ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall

Firewall Settings

Document Version: 20200929

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.Enable or disable Internet Firewall

The Internet Firewall feature allows you to detect traffic between the Internet and public IP addresses in Alibaba Cloud. After Cloud Firewall is activated, you can enable or disable this feature for specific public IP addresses under your Alibaba Cloud account. After you enable Internet Firewall for your IP address, you can use Cloud Firewall to analyze and control the traffic between the Internet and on-cloud hosts.

Prerequisites

The public IP address quota does not exceed the threshold. The public IP address quota refers to the maximum number of public IP addresses that the Internet firewall can protect. Different Cloud Firewall editions have different public IP address quotas. For more information, see Features. You can increase the bandwidth of Cloud Firewall to increase the quota. For more information, see Renewal and upgrade.

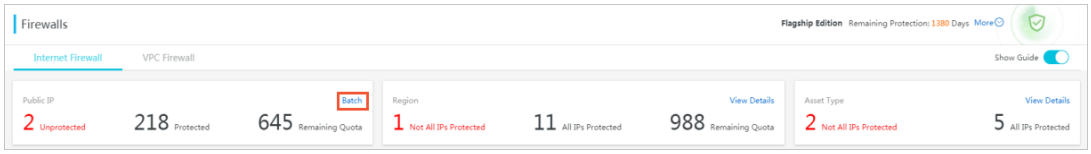
Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, click **Firewall Settings**.
3. On the **Internet Firewall** tab, enable or disable Internet Firewall for specific public IP addresses. You can enable or disable this feature for individual public IP addresses, or for all public IP addresses under the current Alibaba Cloud account with one click.

   > **Note** By default, Internet Firewall is disabled for all IP addresses after Cloud Firewall is activated. We recommend that you enable this feature for all IP addresses. After it is enabled, traffic passes through the Internet firewall. However, the default action of access control policies is **Allow**, so your business is not affected.

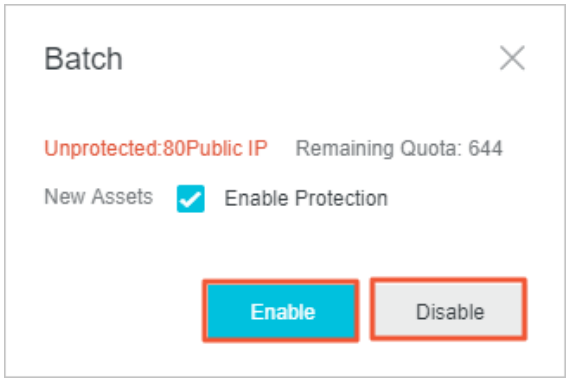
   You can perform the following operations on the **Internet Firewall** tab to enable or disable Internet Firewall.

   - To enable or disable Internet Firewall for all public IP addresses, follow these steps:
     a. In the **Public IP** section, click **Batch**.



b. In the **Batch** dialog box, click **Enable** or **Disable**.

You can also select **Enable Protection** next to **New Assets** and click Enable. Then, Internet Firewall is enabled for new public IP addresses added under the current Alibaba Cloud account by default.

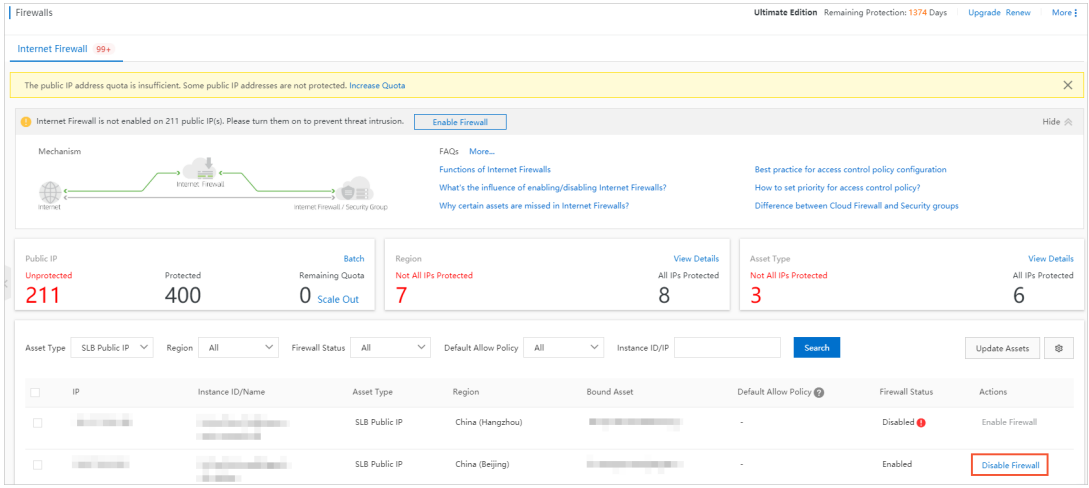


- To enable or disable Internet Firewall for one or more public IP addresses, follow these steps:

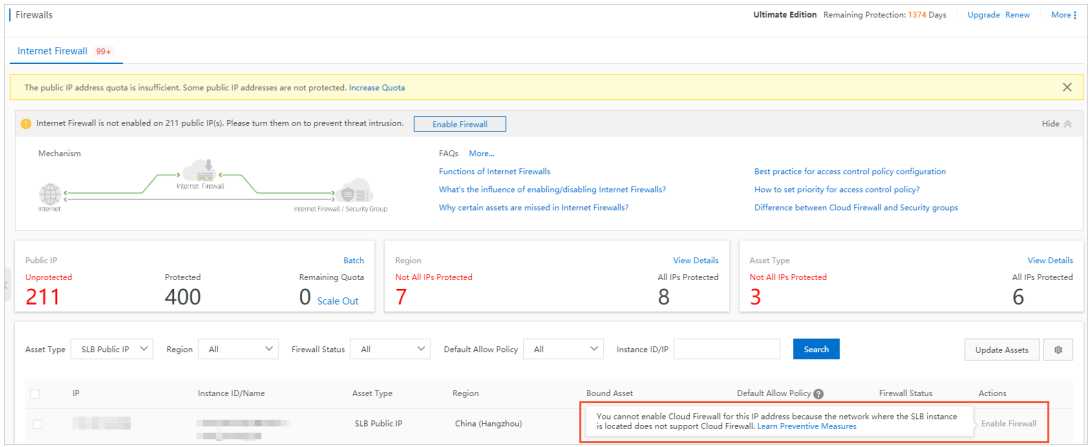
a. In the IP address list at the lower section of the page, find the target public IP addresses.

You can filter the target IP addresses by using **Asset Type**, **Region**, and **Firewall Status**. Alternatively, you can search for the target IP addresses by using **Instance ID/IP**.

b. Select the target IP addresses and click **Enable Firewall** or **Disable Firewall** at the lower section of the page. Alternatively, find the target IP address and click **Enable Firewall** or **Disable Firewall** in the Actions column.



Due to the network restrictions, Internet Firewall cannot be enabled for some public IP addresses of SLB instances. For such IP addresses, the Enable Firewall button is dimmed. When you move your pointer over this button, a message **"You cannot enable Cloud Firewall for this IP address because the network where the SLB instance is located does not support Cloud Firewall."** appears. We recommend that you use another security service, such as Web Application Firewall, to protect these public IP addresses.



Result

After you enable Internet Firewall, wait until **Firewall Status** becomes **Enabled**, which indicates that this feature has been enabled. After you disable Internet Firewall, wait until Firewall Status becomes **Disabled**, which indicates that this feature has been disabled. It may take several seconds for the firewall status to be updated.

What's next

- Traffic analysis overview
- Outbound and inbound traffic control on the Internet firewall

Related information

- Functions of Internet Firewalls
- Why certain assets are missing in Internet Firewalls?
- What are the impacts of disabling the Internet firewall?
- Why certain assets are missing in Internet Firewalls?

2.VPC Firewall

2.1. VPC firewall limits

This topic describes the limits of VPC firewalls.

Item	Description	Handling suggestion
Number of VPCs that can be protected by VPC firewalls in a Cloud Enterprise Network (CEN)	For VPCs that are deployed in the same region, the default number is six and the maximum number is 20.	N/A
VPC custom routes	The number of custom routes increases after you enable VPC Firewall. If the number of custom routes in your VPC route table reaches the upper limit, you cannot enable VPC Firewall. For more information, see Add a custom route entry.	Increase the VPC quota. You can log on to the VPC console, open the **Quota Management** page, and increase the maximum number of custom routes allowed for each route table under your Alibaba Cloud account. **Note** Do not modify or delete custom routes that are added by Cloud Firewall. Otherwise, VPC firewalls cannot protect inbound traffic to ECS instances.
Subnet mask length	VPC firewall users in a CEN cannot publish routes to a network with a 32-bit subnet mask. If such routes are published and VPC Firewall is enabled, the connections to this network are interrupted.	We recommend that you change the subnet mask length to less than or equal to 30 bits before you enable VPC Firewall.
Total number of VPCs and regions for which VPC Firewall is enabled	Less than or equal to 32.	N/A

Item	Description	Handling suggestion
Cross-account VPCs in a CEN	If two VPCs in a CEN are created by different Alibaba Cloud accounts, Cloud Firewall must be authorized to access both VPCs. Otherwise, VPC Firewall cannot be enabled for the CEN.	Before you enable VPC Firewall, you must use the Alibaba Cloud accounts to separately log on to the Cloud Firewall console and complete the authorization. For more information, see Create a VPC firewall for a CEN.
Cross-region VPCs in a CEN	Make ensure that VPC Firewall is available in all the regions in the CEN. Otherwise, VPC Firewall cannot be enabled for the CEN.	N/A
VPC quantity	Each region can have up to 20 VPCs. A VPC that is added by Cloud Firewall consumes this quota. After VPC Firewall is enabled, Cloud Firewall adds a VPC for each region involved. You can log on to the VPC console and open the **VPCs** page. The VPCs named "Cloud_Firewall_VPC" are added by Cloud Firewall. If a region already has 20 VPCs, VPC Firewall cannot be enabled for this region.	If the VPC quota is used up, log on to the VPC console and open the **Quota Management** page to increase the VPC quota. If the VPC quota has reached the upper limit, submit a ticket.
Mutual access between Virtual Border Routers (VBRs)	Mutual access traffic of VBRs does not pass Cloud Firewall.	N/A
Mutual access between Cloud Connect Networks (CCNs)	Mutual access traffic of CCNs does not pass Cloud Firewall.	N/A
Brief disconnection occurred when VPC Firewall is enabled or disabled	When VPC Firewall is enabled or disabled for Server Load Balancer (SLB) or database services such as ApsaraDB for RDS, the persistent connections fail.	You can configure the keep-connection-alive and reconnection mechanisms on the client.
East-west traffic protection only	VPC firewalls can only protect east-west traffic, but cannot protect the traffic from the default route 0.0.0.0/0 to the Internet.	N/A

2.2. Create a VPC firewall

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

Prerequisites

You have purchased a CEN or Express Connect instance, and have connected two VPCs by using the instance. For more information, see Interconnect two VPCs under the same account.

Context

The VPC Firewall feature is available in Cloud Firewall Enterprise and Ultimate Editions. A VPC firewall can be created only between two VPCs that are connected by using an Express Connect or a CEN.

Create a VPC firewall for a CEN

Cloud Firewall of the **Ultimate Edition** can be used to protect VPCs that are connected by using a CEN and are created by using different Alibaba Cloud accounts. If you want to enable VPC Firewall for such VPCs, Cloud Firewall must be authorized to access the cloud assets under both accounts. Otherwise, you cannot create a VPC firewall for the CEN, and the message **It is not allowed to be created because of the existing unauthorized network instance** is displayed on the **CEN** tab. To go to this tab, log on to the Cloud Firewall console, click **Firewall Settings** in the left-side navigation pane, click the **VPC Firewall** tab, and then click the **CEN** tab.

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

1. Log on to the Cloud Firewall console by using the account.
2. On the welcome page of Cloud Firewall, get started as instructed.
3. On the **Cloud Resource Access Authorization** page, click **Confirm Authorization Policy**.

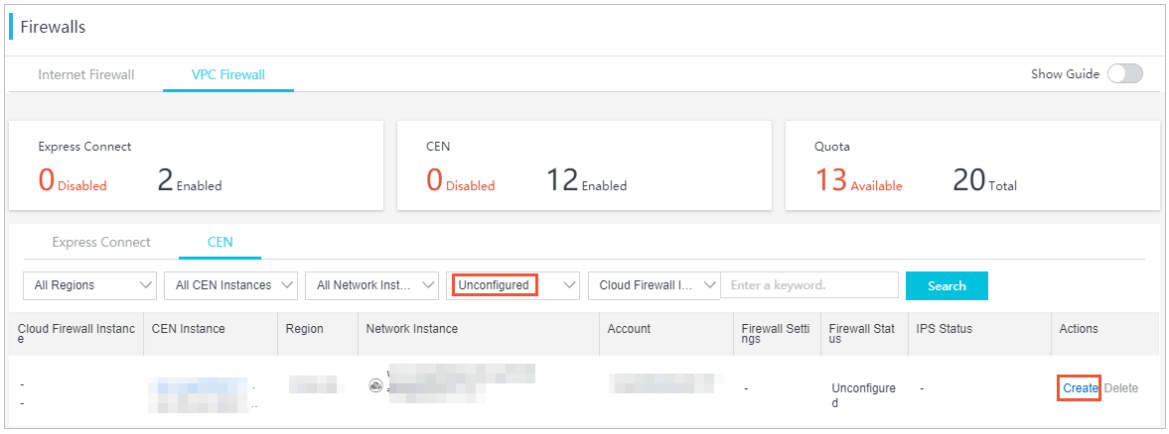
> **Note** If you want to enable VPC Firewall for a CEN, note the following items:
>
> - VPC firewalls can be used to protect VPCs that are deployed in different regions or created by different Alibaba Cloud accounts. If your VPC is connected with a VPC that is created by another Alibaba Cloud account, you can enable VPC Firewall to protect these VPCs even if Cloud Firewall Premium, Enterprise, or Ultimate Edition is not enabled for the VPC that is created by another Alibaba Cloud account.
> - VPC Firewall can be enabled for a maximum of 10 VPCs in a region of a CEN. If you want to increase the quota, submit a ticket.
> - VPC firewalls can protect traffic between VPCs, between a VPC and a Virtual Border Router (VBR), and between a VPC and a Cloud Connect Network (CCN), but cannot protect traffic between VBRs, between CCNs, or between a CCN and a VBR.

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

> **Note** When you create, enable, disable, or delete a VPC firewall, the system automatically modifies custom routes in your VPC route table, causing a short network interruption. If you need to perform batch operations on VPC firewalls or frequently enable and disable VPC firewalls, we recommend that you perform such operations during off-peak hours to prevent the impact on your business.

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, click **Firewall Settings**.

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.If a large number of CEN instances exist, you can filter CEN instances by region, CEN instance name, network instance name, or Cloud Firewall configuration status. For example, you can set the Cloud Firewall configuration status to **Unconfigured** and click **Search** to query all CEN instances for which Cloud firewalls are not configured.



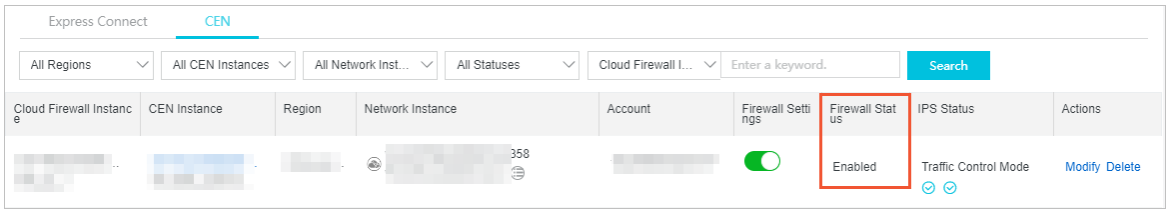
6. In the **Create VPC Firewall** dialog box, configure the required parameters.

   The following table describes the parameters used to create a VPC firewall for a CEN.

Parameter	Description
Instance Name	Enter a name for the VPC firewall. We recommend that you enter a unique name that indicates the specific business to make it easy to identify the VPC firewall.
Connection Type	Specify the type of the connection between VPCs or between a VPC and an on-premises data center. In this scenario, the value is fixed to **CEN**.
Network Instance	Confirm the region and the network instance, and specify **Destination CIDR Blocks**. You can click **Add Destination CIDR Block** next to **Destination CIDR Blocks** to add CIDR blocks.
IPS Mode	Select the work mode of the intrusion prevention system (IPS). Valid values: ○ **Monitoring Mode**: If you select this option, Cloud Firewall monitors traffic and sends alerts when it detects malicious traffic. ○ **Traffic Control Mode**: If you select this option, Cloud Firewall intercepts malicious traffic and blocks intrusion attempts. **Note** This setting is applied to all VPCs that belong to the CEN.

Parameter	Description
Intrusion Prevention	Select the intrusion prevention policies that you want to enable. Valid values: ○ **Monitoring Mode** or **Traffic Control Mode**. In monitoring mode, traffic that hits intrusion prevention rules is monitored but not blocked. In traffic control mode, traffic that hits intrusion prevention rules is blocked. You can select only one of the two modes. ○ **Basic Policies**: This feature provides basic intrusion prevention capabilities such as protection against brute force attacks and attacks that exploit command execution vulnerabilities. It also allows you to manage and control the connections from infected hosts to a command and control (C&C) server. ○ **Virtual Patches**: This feature defends against the most common high-risk application vulnerabilities in real time. **Note** This setting is applied to all VPCs that belong to the CEN.
Enable VPC Firewall	After the VPC firewall is enabled, traffic from the CEN to the configured destination CIDR blocks is protected by Cloud Firewall. If you do not require the VPC firewall to be automatically enabled after it is created, turn off this switch.

7. Click **Submit** and confirm the submission.The VPC firewall is created. If you turn on Enable VPC Firewall when you configure the VPC firewall, the VPC firewall is enabled automatically. When the VPC firewall takes effect, **Firewall Status** of the VPC firewall changes to **Enabled**.



Note After a VPC firewall is enabled, a security group named Cloud_Firewall_Security_Group is automatically added and an access control policy is created to allow traffic to the VPC firewall. Do not modify or delete this security group and the access control policy.

Create a VPC firewall for an Express Connect

If you want to enable VPC Firewall for an Express Connect, note the following items:

- VPC firewalls can control traffic between VPCs that are deployed in the same region, but cannot control traffic between VPCs that are deployed in different regions or are created by using different Alibaba Cloud accounts.
- VPC firewalls cannot control traffic between a VPC and a VBR.

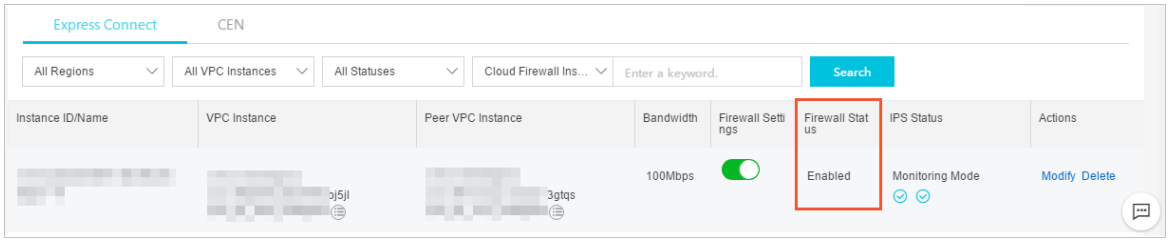
To create a VPC firewall for an Express Connect, perform the following operations:

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, click **Firewall Settings**.
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 for which you want to create a VPC firewall and click **Create** in the Actions column.If a large number of Express Connects exist, you can filter them by region, VPC instance, or Cloud Firewall configuration status. For example, you can set the Cloud Firewall configuration status to **Unconfigured** and click **Search** to query all Express Connects for which Cloud firewalls are not configured.
6. In the **Create VPC Firewall** dialog box, configure the required parameters. The following table describes the parameters used to create a VPC firewall for an Express Connect.

Parameter	Description
Instance Name	Enter a name for the VPC firewall. We recommend that you enter a unique name that indicates the specific business to make it easy to identify the VPC firewall.
Connection Type	Specify the type of the connection between VPCs or between a VPC and an on-premises data center. In this scenario, the value is fixed to **Express Connect**.
VPC	Confirm the region and name of the VPC, 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 as required. For more information, see 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, you can view multiple VPC route tables and can 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 to other CIDR blocks, you can modify this destination CIDR block. You can add multiple CIDR blocks that are separated with commas (,).
Peer VPC	Confirm the region and name of the peer VPC, 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.

Parameter	Description
Intrusion Prevention	Select the intrusion prevention policies that you want to enable. Valid values: ○ **Monitoring Mode** or **Traffic Control Mode**. In monitoring mode, traffic that hits intrusion prevention rules is monitored but not blocked. In traffic control mode, traffic that hits intrusion prevention rules is blocked. You can select only one of the two modes. ○ **Basic Policies**: This feature provides basic intrusion prevention capabilities such as protection against brute force attacks and attacks that exploit command execution vulnerabilities. It also allows you to manage and control the connections from infected hosts to a command and control (C&C) server. ○ **Virtual Patches**: This feature defends against the most common high-risk application vulnerabilities in real time. ○
Enable VPC Firewall	After you turn on Enable VPC Firewall, a VPC firewall is enabled automatically after it is created. If you do not require the VPC firewall to be automatically enabled after it is created, turn off this switch.

7. Click **Submit** and confirm the submission.The VPC firewall is created. If you turn on Enable VPC Firewall when you configure the VPC firewall, the VPC firewall is enabled automatically. When the VPC firewall takes effect, **Firewall Status** of the VPC firewall changes to **Enabled**.



What's next

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

- On the **VPC Firewall** tab, click **Modify** or **Delete** to modify or delete the created 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 **Security Policies** > **Access Control**. On the Access Control page, click the VPC Firewall tab. On the VPC Firewall tab, configure VPC firewall policies to control traffic between VPCs. For more information, see Access control on VPC firewalls.

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 this 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

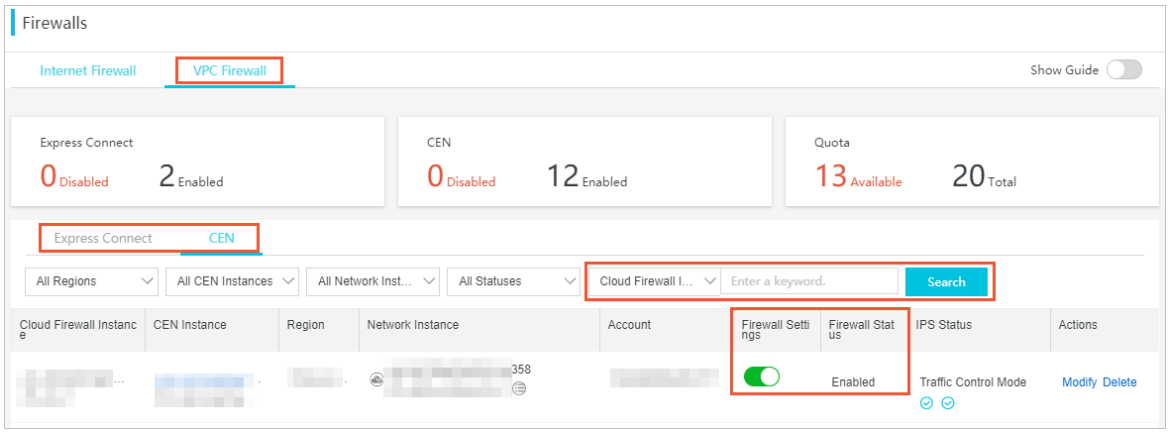
After the VPC Firewall feature is enabled, you can log on to the Cloud Firewall console and choose **Traffic Analysis > VPC Access** in the left-side navigation pane to view information about traffic between VPCs.

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. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, click **Firewall Settings**.
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.