ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall

Firewall Settings

Document Version: 20220712

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings> Network> Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Internet firewall 05

2.VPC Firewall 07

2.1. VPC firewall limits 07

2.2. Create a VPC firewall 09

2.3. Enable or disable VPC Firewall 16

2.4. Protect traffic between VPCs connected by using a CEN tr... 18

2.5. Protect a specific amount of traffic between VPCs connect... 22

1.Internet firewall

The Internet firewall monitors traffic between the Internet and your public IP addresses. After you activate Cloud Firewall, you can enable or disable the Internet firewall for public IP addresses within your Alibaba Cloud account. This topic describes how to enable or disable the Internet firewall.

Background information

You can use Cloud Firewall to protect your traffic only after you enable the required firewalls. After you enable the Internet firewall, Cloud Firewall can monitor and analyze traffic of your public IP addresses.

> ? **Note** We recommend that you enable the Internet firewall for all assets within your Alibaba Cloud account.

Prerequisites

The quota of public IP addresses is not exhausted. The quota refers to the maximum number of public IP addresses that the Internet firewall can protect. For more information about the quotas in different Cloud Firewall editions, see Functions and features. To increase a quota, you can go to the Upgrade/Downgrade page and increase the value of Protected Public IP Addresses. For more information, see Upgrade Cloud Firewall and change configurations.

Procedure

1. Log on to the . In the left-side navigation pane, choose **Firewall Settings > Firewall Settings**.
2. On the **Internet Firewall** tab, enable or disable the Internet firewall for public IP addresses in the following scenarios:
   - Enable or disable the Internet firewall for all public IP addresses

     In the **Public IP**, **By Asset Region**, or **Asset Type** section, click **Enable Firewall** or **Disable Firewall** to enable or disable the Internet firewall for all public IP addresses with a few clicks.
   - Enable or disable the Internet firewall for one or more public IP addresses
     a. In the list of public IP addresses on the **IPv4** or **IPv6** tab, find the IP address for which you want to enable or disable the Internet firewall.

        You can search for the IP address based on conditions such as **Asset Type**, **Region**, and **Protection Status**. Alternatively, you can enter an instance ID or UID to search for the IP address.
     b. Click **Enable Firewall** or **Disable Firewall** in the **Actions** column to enable or disable the Internet firewall for the IP address.
   - Enable or disable the Internet firewall for public IP addresses that are newly added

     By default, **Automatically Enable Firewalls for New Assets** is turned off. If you turn on the switch, the Internet firewall is automatically enabled for public IP addresses that are newly added to your Alibaba Cloud account.

What to do next

You can perform the following operations based on your business requirements:

- Upgrade specifications

Click **Increase Quota for Policies** to upgrade the edition of Cloud Firewall or upgrade the specifications. For more information, see Upgrade Cloud Firewall and change configurations.

- View the numbers of unprotected and protected IPv6 addresses and IPv4 addresses

  i. Click the icon to view the numbers of unprotected and protected IPv6 addresses and IPv4 addresses.

  ii. Click the number of IPv6 addresses or IPv4 addresses. The information about the IP addresses is displayed in the list of public IP addresses in the lower part of the page.

  For example, if you click the number of unprotected IPv6 addresses, the information about the IPv6 addresses is displayed in the list of public IP addresses.

- Synchronize asset information

  Click **Update Assets**. The system synchronizes the information about assets. The process requires one to two minutes.

Result

After you enable the Internet firewall, the firewall status changes to **Enabled** in the **Firewall Status** column. The value Enabled indicates that the Internet firewall takes effect. After you disable the Internet firewall, the firewall status changes to **Disabled** in the Firewall Status column. The value Disabled indicates that the Internet firewall no longer provides protection.

Related information

- Create access control policies for outbound and inbound traffic on the Internet firewall
- FAQ about the Internet firewall

2.VPC Firewall

2.1. VPC firewall limits

This topic describes the limits of virtual private cloud (VPC) firewalls and the solutions that are provided.

General limits

Item	Solution
A VPC quota of 20 is allowed for each region. A VPC firewall that is created by Cloud Firewall consumes this quota. After you enable a VPC firewall, Cloud Firewall automatically creates a VPC named Cloud_Firewall_VPC for each region. This VPC is displayed on the **VPCs** page of the VPC console. If a region has 20 VPCs, you cannot enable VPC firewalls for this region.	If the VPC quota is exhausted, log on to the VPC console and go to the **Quota Management** page to increase the VPC quota. Notice If the VPC quota reaches the upper limit, contact the after-sales service in the specified DingTalk group.

Limits on Cloud Enterprise Network (CEN)

Item	Solution
If multiple VPCs in a CEN instance are created by different Alibaba Cloud accounts, Cloud Firewall must meet the following conditions: Cloud Firewall is authorized to access all VPCs and is of the Ultimate Edition. Otherwise, VPC firewalls cannot be created.	• Before you enable a VPC firewall, you must use your Alibaba Cloud accounts to separately log on to the Cloud Firewall console and complete the authorization. For more information, see Authorize Cloud Firewall to access other cloud resources. • You must upgrade your Cloud Firewall to the Ultimate Edition. For more information, see Upgrade the Cloud Firewall edition.
VPC Firewall can be enabled for a CEN instance only if VPC Firewall is supported in all regions where the VPCs in the CEN instance reside.	Make sure that VPC Firewall is supported in all regions where the VPCs in the CEN instance reside. For more information, see Supported regions.
If you enabled a VPC firewall before May 1, 2021, and you used a public IP address as a private IP address in your network topology, your access to Server Load Balancer (SLB) and ApsaraDB RDS is interrupted. Notice If you enable a VPC firewall on or after May 1, 2021, you are not subject to this limit.	We recommend that you develop a network plan based on the standards. We also recommend that you do not use a public IP address as a private IP address.

Item	Solution
You can advertise up to 100 routes in a CEN instance.	We recommend that you advertise less than or equal to 100 routes. For more information, contact the after-sales service in the specified DingTalk group.
After you enable a VPC firewall, a custom route is added to your VPC route table. If the number of custom routes in your VPC route table reaches the upper limit, you can no longer enable VPC firewalls. The maximum number of custom routes allowed for each VPC route table is 400.	Increase the VPC quota. Log on to the VPC console. Then, go to the **Quota Management** page and increase the maximum number of custom routes allowed for each route table within your Alibaba Cloud account.
If a VPC in a CEN instance has a custom route table that is associated with a vSwitch, you cannot enable a VPC firewall for the CEN instance.	Delete the custom route table or disassociate the custom route table from the vSwitch.
Cloud Firewall does not protect the following mutual access traffic that does not pass through Cloud Firewall: • Mutual access traffic between Virtual Border Routers (VBRs) • Mutual access traffic between Cloud Connect Networks (CCNs) • Mutual access traffic between VBRs and CCNs	For more information, contact the after-sales service in the specified DingTalk group.
When you enable or disable VPC Firewall for an SLB or ApsaraDB RDS instance, existing persistent connections may fail.	• Before you enable or disable VPC Firewall, make sure that the SLB instance and its backend server reside in the current VPC. This way, network latency and network jitter are prevented. • Configure the keep-connection-alive and reconnection mechanisms on the client.
The total number of VPCs and regions for which VPC Firewall is enabled must be less than or equal to 32.	None.
When you enable a VPC firewall for a CEN instance, you can add up to 15 network instances.	We recommend that you use a CEN transit router. For more information, contact the after-sales service in the specified DingTalk group.
If a CEN instance has routing policies whose **Routing Policy Action** is set to **Deny**, services are interrupted if you create a VPC firewall for the CEN instance. The routing policies exclude system routing policies whose priority is set to 5000 and Routing Policy Action is set to Deny.	We recommend that you delete the relevant routing policies or contact the after-sales service in the specified DingTalk group.

Limits on a CEN transit router

Item	Solution
When you enable a VPC firewall for a CEN instance, you can add up to 100 network instances such as VPCs, VBRs, and CCNs to the transit router in each region. **Note** The total number of VPCs that you can add to a transit router includes the VPC that is automatically created when you enable the VPC firewall. The created VPC is named Cloud_Firewall_VPC and is displayed on the **VPCs** page of the VPC console.	None.
A transit router is subject to the following limits: ● After you create a VPC firewall in **automatic mode**, you must contact the after-sales service to add the automatically created VPC named Cloud_Firewall_VPC to the required whitelist. After the VPC is added to the whitelist, you can enable the VPC firewall. ● After you create a VPC firewall in **manual mode**, you must contact the after-sales service to add the newly created VPC to the required whitelist. After the VPC is added to the whitelist, you can enable the VPC firewall.	To add a VPC to the whitelist, contact the after-sales service in the specified DingTalk group.

Limits on Express Connect

Item	Solution
If you enable a VPC firewall for Express Connect, the firewall does not protect the mutual access traffic between VPCs that reside in different regions or belong to different Alibaba Cloud accounts. The firewall also does not protect the mutual access traffic between VPCs and VBRs.	If you want to protect the mutual access traffic in these scenarios, we recommend that you use CEN to replace Express Connect. For more information, contact the after-sales service in the specified DingTalk group.
After you enable a VPC firewall, a custom route is added to your VPC route table. If the number of custom routes in your VPC route table reaches the upper limit, you can no longer enable VPC firewalls. The maximum number of custom routes allowed for each VPC route table is 400.	Increase the VPC quota. Log on to the VPC console. Then, go to the **Quota Management** page and increase the maximum number of custom routes allowed for each route table within your Alibaba Cloud account.
You cannot advertise routes that use 32-bit subnet masks in Express Connect. If the routes that use 32-bit subnet masks are advertised and the VPC firewall is enabled, the connections to the network of the subnet masks are interrupted.	Before you enable a VPC firewall, we recommend that you use the subnet masks that are less than or equal to 30 bits in length. Alternatively, contact the after-sales service in the specified DingTalk group.

2.2. Create a VPC firewall

You can use a virtual private cloud (VPC) firewall to detect and manage traffic between two VPCs. If your VPCs are connected by using an Express Connect circuit or if the VPCs belong to the same Cloud Enterprise Network (CEN) instance, you can create a VPC firewall for the Express Connect circuit or the CEN instance. Cloud Firewall can be used to manage the traffic between two VPCs only after a VPC firewall is created and enabled.

Prerequisites

A CEN instance or an Express Connect circuit is created, and two VPCs are connected by using the instance or circuit. For more information, see Connect two VPCs under the same Alibaba Cloud account.

Context

A VPC firewall can protect the traffic between two connected VPCs and the traffic between a VPC and a data center.

A VPC firewall is suitable for the following scenarios:

- Two VPCs are connected by using a CEN instance. For more information, see Create a VPC firewall for a CEN instance.

  > **Note** Cloud Firewall can protect the traffic that passes through the custom routes added to CEN transit routers.

- Two VPCs are connected by using an Express Connect circuit. For more information, see Create a VPC firewall for an Express Connect circuit.

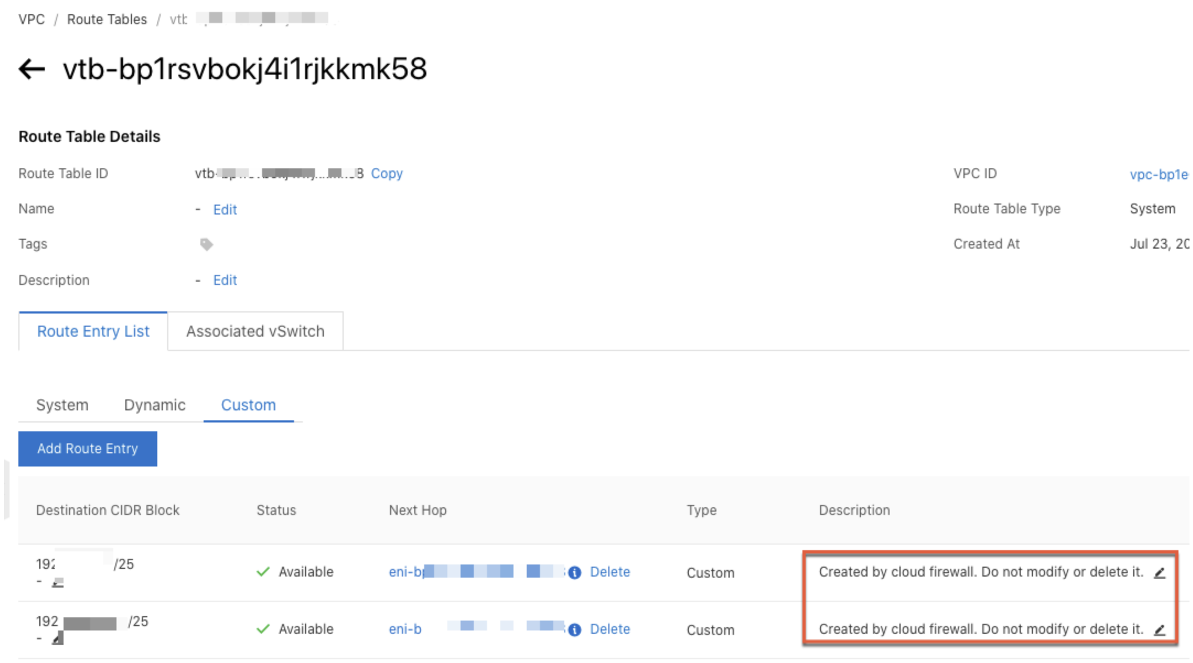
Editions that support VPC Firewall

Cloud Firewall Enterprise Edition and Ultimate Edition support VPC Firewall. Cloud Firewall Premium Edition does not support VPC Firewall. The VPC Firewall tab is not displayed in the console of Cloud Firewall Premium Edition.

Usage notes

After you create a VPC firewall in the Cloud Firewall console, Cloud Firewall automatically creates the following resources:

- A VPC named `Cloud_Firewall_VPC` .
- A vSwitch named `Cloud_Firewall_VSWITCH` . The vSwitch uses the CIDR block 10.219.219.216/29.
- A custom route entry that has the following remarks: `Created by cloud firewall. Do not modify or delete it.`



VPC / Route Tables / vtb [redacted]

← vtb-bp1rsvbokj4i1rjkkmk58

Route Table Details

Route Table ID	vtb-[redacted]8 Copy	VPC ID	vpc-bp1e
Name	- Edit	Route Table Type	System
Tags		Created At	Jul 23, 20
Description	- Edit		

Destination CIDR Block	Status	Next Hop	Type	Description
19[redacted]/25 -	✓ Available	eni-b[redacted] Delete	Custom	Created by cloud firewall. Do not modify or delete it.
192[redacted]/25 -	✓ Available	eni-b[redacted] Delete	Custom	Created by cloud firewall. Do not modify or delete it.

Take note of the following items:

- Do not add other cloud resources to the created VPC.
- Do not manually modify or delete the network resources in the created VPC.
- Do not use the CIDR block 10.219.219.216/29 that the created vSwitch uses during network planning. This way, you can prevent CIDR block conflicts that cause communication failures between two VPCs.

Create a VPC firewall for a CEN instance

Cloud Firewall can protect cross-account VPCs that are connected by using a CEN instance. A cross-account VPC indicates that the Alibaba Cloud account used to create the VPC is different from the current Alibaba Cloud account of the CEN instance in which the VPC exists. If a cross-account VPC exists in a CEN instance, you must authorize Cloud Firewall to access the cloud resources of the account that is used to create the cross-account VPC. If you create a VPC firewall for the cross-account VPC but do not authorize Cloud Firewall to access the cloud resources, a message indicating that unauthorized VPCs exist and you cannot create a VPC firewall is displayed.

To authorize Cloud Firewall to access the cloud resources of an Alibaba Cloud account, perform the following steps:

1. Log on to the by using the Alibaba Cloud account.
2. In the **Service-Linked Role for Cloud Firewall** dialog box, click **OK**.

Note If you want to create a VPC firewall for a CEN instance, take note of the following items:

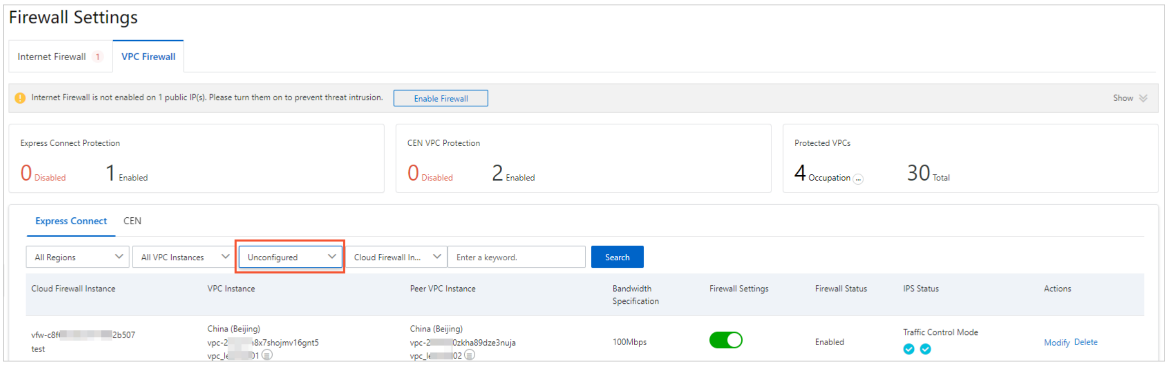
- The VPC firewall can be used to protect the cross-region VPCs and cross-account VPCs. If the Alibaba Cloud account of the CEN instance uses a paid edition of Cloud Firewall, VPC Firewall is supported for a cross-account VPC in the CEN instance regardless of whether the Alibaba Cloud account of the VPC uses a paid edition. The paid editions of Cloud Firewall are Enterprise and Ultimate. VPC Firewall is supported only if the Alibaba Cloud account that is used to create the CEN instance purchases a paid edition of Cloud Firewall.
- VPC Firewall can be enabled for a maximum of 10 VPCs in a region of a CEN instance. If you want to increase the quota, submit a .
- VPC firewalls can protect traffic between VPCs, between a VPC and a Virtual Border Router (VBR) or a data center, and between a VPC and a Cloud Connect Network (CCN) instance. However, VPC firewalls cannot protect traffic between VBRs, between CCN instances, or between a CCN instance and a VBR.

To create a VPC firewall for a CEN instance, perform the following steps:

Note

1.
2.
3. On the **Firewall Settings** page, click the **VPC Firewall** tab.
4. On the **VPC Firewall** tab, click the **CEN** tab.
5. Find the CEN instance for which you want to create a VPC firewall and click **Create** in the Actions column.

   Cloud Firewall can manage traffic between two VPCs that are connected by using an Enterprise Edition transit router of the CEN instance.

   Internet Firewall is not enabled on 1 public IP(s). Please turn them on to prevent threat intrusion.

Cloud Firewall Instance	VPC Instance	Peer VPC Instance	Bandwidth Specification	Firewall Settings	Firewall Status	IPS Status	Actions
vfw-c8f[redacted]2b507 test	China (Beijing) vpc-2[redacted]8x7shojmv16gnt5 vpc_le[redacted]01	China (Beijing) vpc-2[redacted]0zkha89dze3nuja vpc_le[redacted]02	100Mbps		Enabled	Traffic Control Mode ✓ ✓	Modify Delete

   If a large number of CEN instances exist, you can search for CEN instances by region, CEN name, VPC name, or configuration status of Cloud Firewall. For example, you can select **Unconfigured** from the configuration status drop-down list and click **Search** to query all CEN instances for which Cloud Firewall is not configured.
6. In the **Create VPC Firewall** dialog box, configure the parameters.

   The following table describes the parameters that are required to create a VPC firewall for CEN-connected VPCs.

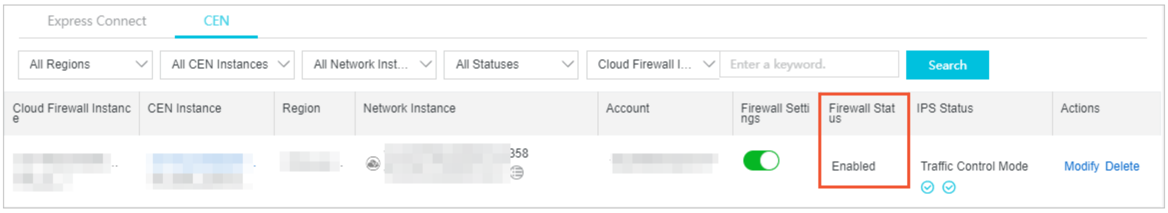
Parameter	Description
Instance Name	The name of the VPC firewall. We recommend that you enter a unique name to help you identify the VPC firewall based on your business requirements.
Routing Mode	The routing mode of the traffic that passes through Cloud Firewall. This parameter is required only when you use an Enterprise Edition transit router of the CEN instance. Valid values: ○ Automatic: If you select this option, Cloud Firewall automatically assigns a VPC and a CIDR block that the vSwitch uses for the VPC firewall. ○ Manual: You can select this option to manually assign a VPC and a CIDR block that the vSwitch uses for the VPC firewall without affecting the existing network architecture. This option applies if you deployed multiple VPCs and CIDR blocks in your network, used CEN transit routers to connect the VPCs, and planned CIDR blocks for Cloud Firewall. **Notice** If you select this option, you must select the VPC with which the CEN instance is associated and the vSwitch that the CEN instance uses. In manual mode, you must renew your Cloud Firewall at the earliest opportunity before it expires. If your Cloud Firewall expires, the features of Cloud Firewall become unavailable, and traffic cannot be directed to the VPC firewall that you created. As a result, network interruptions occur.
IPS Mode	The working mode of the intrusion prevention system (IPS). Valid values: ○ **Monitoring Mode**: If you select this option, Cloud Firewall monitors traffic and sends alerts when malicious traffic is detected. ○ **Traffic Control Mode**: If you select this option, Cloud Firewall intercepts malicious traffic and blocks intrusion attempts. **Note** This setting applies to all VPCs that belong to a CEN instance.

Parameter	Description
IPS Capabilities	The intrusion prevention policies that you want to enable. Valid values: ○ **Basic Policies**: Basic policies provide basic intrusion prevention capabilities such as protection against brute-force attacks and attacks that exploit command execution vulnerabilities. Basic policies also allow you to manage the connections from compromised hosts to a command and control (C&C) server. ○ **Virtual Patches**: Virtual patches can be used to defend against the common high-risk application vulnerabilities in real time. Note This setting applies to all VPCs that belong to a CEN instance.

7. Click **Submit**. In the message that appears, click Submit. The VPC firewall is created.

8. Turn on ● in the Firewall Settings column.

   Wait until the VPC firewall takes effect. If the status in the **Firewall Status** column of the VPC firewall changes to **Enabled**, the VPC firewall takes effect.



Express Connect | CEN

All Regions | All CEN Instances | All Network Inst... | All Statuses | Cloud Firewall I... | Enter a keyword. | Search

Cloud Firewall Instance	CEN Instance	Region	Network Instance	Account	Firewall Settings	Firewall Status	IPS Status	Actions
[redacted]	[redacted]	[redacted]	[redacted] 358	[redacted]	●	Enabled	Traffic Control Mode ✓ ✓	Modify Delete

Note

Create a VPC firewall for an Express Connect circuit

Note If your VPCs are connected by using an Express Connect circuit, you can create a VPC firewall to protect traffic between VPCs in the same region. However, the VPC firewall cannot protect traffic between a VPC and a VBR or between the VPCs that are deployed in different regions or created by using different Alibaba Cloud accounts.

To create a VPC firewall for an Express Connect circuit, perform the following steps:

1.
2.
3. On the **Firewall Settings** page, click the **VPC Firewall** tab.
4. On the **VPC Firewall** tab, click the **Express Connect** tab.
5. Find the Express Connect circuit for which you want to create a VPC firewall and click **Create** in the Actions column.

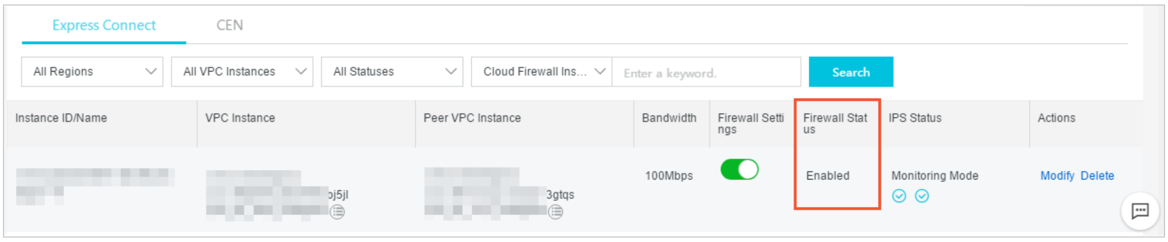
   If a large number of Express Connect circuits exist, you can search for circuits by region, VPC, or configuration status of Cloud Firewall. For example, you can select **Unconfigured** from the configuration status drop-down list and click **Search** to query all Express Connect circuits for which Cloud Firewall is not configured.

6. In the **Create VPC Firewall** dialog box, configure the parameters. The following table describes the parameters.

Parameter	Description
Instance Name	The name of the VPC firewall. We recommend that you enter a unique name to help you identify the VPC firewall based on your business requirements.
Connection Type	The type of the connection between VPCs or between a VPC and a data center. In this scenario, the value is fixed to **Express Connect**.
VPC	The region and the name of the VPC. Confirm the information and configure **Route Table** and **Destination CIDR Block**. ○ Route table When you create a VPC, the system automatically creates a default route table. You can add system routes to the route table to manage VPC traffic. VPC allows you to create multiple route tables based on your business requirements. For more information, see Route table overview. When you create a VPC firewall in the Cloud Firewall console, Cloud Firewall automatically reads your VPC route tables. Express Connect supports multiple route tables. When you create a VPC firewall for an Express Connect circuit, you can view multiple VPC route tables and select the route tables that you want to protect. ○ Destination CIDR block After you select a route table from the Route Table drop-down list, the default destination CIDR block of the route table is displayed in the Destination CIDR Block section. If you need to protect traffic that is destined for other CIDR blocks, you can modify the destination CIDR block. You can add multiple CIDR blocks. Separate the CIDR blocks with commas (,).
Peer VPC	The region and the name of the peer VPC. Confirm the information and configure **Peer Route Table** and **Peer Destination CIDR Blocks**. For more information about route tables and destination CIDR blocks, see the **VPC** configuration description.
Intrusion Prevention	The intrusion prevention policies that you want to enable. Valid values: ○ **Basic Policies**: Basic policies provide basic intrusion prevention capabilities such as protection against brute-force attacks and attacks that exploit command execution vulnerabilities. Basic policies also allow you to manage the connections from compromised hosts to a command and control (C&C) server. ○ **Virtual Patches**: Virtual patches can be used to defend against the common high-risk application vulnerabilities in real time.
Enable VPC Firewall	After you turn on Enable VPC Firewall, a VPC firewall is automatically enabled after you create the firewall. If you do not require the VPC firewall to be automatically enabled after it is created, turn off Enable VPC Firewall.

7. Click **Submit**. In the message that appears, click Submit.

   The VPC firewall is created. If you turn on Enable VPC Firewall when you configure the VPC firewall, wait until the VPC firewall is enabled. If the status in the **Firewall Status** column of the VPC firewall changes to **Enabled**, the VPC firewall takes effect.

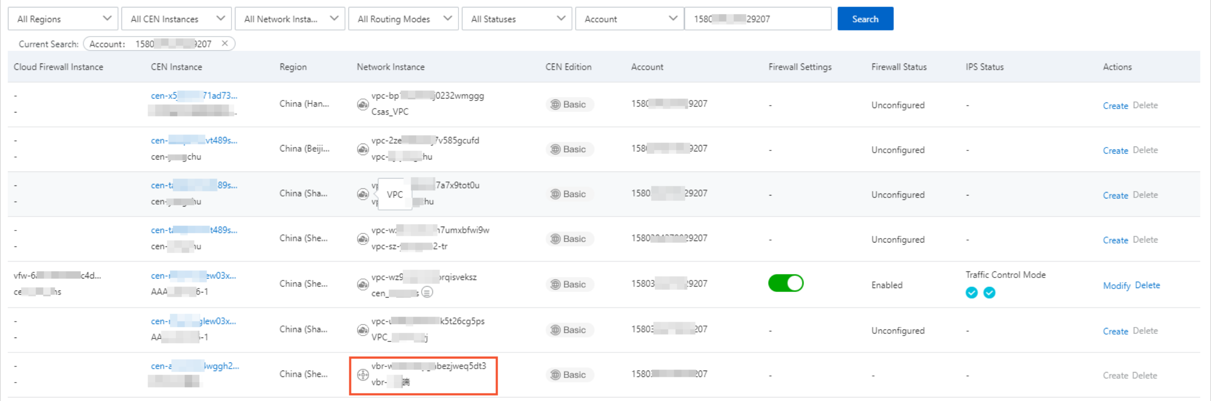


Instance ID/Name	VPC Instance	Peer VPC Instance	Bandwidth	Firewall Settings	Firewall Status	IPS Status	Actions
[redacted]	[redacted]oj5jl	[redacted]3gtqs	100Mbps	●	Enabled	Monitoring Mode ✓ ✓	Modify Delete

Use a VPC firewall to protect traffic between a VPC and a data center

A VPC firewall can protect traffic between a VPC and a data center that are connected by a VBR. If a VPC and a data center are connected by the VBR of a CEN instance, traffic between the VPC and the data center is automatically protected after you enable the VPC firewall created for the CEN instance. You do not need to create or enable a VPC firewall for the VBR.

You can perform the following operations to view the protection details of the VBR: Log on to the , go to the **Firewall Settings** page, and then click the **VPC Firewall** tab. On the **CEN** tab of the tab that appears, view the details about the VBR.



Account: 1580[redacted]29207

Current Search: Account: 1580[redacted]9207

Cloud Firewall Instance	CEN Instance	Region	Network Instance	CEN Edition	Account	Firewall Settings	Firewall Status	IPS Status	Actions
- -	cen-x5[redacted]71ad73... [redacted]	China (Han...	vpc-bp[redacted]j0232wmggg Csas_VPC	Basic	1580[redacted]9207	-	Unconfigured	-	Create Delete
- -	cen-[redacted]vt489s... cen-[redacted]chu	China (Beiji...	vpc-2ze[redacted]7v585gcufd vpc-[redacted]hu	Basic	158[redacted]9207	-	Unconfigured	-	Create Delete
- -	cen-t[redacted]89s... cen-[redacted]hu	China (Sha...	v[redacted]7a7x9tot0u v[redacted]hu	Basic	1580[redacted]29207	-	Unconfigured	-	Create Delete
- -	cen-t[redacted]t489s... cen-[redacted]u	China (She...	vpc-w[redacted]7umxbfwi9w vpc-sz-[redacted]2-tr	Basic	1580[redacted]29207	-	Unconfigured	-	Create Delete
vfw-6[redacted]c4d... ce[redacted]hs	cen-[redacted]ew03x... AAA[redacted]6-1	China (She...	vpc-wz9[redacted]orqisveksz cen_[redacted]s	Basic	15803[redacted]9207	●	Enabled	Traffic Control Mode ✓ ✓	Modify Delete
- -	cen-[redacted]glew03x... AA[redacted]-1	China (Sha...	vpc-[redacted]k5t26cg5ps VPC_[redacted]j	Basic	15803[redacted]207	-	Unconfigured	-	Create Delete
- -	cen-[redacted]wggh2... [redacted]	China (She...	vbr-w[redacted]bezjweq5dt3 vbr-[redacted]端	Basic	1580[redacted]207	-	-	-	Create Delete

What's next

After a VPC firewall is created, you can perform the following operations:

- On the **VPC Firewall** tab, click **Modify** or **Delete** in the Actions column to modify or delete an existing VPC firewall.
- On the **VPC Firewall** tab, enable or disable the VPC firewall. For more information, see Enable or disable VPC Firewall.
- In the left-side navigation pane, choose **Access Control > Access Control**. On the Access Control page, click the VPC Firewall tab. On the VPC Firewall tab, configure VPC firewall policies to manage traffic between VPCs. For more information, see Create an access control policy for a VPC firewall.

After a VPC firewall is enabled, VPC access traffic is collected and analyzed. You can view the statistics and analysis results on the VPC Access page. To go to the VPC Access page, choose **Traffic Analysis > VPC Access** in the left-side navigation pane. For more information, see VPC access.

2.3. Enable or disable VPC Firewall

The VPC Firewall feature can detect and collect statistics on traffic between connected VPCs. This feature helps you detect attacks and perform troubleshooting. You can enable or disable this feature in the Cloud Firewall console.

Prerequisites

A VPC firewall is created. For more information, see Create a VPC firewall.

Context

After the VPC Firewall feature is enabled, you can log on to the Cloud Firewall console and choose **Traffic Analysis > VPC Access** in the left-side navigation pane to view information about traffic between VPCs.

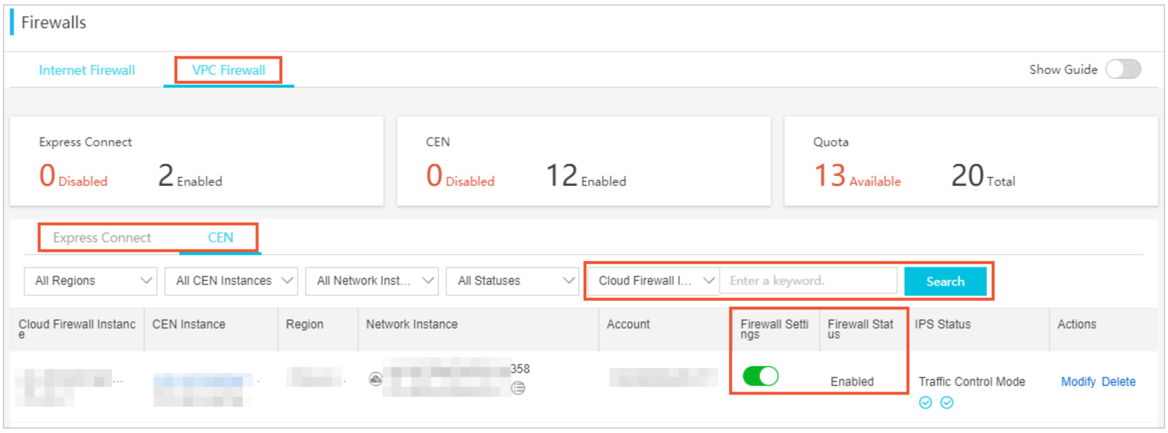
After the VPC Firewall feature is enabled, a security group named Cloud_Firewall_Security_Group and an allow policy appear on the **Security Groups** page of the ECS console. The allow policy is also referred to as an **authorization policy**, which is used to allow inbound traffic from the VPC firewall to ECS instances. To go to the Security Groups page, log on to the ECS console and click **Network & Security** in the left-side navigation pane.

> **Note** Do not delete the security group Cloud_Firewall_Security_Group and the allow policy. Otherwise, the inbound traffic from the VPC firewall to ECS instances cannot be protected by the VPC firewall.

Procedure

1.
2.
3. On the **Firewall Settings** page, click the **VPC Firewall** tab.
4. On the **VPC Firewall** tab, click the **Express Connect** or **CEN** tab based on your VPC connection type.
5. Find the target Cloud Firewall instance and turn on or turn off **Firewall Settings**.

   If a large number of Cloud Firewall instances exist, we recommend that you use the filter or search function to find the target Cloud Firewall or VPC instance.

6. Wait for a few seconds until the VPC Firewall feature is enabled or disabled.

Result

- After you turn on Firewall Settings, **Firewall Status** becomes **Enabling**. If Firewall Status becomes **Enabled**, the VPC Firewall feature is enabled.
- After you turn off Firewall Settings, **Firewall Status** becomes **Disabling**. If Firewall Status becomes **Disabled**, the VPC Firewall feature is disabled.

What's next

After the VPC Firewall feature is enabled, traffic between VPCs is collected and analyzed. You can view the statistics and analysis results on the VPC Access page. To go to the VPC Access page, choose **Traffic Analysis > VPC Access** in the left-side navigation pane of the Cloud Firewall console. For more information about VPC access traffic, see VPC access.

2.4. Protect traffic between VPCs connected by using a CEN transit router

If you use a Cloud Enterprise Network (CEN) transit router, you must configure routing between the CEN transit router and a virtual private cloud (VPC) firewall before you can use the VPC firewall to protect the traffic between VPCs that are connected by using the CEN transit router. In this topic, a transit router of the Enterprise Edition is used. This topic describes how to configure routing between a CEN transit router and a VPC firewall.

Prerequisites

1. A CEN instance is created in the CEN console. Two VPCs are created. In this topic, `VPC-01` and `VPC-02` are used.

   For more information, see Create a CEN instance.
2. A VPC is created in the VPC console. In the following procedure, you must create a VPC firewall for the VPC. In this topic, `Cfw-TR-manual-VPC` is used. In addition, three vSwitches are created for the VPC. In this topic, `TR-Vswitch-01` , `TR-VSwitch-02` , and `Cfw-Vswitch` are used. TR-Vswitch-01 and TR-VSwitch-02 are used by a transit router to connect network instances. Cfw-Vswitch is used when you create a VPC firewall.
3. The ID of `Cfw-TR-manual-VPC` is added to the required whitelist before you can create a VPC firewall for `Cfw-TR-manual-VPC` . To add the ID of Cfw-TR-manual-VPC to the required whitelist, contact after-sales support engineers in the DingTalk group.

Usage notes

Cloud Firewall can protect the traffic between network instances that are connected by using CEN transit routers. The network instances refer to VPCs, virtual border routers (VBRs), and Cloud Connect Networks (CCNs).

If you want to protect the traffic between VPCs in the same region, you can follow the procedure in this topic.

> **Notice** If you want to use the feature, contact after-sales support engineers in the DingTalk group to add the ID of Cfw-TR-manual-VPC to the required whitelist. If the ID of Cfw-TR-manual-VPC is not added to the required whitelist, the Create button is dimmed on the **VPC Firewall** tab. The system prompts you to add the ID of Cfw-TR-manual-VPC to the required whitelist.

Step 1: Connect Cfw-TR-manual-VPC to a transit router

This step establishes a connection between `Cfw-TR-manual-VPC` and the transit router.

1.
2. On the **Instances** page, find the CEN instance whose traffic you want to redirect to a VPC firewall and click the ID of the instance.
3. On the **Basic Settings** tab, click **Create Connection** in the **Actions** column or click the ⊕ icon to the right of VPC in the upper part of the tab.
4. On the **Connection with Peer Network Instance** page, configure the parameters. `Cfw-TR-manual-VPC`

   The following table describes the important parameters.

Parameter	Description
Instance Type	The type of the network instance that you want to connect to the CEN instance. In this example, select VPC.
Region	The region where the network instance resides. Set this parameter to the region that you specify when you create `Cfw-TR-manual-VPC`.
Networks	The network instance that you want to connect to the CEN instance. In this example, select the ID of `Cfw-TR-manual-VPC`.
VSwitch	The vSwitches that can be bound to the network instance. In this example, select `TR-Vswitch-01` for **Primary Zone** and `TR-Vswitch-02` for **Secondary Zone**.

   For more information about other parameters, see Use an Enterprise Edition transit router to create VPC connections.

Step 2: Connect VPC-01 and VPC-02 to the transit router

You must establish a connection between `VPC-01` and the transit router and a connection between `VPC-02` and the transit router. This way, both VPCs are connected to the CEN instance.

For more information, see Use an Enterprise Edition transit router to create VPC connections.

Step 3: Create a VPC firewall

This step creates a VPC firewall for `Cfw-TR-manual-VPC`.

To create a VPC firewall, log on to the Cloud Firewall console, choose **Firewall Settings > Firewall Settings**, and then click **VPC Firewall**. On the VPC Firewall tab, click the **CEN** tab, find `Cfw-TR-manual-VPC`, and then click **Create** in the **Actions** column. In the Create VPC Firewall dialog box, select **Manual** for **Routing Mode**, `Cfw-TR-manual-VPC` for **VPC**, and `Cfw-Vswitch` for vSwitch. For more information, see Create a VPC firewall for a CEN instance.

> ⓘ **Note** After this step is complete, an elastic network interface (ENI) is created. To view the ENI, log on to the ECS console and choose **Network & Security > ENIs**. By default, an ENI named cfw-bonding-eni is created.

Step 4: Create routes for VPC-01 and VPC-02

This step creates routes between the CEN instance and the VPC firewall.

1.
2. On the **Instances** page, find the CEN instance whose traffic you want to redirect to the VPC firewall and click the ID of the instance.
3. On the Transit Router tab, click the number in the **Route Table** column. The **Route Table** tab appears.
4. On the **Route Table** tab, click **Create Route Table** at the top of the left-side route table list.
5. In the **Create Route Table** dialog box, configure the parameters.

   Retain the default value for **Transit Router**. Set the Name parameter to `Cfw-TR-RouteTable`.

   You can add routes to the `Cfw-TR-RouteTable` route table to forward the traffic from `VPC-01` or `VPC-02` to `Cfw-TR-manual-VPC`.
6. Click the `Cfw-TR-RouteTable` route table. Then, click **Add Route Entry**.
7. In the **Add Route Entry** dialog box, configure the parameters.

   Parameter description:

   - **Destination CIDR**: Retain the default value `0.0. 0.0/0`
   - **Blackhole Route**: Retain the default value `No`.
   - **Next Hop**: Select `Cfw-TR-manual-VPC`.

   After you add the route, traffic is forwarded to the VPC firewall based on the `Cfw-TR-RouteTable` route table.
8. On the **Route Table** tab, click the system route table in the left-side route table list. In the **Route Table Details** section, click the **Route Table Association** tab.
9. On the **Route Table Association** tab, delete the association created for `VPC-01` and `VPC-02`.
10. On the **Route Table** tab, click the `Cfw-TR-RouteTable` route table in the left-side route table list.
11. In the **Route Table Details** section, click the **Route Table Association** tab and click **Create Association**.
12. In the **Add Association** dialog box, select `VPC-01` and `VPC-02` for **Association** and click **OK**.

    After the association is created, the traffic between the two VPCs is forwarded to the `Cfw-TR-RouteTable` route table.

13. On the **Route Table** tab, click the system route table in the left-side route table list.
14. In the **Route Table Details** section, click the **Route Propagation** tab
15. On the **Route Propagation** tab, enable route propagation for VPC-01 and VPC-02. To enable Route Propagation for VPC-01, select `VPC-01` for **Association**. To enable route propagation for VPC-02, select `VPC-02` for Association.

    After route propagation is enabled, the routes created for `VPC-01` and `VPC-02` are automatically propagated to the system route table.

    After route propagation is enabled, you can view the information about the automatically propagated routes on the **Route Entry** tab.
16. Click the system route table in the left-side route table list. In the **Route Table Details** section, click the **Route Table Association** tab.
17. On the **Route Table Association** tab, click **Create Association**.
18. In the **Add Association** dialog box, select `Cfw-TR-manual-VPC` for Association.

After the step is complete, the routes between the CEN instance and the VPC firewall are created, and traffic can be forwarded to Cfw-TR-manual-VPC.

Step 5: Configure route tables for the VPC firewall

This step redirects the traffic from Cfw-TR-manual-VPC to the VPC firewall.

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Route Tables**. On the Route Tables page, click Create Route Table. On the Create Route Table page, select `Cfw-TR-manual-VPC` for **VPC** and set the Name parameter to `VPC-CFW-RouteTable`.
3. Click the name of the `VPC-CFW-RouteTable` route table. On the page that appears, click the **Associated vSwitch** tab.
4. Click **Associate vSwitch**. In the Associate vSwitch dialog box, select `Cfw-Vswitch` for vSwitch.
5. On the **Route Entry List** tab, click the **Custom Route** tab.
6. Click **Add Route Entry**. In the Add Route Entry panel, configure the parameters.

    Parameter description:

    - **Destination CIDR Block**: Specify `0.0.0.0/0`.
    - **Next Hop Type**: Select `Forwarding Router`.
    - **Forwarding Router**: Retain the default value Cfw-TR-manual-VPC.

    After this operation is complete, the outbound traffic of the VPC firewall is forwarded to the CEN transit router.
7. On the Route Tables page, click the name of the system route table that is created for `Cfw-TR-manual-VPC`.
8. On the page that appears, click the **Route Entry List** tab and then click the **Custom Route** tab.
9. Click **Add Route Entry**. In the Add Route Entry panel, configure the parameters.

    Parameter description:

    - **Destination CIDR Block**: Specify 0.0.0.0/0.
    - **Next Hop Type**: Select Secondary ENI.

- **Secondary ENI**: Select Cfw-bonding-eni.

10. On the **Custom** tab, delete other route entries. To delete a route entry, click **Delete** in the **Actions** column.

    After the step is complete, the traffic from Cfw-TR-manual-VPC is redirected to the VPC firewall.

Step 6: Check whether the forwarding configuration is successful

You can go to the Traffic Logs tab of the Log Audit page to check whether the traffic logs of the CEN instance are recorded. If the traffic logs are recorded, the forwarding configuration is successful. For more information, see Traffic logs.

2.5. Protect a specific amount of traffic between VPCs connected by using a CEN transit router

If you use a Cloud Enterprise Network (CEN) transit router, you must manually configure routing between the CEN transit router and a virtual private cloud (VPC) firewall before you can use the VPC firewall to protect traffic between VPCs and virtual border routers (VBRs) that are connected by using the CEN transit router. This topic describes how to configure routing between a CEN transit router and a VPC firewall.

Prerequisites

1. A CEN instance is created in the CEN console. Three VPCs are created. In this topic, **VPC1**, **VPC2**, and **DMZ VPC** are used. Two VBRs are created. In this topic, **IDC-1** and **IDC-2** are used.

   For more information, see Create a CEN instance.

2. A VPC is created in the VPC console for a VPC firewall. In this topic, **FW VPC** is used. In addition, three vSwitches are created for the VPC. In this topic, **TR-Vswitch-01**, **TR-VSwitch-02**, and **Cfw-Vswitch** are used. TR-Vswitch-01 and TR-VSwitch-02 are used by a transit router to connect network instances. Cfw-Vswitch is used when you create the VPC firewall.
3. The ID of **FW VPC** is added to the required whitelist before you can create a VPC firewall for **FW VPC**. To add the ID of FW VPC to the required whitelist, you must contact after-sales support engineers in the DingTalk group of Cloud Firewall.

   > **Notice** If you want to use the feature, contact the after-sales support engineers to add the ID of FW VPC to the whitelist. If the ID of FW VPC is not added to the whitelist, the Create button is dimmed on the **VPC Firewall** tab of the Cloud Firewall console. The system prompts you to add the ID of FW VPC to the whitelist.

In this topic, the traffic between other VPCs and each of the following network instances is protected by Cloud Firewall: **VPC1**, **IDC-1**, **IDC-2**. The traffic between **VPC2** and **DMZ VPC** is not protected by Cloud Firewall. The traffic from any VPC, IDC-1, or IDC-2 to the default route 0.0.0.0/0 is not protected by Cloud Firewall.

Application scope

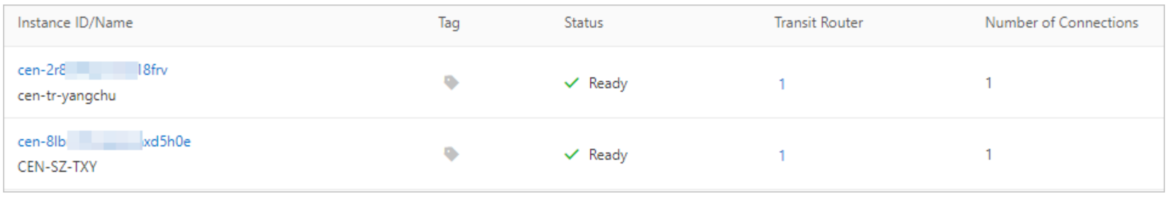
Cloud Firewall can protect the traffic between network instances that are connected by using CEN transit routers. The network instances include VPCs, VBRs, and Cloud Connect Network (CCN) instances.

If you want to protect the traffic between VPCs in the same region, you can follow the procedure in this topic.

Step 1: Connect FW VPC to a transit router

This step establishes a connection between **FW VPC** and the transit router.

1.
2. On the **Instances** page, find the CEN instance whose traffic you want to redirect to a VPC firewall and click the ID of the instance.



Instance ID/Name	Tag	Status	Transit Router	Number of Connections
cen-2r[redacted]18frv cen-tr-yangchu	🏷	✓ Ready	1	1
cen-8lb[redacted]xd5h0e CEN-SZ-TXY	🏷	✓ Ready	1	1

3. On the **Basic Settings** tab, click **Create Connection** in the **Actions** column or click the ⊕ icon to the right of VPC in the upper part of the tab.
4. On the **Connection with Peer Network Instance** page, configure the parameters.

   The following table describes the important parameters.

Parameter	Description
Network Type	The type of the network instance that you want to connect to the CEN instance. Select **VPC**.
Region	The region in which the network instance resides. Set this parameter to the region that you specify when you create **FW VPC**.
Networks	The network instance that you want to connect to the CEN instance. Select the ID of **FW VPC**.
VSwitch	The vSwitches that can be bound to the network instance. Select **TR-Vswitch-01** for the primary vSwitch and **TR-VSwitch-02** for the secondary vSwitch.

   For more information about other parameters, see Use an Enterprise Edition transit router to create VPC connections.

Step 2: Connect the VPCs and VBRs to the transit router

You must separately establish a connection between the transit router and each of the following network instances: **VPC1**, **VPC2**, **DMZ VPC**, **IDC-1**, and **IDC-2**. This way, the VPCs and VBRs are connected to the CEN instance.

For more information, see Use an Enterprise Edition transit router to create VPC connections.

Step 3: Create a VPC firewall

This step creates a VPC firewall for **FW VPC**.

To create a VPC firewall, log on to the Cloud Firewall console, go to the **Firewall Settings** page, and then click the **VPC Firewall** tab. On the VPC Firewall tab, click the **CEN** tab, find **FW VPC**, and then click **Create** in the **Actions** column. In the Create VPC Firewall dialog box, select **Manual** for **Routing Mode**, **FW VPC** for **VPC**, and **Cfw-Vswitch** for **vSwitch**.

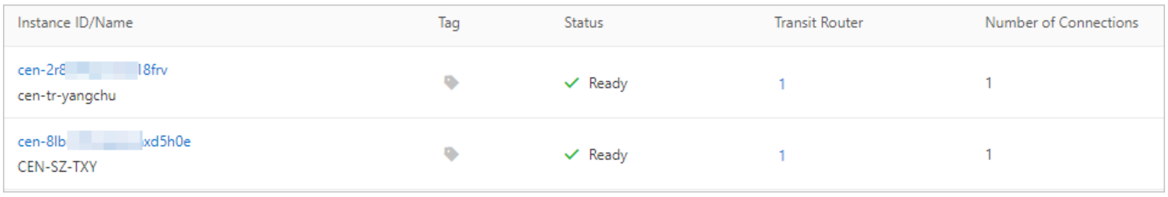
For more information, see Create a VPC firewall for a CEN instance.

> **Note** After this step is complete, an elastic network interface (ENI) is created. To view the ENI, log on to the ECS console and choose **Network & Security > ENIs**. By default, an ENI named cfw-bonding-eni is created.

Step 4: Create routes for VPC1, VPC2, and DMZ VPC

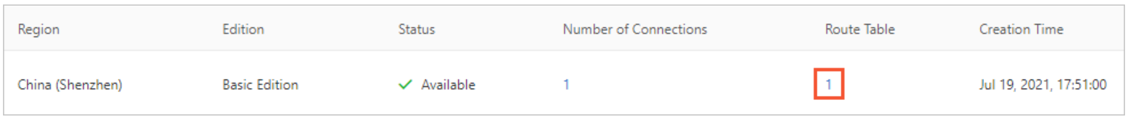
This step creates routes between the CEN instance and the VPC firewall.

1.
2. On the **Instances** page, find the CEN instance whose traffic you want to redirect to the VPC firewall and click the ID of the instance.



Instance ID/Name	Tag	Status	Transit Router	Number of Connections
cen-2r[redacted]l8frv cen-tr-yangchu		✓ Ready	1	1
cen-8lb[redacted]xd5h0e CEN-SZ-TXY		✓ Ready	1	1

3. On the **Transit Router** tab, click the number in the **Route Table** column.



Region	Edition	Status	Number of Connections	Route Table	Creation Time
China (Shenzhen)	Basic Edition	✓ Available	1	1	Jul 19, 2021, 17:51:00

4. Create route tables named **Cfw-Untrust-RouteTable** and **Cfw-Trust-RouteTable**.
   i. On the **Route Table** tab, click **Create Route Table**.
   ii. In the **Create Route Table** dialog box, configure the parameters for the **Cfw-Untrust-RouteTable** and **Cfw-Trust-RouteTable** route tables.

      Transit Router: Retain the default value.

      > **Note**
      > - You can add routes to the **Cfw-Untrust-RouteTable** route table to forward traffic from **VPC1**, **IDC-1**, and **IDC-2** to **FW VPC**.
      > - You can add routes to the **Cfw-Trust-RouteTable** route table to forward traffic from **FW VPC** to **VPC1**, **VPC2**, **DMZ VPC**, **IDC-1**, or **IDC-2**.

5. Configure the **Cfw-Trust-RouteTable** route table.

   The routes added to **VPC1**, **VPC2**, **DMZ VPC**, **IDC-1**, and **IDC-2** are automatically propagated to the **Cfw-Trust-RouteTable** route table. The traffic from **FW VPC** is forwarded to the **Cfw-Trust-RouteTable** route table.

   i. Click the **Cfw-Trust-RouteTable** route table that you create. In the right-side section, click the **Route Propagation** tab.
   ii. On the **Route Propagation** tab, click **Enable Route Propagation**.

iii. In the **Enable Route Propagation** dialog box, select **VPC1**, **VPC2**, **DMZ VPC**, **IDC-1**, and **IDC-2** for Attachment. Then, click **OK**.
After route propagation is enabled, you can view the information about the automatically propagated routes on the **Route Entry** tab.

iv. On the **Route Table** tab, click the system route table in the left-side route table list. In the **Route Table Details** section, click the **Route Table Association** tab.

v. On the **Route Table Association** tab, delete the association created for **FW VPC**.

vi. Click the **Cfw-Trust-RouteTable** route table that you create. On the **Route Table Association** tab, click **Create Association**.

vii. In the **Add Association** dialog box, select **FW VPC** for **Association**. Then, click **OK**.

6. Configure the **Cfw-Untrust-RouteTable** route table.

   After configuration, traffic is forwarded to the VPC firewall based on the **Cfw-Untrust-RouteTable** route table.

   i. Click the **Cfw-Untrust-RouteTable** route table that you create. In the right-side section, click the **Route Entry** tab.

   ii. On the **Route Entry** tab, click **Add Route Entry**.

   iii. In the **Add Route Entry** dialog box, configure the parameters.

   Parameter description:

   - **Destination CIDR**: Retain the default value **10.0.0.0/8**.
   - **Blackhole Route**: Retain the default value **No**.
   - **Next Hop**: Select **FW VPC**.

   iv. Repeat the preceding steps to add the following routes:

   - The route whose Destination CIDR is **172.16.0.0/12** and Next Hop is **FW VPC**.
   - The route whose Destination CIDR is **192.168.0.0/16** and Next Hop is **FW VPC**.
   - The route whose Destination CIDR is **61.20.0.0/16** and Next Hop is **FW VPC**.
   - The route whose Destination CIDR is **0.0.0.0/0** and Next Hop is **DMZ VPC**.

7. Configure the system route table.

   i. On the **Route Table** tab, click the system route table in the left-side route table list. In the right-side section, click the **Route Propagation** tab.

   ii. On the **Route Propagation** tab, delete the routes that are propagated for **VPC1**, **IDC-1**, **FW VPC**, and **IDC-2**.
   After this operation is complete, only the routes created for **VPC2** and **DMZ VPC** are propagated to the system route table. You can view the information about the automatically propagated routes on the Route Entry tab.

   iii. On the **Route Entry** tab, click **Add Route Entry**.

   iv. In the **Add Route Entry** dialog box, add the following routes:

   - The route whose Destination CIDR is **10.0.0.0/24** (**VPC1**) and Next Hop is **FW VPC**.
   - The route whose Destination CIDR is **172.16.0.0/12** (**IDC-1**) and Next Hop is **FW VPC**.
   - The route whose Destination CIDR is **61.20.0.0/16** (**IDC-2**) and Next Hop is **FW VPC**.

   v. On the **Route Table Association** tab, delete the associations whose Next Hop is set to **VPC1**, **IDC-1**, and **IDC-2**.

8. Configure the **Cfw-Untrust-RouteTable** route table.

   After the configuration, the traffic from **VPC1**, **IDC-1**, and **IDC-2** is forwarded to the **Cfw-Untrust-RouteTable** route table.

   i. Click the **Cfw-Untrust-RouteTable** route table that you create. In the right-side section, click the **Route Table Association** tab.

   ii. On the **Route Table Association** tab, click **Create Association**.

   iii. In the **Add Association** dialog box, select **VPC1**, **IDC-1**, and **IDC-2** for **Association**. Click **OK**.

After the step is complete, the routes between the CEN instance and the VPC firewall are created, and traffic can be forwarded to FW VPC.

Step 5: Configure route tables for the VPC firewall

This step forwards the traffic from FW VPC to the VPC firewall.

1. Log on to the VPC console. In the left-side navigation pane, click **Route Tables**.
2. On the **Route Tables** page, click **Create Route Table**. Select **FW VPC** for **VPC** and set the Name parameter to **VPC-CFW-RouteTable**. Click **OK**.
3. Click the name of the **VPC-CFW-RouteTable** route table. On the **Associated vSwitch** tab, click **Associate vSwitch**. Select **Cfw-Vswitch** for **vSwitch**. Click **OK**.
4. On the **Custom Route** tab of the **Route Entry List** tab, click **Add Route Entry** and configure the parameters.

   Parameter description:

   - **Destination CIDR Block**: Specify `0.0.0.0/0`.
   - **Next Hop Type**: Specify `Transit Router`.
   - **Transit Router**: Retain the default value FW VPC.

   After this operation is complete, the outbound traffic of the VPC firewall is forwarded to the CEN transit router.
5. On the Route Tables page, click the name of the system route table that is created for **FW VPC**.
6. On the page that appears, click the **Route Entry List** tab and click the **Custom Route** tab.
7. Click **Add Route Entry**. In the Add Route Entry panel, configure the parameters.

   Parameter description:

   - **Destination CIDR Block**: Specify 0.0.0.0/0.
   - **Next Hop Type**: Select Secondary ENI.
   - **Secondary ENI**: Select **Cfw-bonding-eni**.
8. On the **Custom Route** tab, delete other routes. To delete a route, click **Delete** in the **Actions** column.

   After the step is complete, the traffic from FW VPC is redirected to the VPC firewall.

Step 6: Check whether the forwarding configuration is successful

You can check whether the traffic logs of the CEN instance are displayed on the Traffic Logs tab. If the traffic logs are recorded, the forwarding configuration is successful. Examples:

- **VPC1** and **VPC2** can communicate with each other, and traffic logs are recorded.

- **VPC2** and **DMZ VPC** can communicate with each other, but no traffic logs are recorded.

For more information, see Traffic logs.