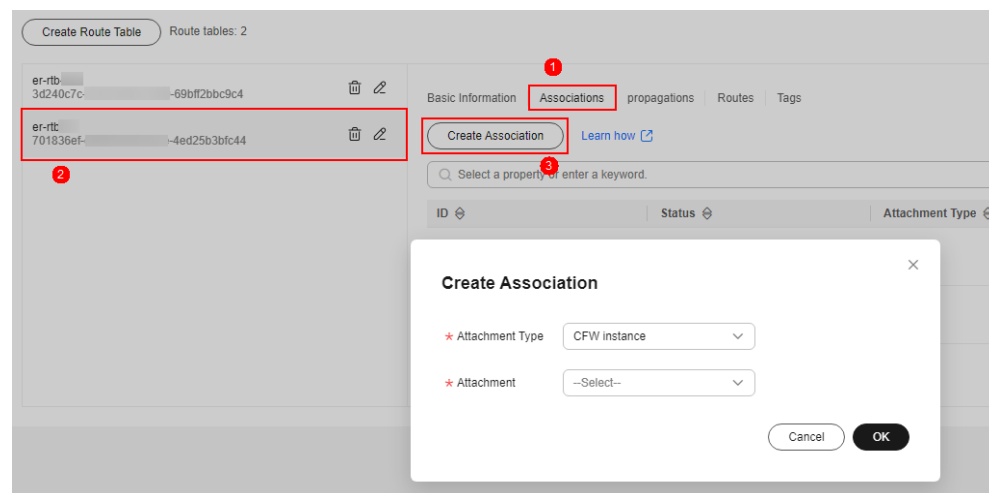


Table 4-4 Association parameters

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

Step 3 Create a propagation for VPC1. On the route table setting page, click the **Propagations** tab and click **Create Propagation**. For more information, see [Table 4-5](#).

Figure 4-5 Creating a propagation

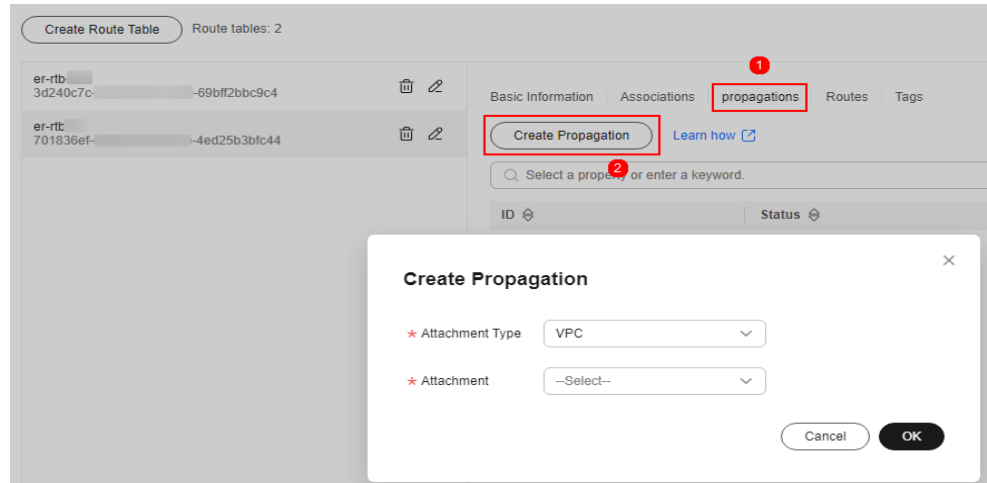


Table 4-5 Propagation parameters

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

Step 4 Add a static route to VPC-NAT. Click the **Routes** tab and click **Create Route**. For more information, see [Table 4-6](#).

Table 4-6 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

4.3 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 billing, see [Billing \(Public NAT Gateway\)](#).

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 4-7](#).

Table 4-7 Adding an SNAT rule

Parameter	Description
Scenario	Scenario where the SNAT rule is used. Select VPC .
CIDR Block	<p>Select Custom to enable servers in this subnet to use the SNAT rule to access the Internet.</p> <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>

Parameter	Description
EIP	EIP used for accessing the Internet. 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 4-8](#).

Table 4-8 Route parameters

Parameter	Description
Destination Type	Select IP address .
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.

Parameter	Description
Description	(Optional) Supplementary information about the route. NOTE Enter up to 255 characters. Angle brackets (< or >) are not allowed.

----End

4.4 Configuring a Route Table for VPC1

Procedure

- 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 4-9](#).

Table 4-9 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

4.5 Configuring a NAT Protection Rule

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

Procedure

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



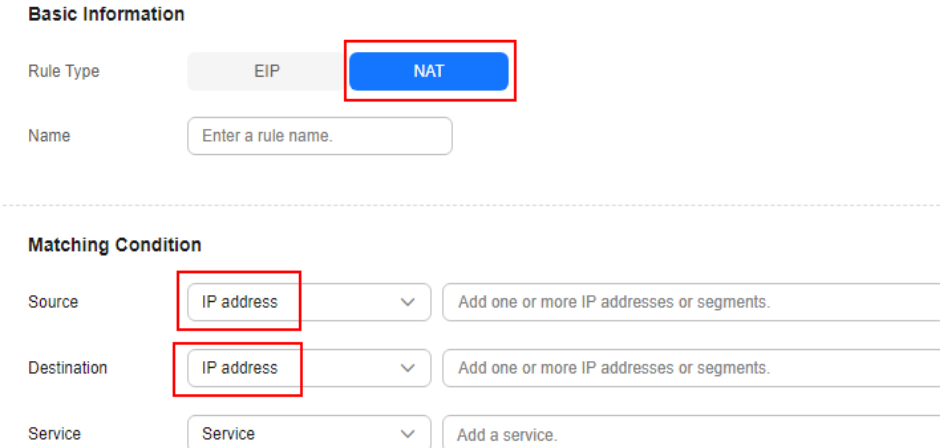
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details 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 the following parameters:
- **Protection Rule:** NAT protection
 - **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**.

Figure 4-6 Configuring a NAT protection rule



Basic Information

Rule Type: EIP NAT

Name:

Matching Condition

Source:

Destination:

Service:

Step 7 Click **OK**.

----End

5 Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN

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

Application Scenarios

If you purchase other Huawei Cloud products, service traffic is protected by multiple layers. In this case, reverse proxies may translate request IP addresses.

If a reverse proxy service (such as CDN, Advanced Anti-DDoS, or cloud WAF) is deployed before CFW, you need to configure a policy to permit the back-to-origin IP addresses so that traffic can be forwarded to and checked by CFW. For details, see [Configuring Policies](#). If you purchase dedicated or ELB-mode WAF instances, configure policies based on service requirements.

NOTE

If you purchase dedicated WAF instances, there are two protection scenarios:

- 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).

After the traffic passes through the reverse proxy, the source IP address is translated into the back-to-origin IP address. In this case, if an external attack occurs, CFW cannot obtain the real IP address of the attacker. You can obtain the real IP address based on the **X-Forwarded-For** field. For details, see [Viewing X-Forwarded-For](#).

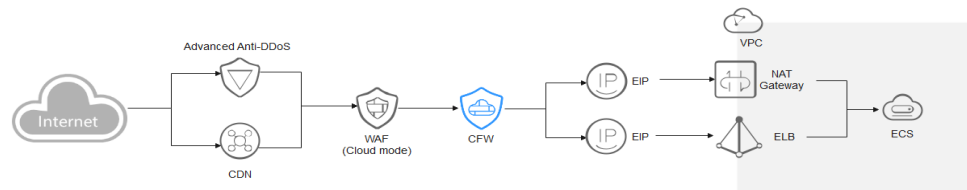
Traffic Flow

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.

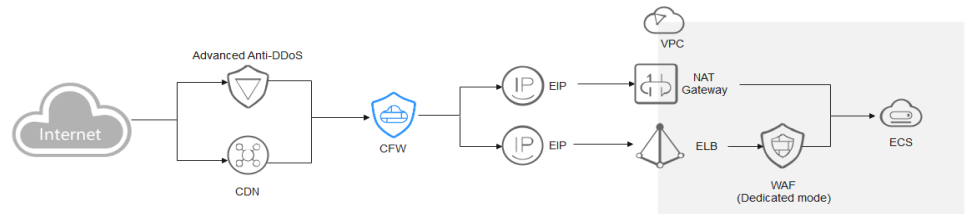
WAF supports three modes: cloud, dedicated, and ELB modes. The architecture varies depending on the mode, but the deployment positions of Advanced Anti-DDoS and CDN are fixed.

The following figures show the traffic flow.

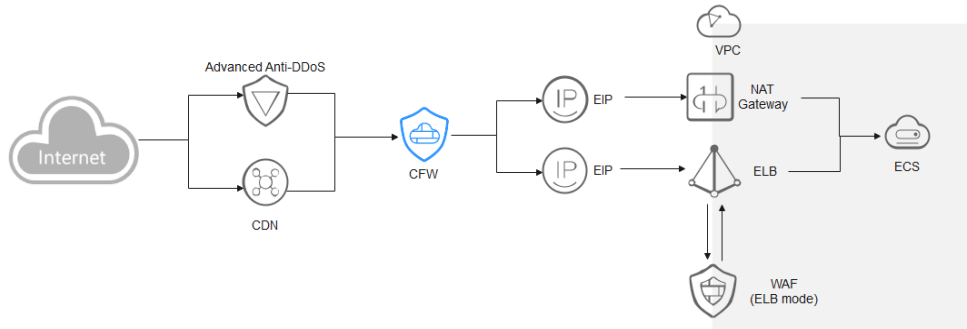
- Cloud WAF



- Dedicated WAF



- ELB-mode WAF



Configuring Policies

- You are advised to create a policy with the highest priority to permit all back-to-origin IP addresses. In this way, traffic still goes to CFW for check.
- If you whitelist back-to-origin IP addresses, the traffic is directly permitted to pass through and will not be checked by CFW.


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.

- 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?](#)

Viewing X-Forwarded-For

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

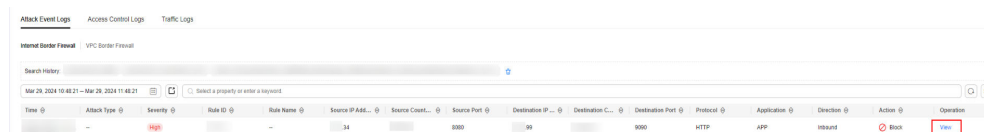
Step 2 Click  in the upper left corner of the management console and select a region or project.

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

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

Step 5 In the navigation pane, choose **Log Audit > Log Query**. Click **Attack Event Logs** tab. In the **Operation** column of the target event, click **View**.

Figure 5-1 Viewing attack event log details

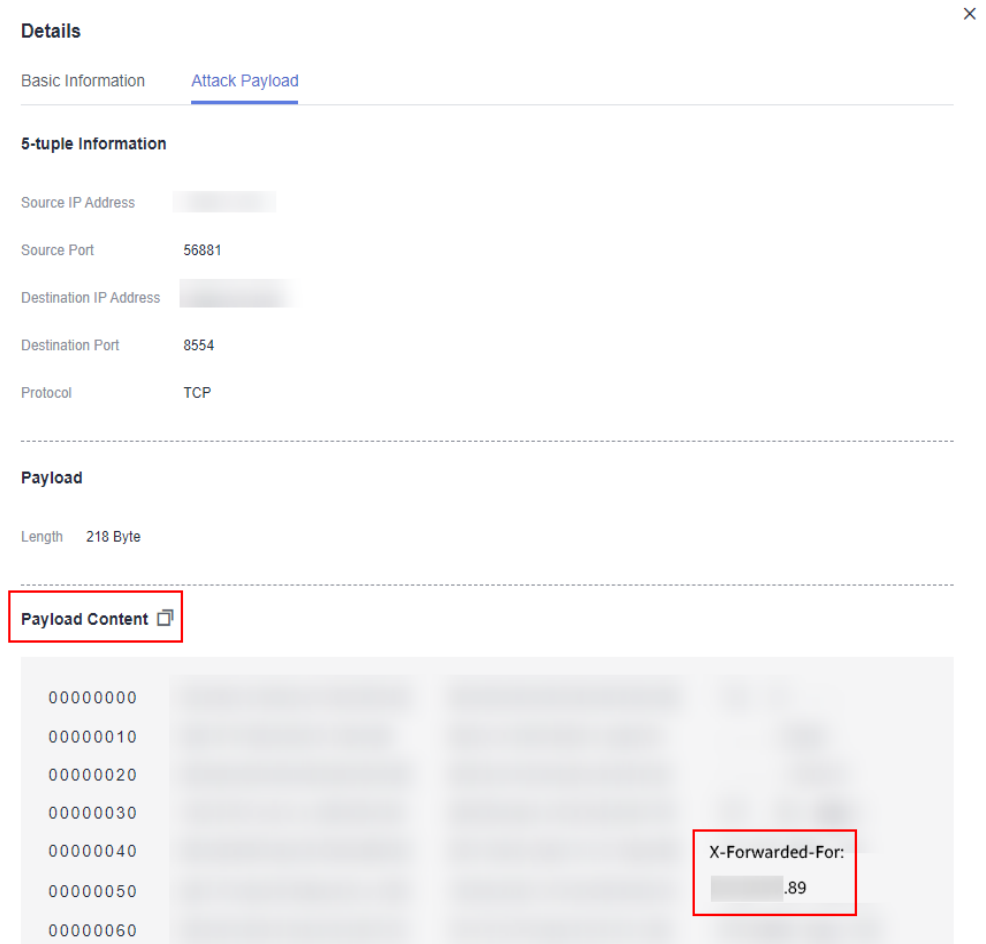


Time	Attack Type	Severity	Rule Name	Source IP Address	Source Port	Destination IP	Destination Port	Protocol	Application	Direction	Action	Operation
Mar 29, 2024 10:48:21 - Mar 29, 2024 11:48:21		High		34	8080	98	8080	HTTP	APP	Inbound	Block	View

Step 6 In the **Details** page, click the **Attack Payload** tab, and obtain the value of **X-Forwarded-For** field.

- Method 1: Check **X-Forwarded-For** (all IP addresses from the client to the last proxy server) in the **Payload Content** area.

Figure 5-2 X-Forwarded-For in the payload



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

Figure 5-3 Example of the Base64 decoding result

```

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

----End



6 Migrating Security Rules

CFW allows you to import protection rules in batches, helping you quickly migrate security rules.

Application Scenarios

If you need to migrate security rules from other clouds to Huawei Cloud or from other firewalls to CFW, you can import the security rules in batches.

Procedure

- Step 1** Export the rules configuration file from other firewalls through the API/policy backup function.
- Step 2** [Log in to the management console](#).
- Step 3** Click  in the upper left corner of the management console and select a region or project.
- Step 4** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
- Step 5** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 6** In the navigation pane, choose **Access Control > Access Policies**.
- Step 7** Click **Download Center** on the upper right of the list.
- Step 8** Click **Download Template** to download the rule import template to the local host.
- Step 9** Set parameters. For details about the parameters, see [Parameters of Rule Import Template](#).
 - [Example of Importing Parameters - Inbound Blocking Rule](#)
 - [Example of Importing Parameters - Access of Address Group Members to Domain Group Members](#)

 NOTE

- 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 object group in the protection rule table.

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. Check whether the resources corresponding to the protection rules are protected by CFW. For details about EIP resources, see [Viewing EIP Information](#). For details about VPC resources, 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.

Step 13 (Optional) Periodically check the rule matching status by viewing the policy assistant or 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](#).

----End

Example of Importing Parameters - Inbound Blocking Rule

Original 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

Enter the converted rule.

- 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

Example of Importing Parameters - Access of Address Group Members to Domain Group Members

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

A Change History

Released On	Description
2024-04-09	This is the sixth official release. Added Migrating Security Rules .
2024-01-04	This is the fifth official release. Added Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN .
2023-11-10	This issue is the fourth official release. Optimized: Description about checking protection details in Configuring Access Policies for IP Address Groups and Service Groups . Version constraints in Configuring the VPC Border Firewall .
2023-08-30	This issue is the third official release. Added Using CFW to Protect SNAT .
2023-03-30	This issue is the second official release. Added Configuring the VPC Border Firewall .
2022-07-30	This issue is the first official release.