Alibaba Cloud
Cloud Firewall

Security Policy

Issue: 20200624

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individual s arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary , incidental, 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
⛔	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.
⚠	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.
❗	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.
📋	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]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 Access control

1.1 Overview of access control policies

You can configure access control policies in Cloud Firewall to restrict the inbound and outbound traffic of your servers. This helps reduce the risk of intrusions.

Limits on the number of access control policies in each Cloud Firewall edition

The maximum number of access control policies varies with the Cloud Firewall edition.

- In **Pro** Edition, you can configure up to 1,000 outbound policies and 1,000 inbound policies.
- In **Enterprise** Edition, you can configure up to 2,000 outbound policies and 2,000 inbound policies.
- In **Flagship** Edition, you can configure up to 5,000 outbound policies and 5,000 inbound policies.

Note:

Cloud Firewall allows you to control the traffic bound to specified domains. After you configure an access control policy for a domain, all traffic bound to this domain is controlled. The policy actions include **Allow**, **Deny**, and **Monitor**.

Limits on the number of internal firewall policies

By default, you can create up to 100 policy groups and 100 policies between your servers. The policies include those created in the ECS security group module and synchronized to Cloud Firewall and those created on the Internal Firewall page in Cloud Firewall.

Note:

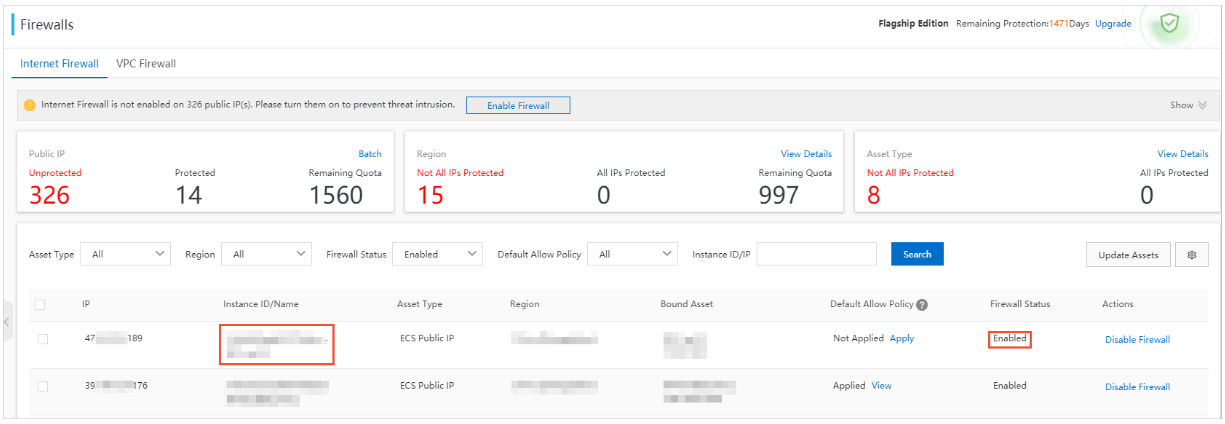
If you want to create more policies than allowed, we recommend that you delete unnecessary policies or submit a ticket for technical support.

1.2 Outbound and inbound traffic control on the Internet firewall

Cloud Firewall supports access control on the Internet firewall. You can configure policies to control the traffic between the Internet and your ECS instances.

Prerequisites

The firewall for ECS instances is enabled on the **Internet Firewall** tab. Otherwise, the access control policies you configure do not take effect.



Internet Firewall is not enabled on 326 public IP(s). Please turn them on to prevent threat intrusion.

Public IP		
Unprotected	Protected	Remaining Quota
326	14	1560

Region		
Not All IPs Protected	All IPs Protected	Remaining Quota
15	0	997

Asset Type	
Not All IPs Protected	All IPs Protected
8	0

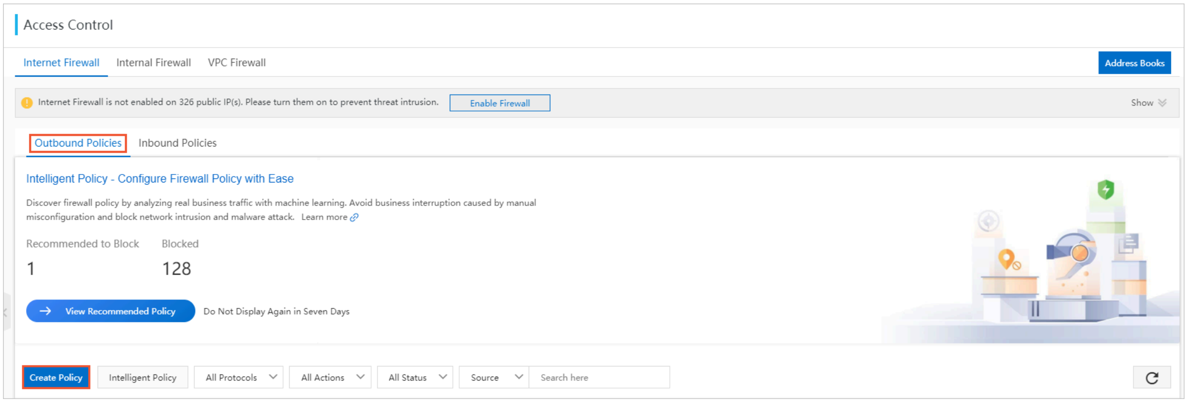
□	IP	Instance ID/Name	Asset Type	Region	Bound Asset	Default Allow Policy	Firewall Status	Actions
□	47[redacted]189	[redacted]	ECS Public IP	[redacted]	[redacted]	Not Applied Apply	Enabled	Disable Firewall
□	39[redacted]176	[redacted]	ECS Public IP	[redacted]	[redacted]	Applied View	Enabled	Disable Firewall

Context

You can configure **outbound** and **inbound** access control policies.

Outbound traffic control

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.
3. Navigate to **Internet Firewall** > **Outbound Policies**, click **Create Policy**.



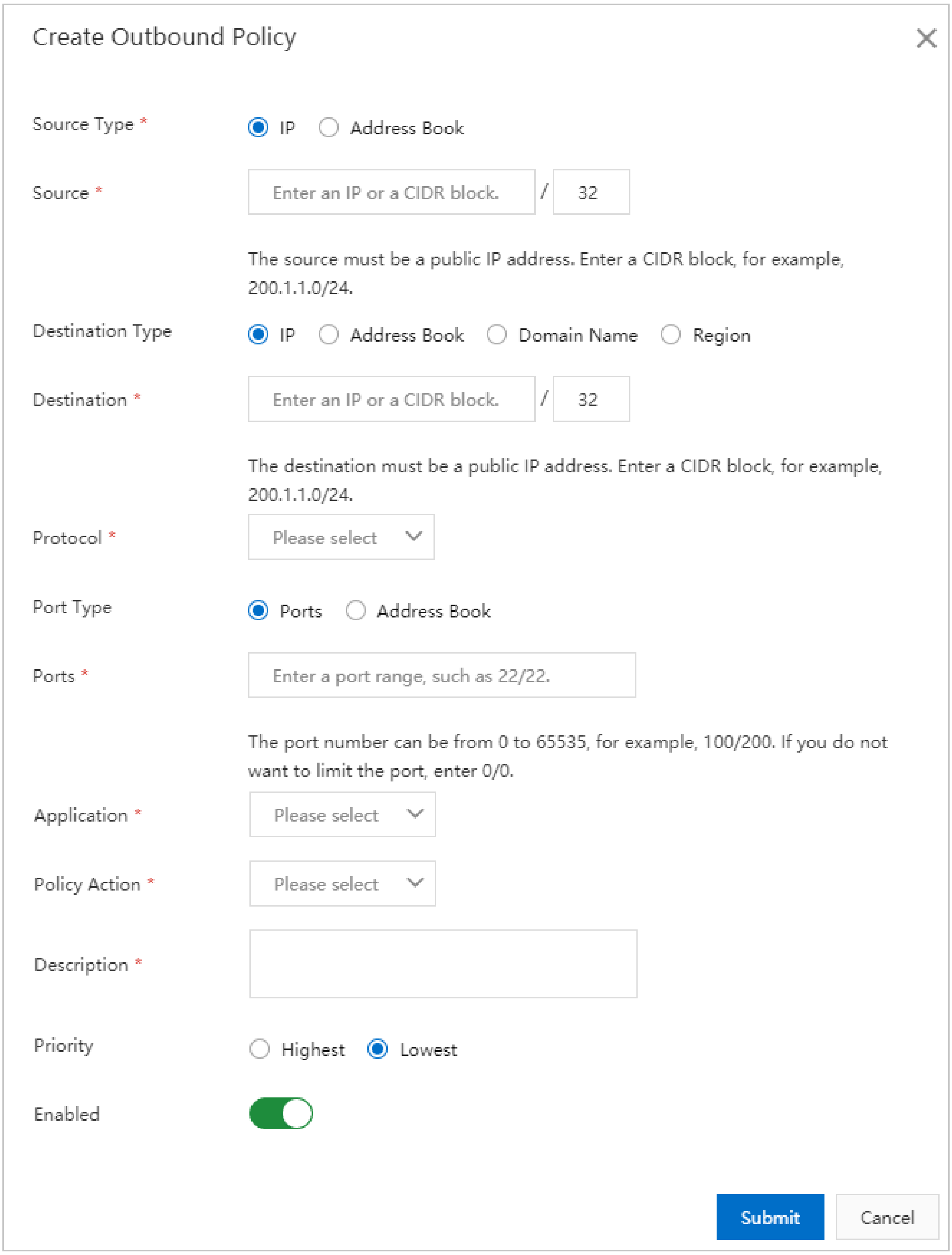
Internet Firewall is not enabled on 326 public IP(s). Please turn them on to prevent threat intrusion.

Intelligent Policy - Configure Firewall Policy with Ease

Discover firewall policy by analyzing real business traffic with machine learning. Avoid business interruption caused by manual misconfiguration and block network intrusion and malware attack. Learn more

Recommended to Block	Blocked
1	128

4. In the **Create Outbound Policy** dialog box, configure the policy parameters.



Create Outbound Policy

Source Type * ● IP ○ Address Book

Source * Enter an IP or a CIDR block. / 32

The source must be a public IP address. Enter a CIDR block, for example, 200.1.1.0/24.

Destination Type ● IP ○ Address Book ○ Domain Name ○ Region

Destination * Enter an IP or a CIDR block. / 32

The destination must be a public IP address. Enter a CIDR block, for example, 200.1.1.0/24.

Protocol * Please select

Port Type ● Ports ○ Address Book

Ports * Enter a port range, such as 22/22.

The port number can be from 0 to 65535, for example, 100/200. If you do not want to limit the port, enter 0/0.

Application * Please select

Policy Action * Please select

Description *

Priority ○ Highest ● Lowest

Enabled

a. In the first outbound policy, **allow** traffic from trusted IP addresses.

A. Configure the following parameters.

Parameter	Description
Source Type	Select IP or Address Book. • **IP**: Specify only one CIDR block. • **Address Book**: Select a pre-configured address book. The address book contains multiple CIDR blocks, which simplifies the configuration of access control policies.
Source	Specify the source addresses that are allowed to access the Internet. • If Source Type is set to **IP**, enter a CIDR block, for example, 1.1.1.1/32. • If Source Type is set to **Address Book**, find the target address book and click **Select** in the Actions column to configure IP addresses in the address book as the source.
Destination Type	Select IP, Address Book, Domain Name, or Region. **Note:** If you select Region, you can select a destination from all seven continents in the world and regions in China. The regions in China include 23 provinces, 4 municipalities, 5 autonomous regions, and 2 special administrative regions.
Destination	Specify the destination address that can be accessed.
Protocol	Specify the protocol used in outbound traffic, which can be TCP, UDP, or ICMP. If you are not sure about the protocol, select ANY, which means that all protocols are matched.
Port Type	Select Port or Address Book. • **Port**: Enter only one port range. • **Address Book**: Select a pre-configured **port address book**, which contains multiple ports.
Ports	Specify the ports whose traffic is to be allowed or denied. Enter a port number range or select a port address book, depending on whether you select **Ports** or **Address Book** in the **Port Type** field.
Application	Select the application to which the policy applies. **Note:** If **Destination Type** is set to Domain Name, you can set this parameter to HTTP, HTTPS, SMTP, or SMTPS.

Parameter	Description
Policy Action	Specify whether the policy allows or denies traffic on the Internet firewall. Select Allow for this policy.
Description	Enter a description to identify the policy.
Priority	Configure the priority of the policy, which defaults to **Lowest**.

B. Click **Submit**.

> **Note:**
>
> The created policy is displayed in the last row on the last page of the policy list.

b. In the second **outbound** policy, deny traffic from all other IP addresses.

Set **Source** to 0.0.0.0/0 and **Policy Action** to **Deny** to prevent all unauthorized access activities. Configure the other parameters according to the descriptions in the preceding table.

c. Check that the priority of the **allow** policy on the trusted IP addresses is higher than that of the **deny** policy.

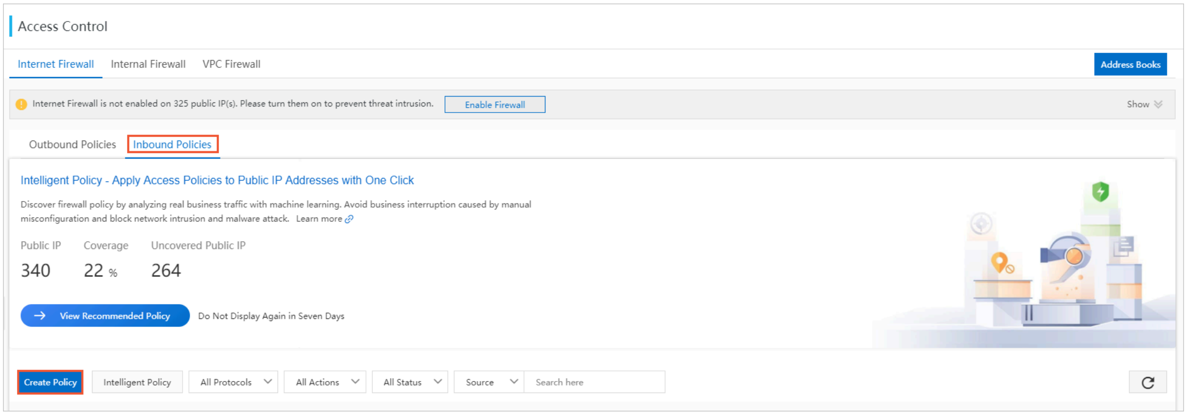
> **Note:**
>
> By default, Cloud Firewall assigns priorities to access control policies based on the order in which they are created. A new policy has a lower priority than all existing policies. For more information about the policy priorities, see Change the priority of an access control policy.

For more information about policy parameters, see Parameters in an access control policy.

Inbound traffic control

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.

3. Navigate to **Internet Firewall** > **Inbound Policies**, click **Create Policy**.



Internet Firewall is not enabled on 325 public IP(s). Please turn them on to prevent threat intrusion.

Intelligent Policy - Apply Access Policies to Public IP Addresses with One Click

Discover firewall policy by analyzing real business traffic with machine learning. Avoid business interruption caused by manual misconfiguration and block network intrusion and malware attack. Learn more

Public IP	Coverage	Uncovered Public IP
340	22 %	264

4. In the **Create Inbound Policy** dialog box, create a policy to **allow** traffic from trusted external IP addresses.

   Set **Source** to a trusted CIDR block or an IP address book. Set **Policy Action** to **Allow**. For information about other parameters, see the parameter descriptions in Outbound traffic control.

   > **Note:**
   > If you set **Source Type** to Address Book for an inbound policy, you can set **Source** to an IP address book or cloud address book. If you set Destination Type to Address Book, you can only set Destination to an IP address book.

5. In the second inbound policy, **deny** the traffic from all other external IP addresses.

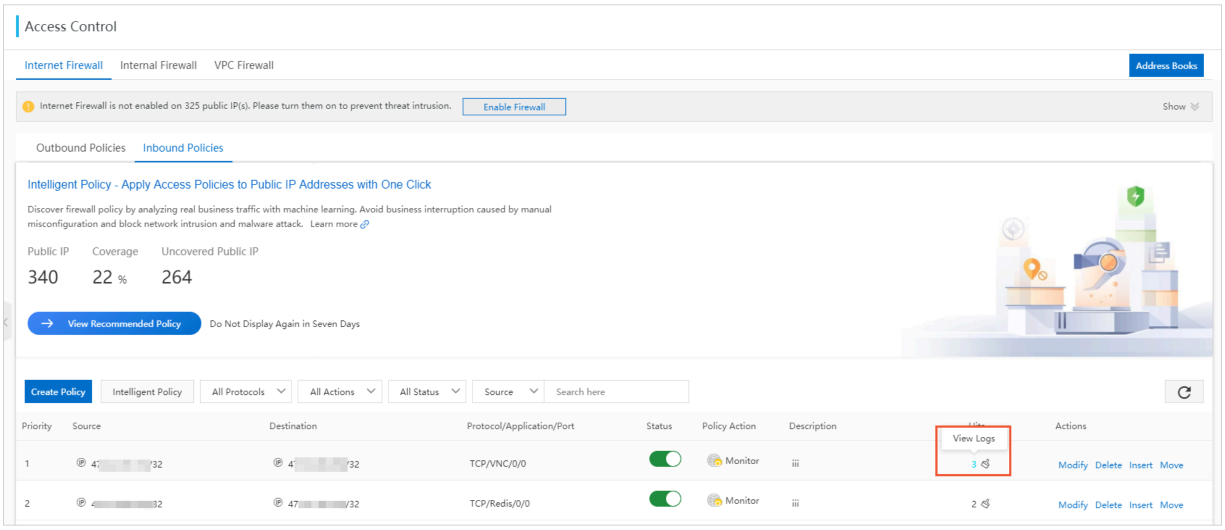
   Set **Source** to 0.0.0.0/0 and **Policy Action** to **Deny** to prevent all unauthorized access activities.

6. Check that the priority of the **allow** policy on the trusted IP addresses is higher than that of the **deny** policy.

Check whether the policies have taken effect

A created policy takes effect immediately. However, if the policy parameters are invalid or the Internet firewall is disabled, the policy does not take effect.

In the policy list, find the target policy and click the number in the Hits column. The **Traffic Logs** page appears. If the name of the policy is displayed in the **Policy Name** column, this policy has taken effect.



Internet Firewall is not enabled on 325 public IP(s). Please turn them on to prevent threat intrusion.

Intelligent Policy - Apply Access Policies to Public IP Addresses with One Click

Discover firewall policy by analyzing real business traffic with machine learning. Avoid business interruption caused by manual misconfiguration and block network intrusion and malware attack. Learn more

Public IP	Coverage	Uncovered Public IP
340	22 %	264

Priority	Source	Destination	Protocol/Application/Port	Status	Policy Action	Description	Hits	Actions
1	47[redacted]/32	4[redacted]/32	TCP/VNC/0/0	●	Monitor	iii	3	Modify Delete Insert Move
2	4[redacted]32	47[redacted]/32	TCP/Redis/0/0	●	Monitor	iii	2	Modify Delete Insert Move

Note:

If you delete a policy, the allow or deny action configured in this policy becomes invalid. Exercise caution when you perform this operation.

Parameters in an access control policy

Parameter	Description
Source Type	The type of the source address. You can select IP or Address Book. • If you select **IP**, enter a CIDR block in the **Source** field. • If you select **Address Book**, set **Source** to a pre-configured address book. You can add multiple IP addresses to an address book to simplify the policy configuration.

Parameter	Description
Source	The source IP address or CIDR block of the traffic. **Note:** You can only specify one CIDR block, for example, 1.1.1.1/32. If you set **Source Type** to **Address Book**, select a pre-configured address book as the source. **Note:** • In an outbound policy, the source can only be an IP address book , but the destination can be an IP address book, domain address book, or cloud address book. • In an inbound policy, the source can be an IP address book or cloud address book, but the destination can only be an IP address book.
Destination Type	• **IP**: Set the destination to an IP address or CIDR block. • **Address Book**: Set the destination to an address book. • **Domain Name**: Set the destination to a domain name. You can specify a wildcard domain name, for example, `*.aliyun.com`. **Note:** By default, if an HTTP header does not contain the host field or an HTTPS request does not contain the Server Name Indication (SNI), Cloud Firewall **allows** the traffic. • **Region**: Set the destination to a region. You can select a region inside or outside China.

Parameter	Description
Destination	Set the destination to a CIDR block. If you set **Destination Type** to Domain Name, set the destination to a domain name. Wildcard domain names are supported. **Note:** • In an outbound policy, the source can only be an IP address book , but the destination can be an IP address book, domain address book, or cloud address book. • In an inbound policy, the source can be an IP address book or cloud address book, but the destination address book can only be an IP address book.
Protocol	• ANY (All protocols are matched.) • TCP • UDP • ICMP
Port Type	Select **Port** or **Address Book**. • **Port**: You can specify only one port range. • **Address Book**: You can select a pre-configured **port address book**, which contains multiple ports.
Ports	You can specify a port range. 0/0 indicates all ports can be matched. **Note:** If you set Protocol to ICMP, the destination ports are not required. If you set Protocol to ANY, the destination ports you specify do not take effect in ICMP traffic control.
Application	You can set the application to ANY, HTTP, HTTPS, Memcache, MongoDB, MQTT, MySQL, RDP, Redis, SMTP, SMTPS, SSH, or VNC. If **Protocol** is set to TCP, multiple applications are available. Otherwise, you can only set the application to ANY. **Note:** Cloud Firewall identifies applications based on packet characteristics, instead of port numbers. If Cloud Firewall fails to identify the application in a packet, it **allows** the packet.

Parameter	Description
Policy Action	Specify whether the policy allows or denies traffic. • **Allow**: Matched traffic is allowed. • **Deny**: Matched traffic is denied without notifications. • **Monitor**: Matched traffic is monitored but allowed. After you observe the traffic for a period of time, you can change the policy action to **Allow** or **Deny**.
Description	Enter a description to identify the policy.
Priority	The priority of the policy, which defaults to Lowest. • **Lowest**: The policy takes effect in the last priority. • **Highest**: The policy takes effect in the first priority.

1.3 Strict mode of the Internet firewall

The strict mode of the Internet firewall blocks traffic that matches an access control policy but contains an application unknown to Cloud Firewall. Cloud Firewall identifies applications based on packet characteristics. If Cloud Firewall fails to identify the application in the traffic, it allows the traffic by default. If you want to discard traffic with unknown applications, you can enable the strict mode.

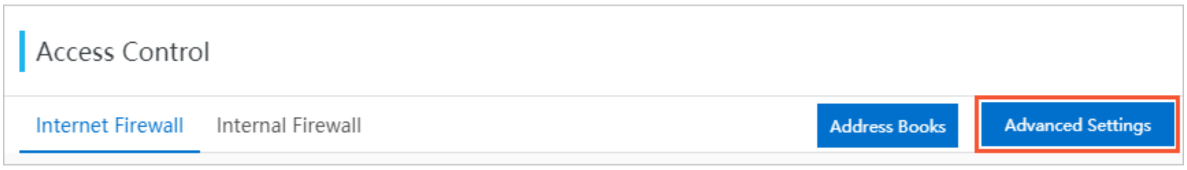
Context

The strict mode only takes effect on traffic that matches an access control policy, regardless of whether the policy action is allow, deny, or monitor. If the traffic does not match any access control policy, the traffic is allowed even if its application is unknown.

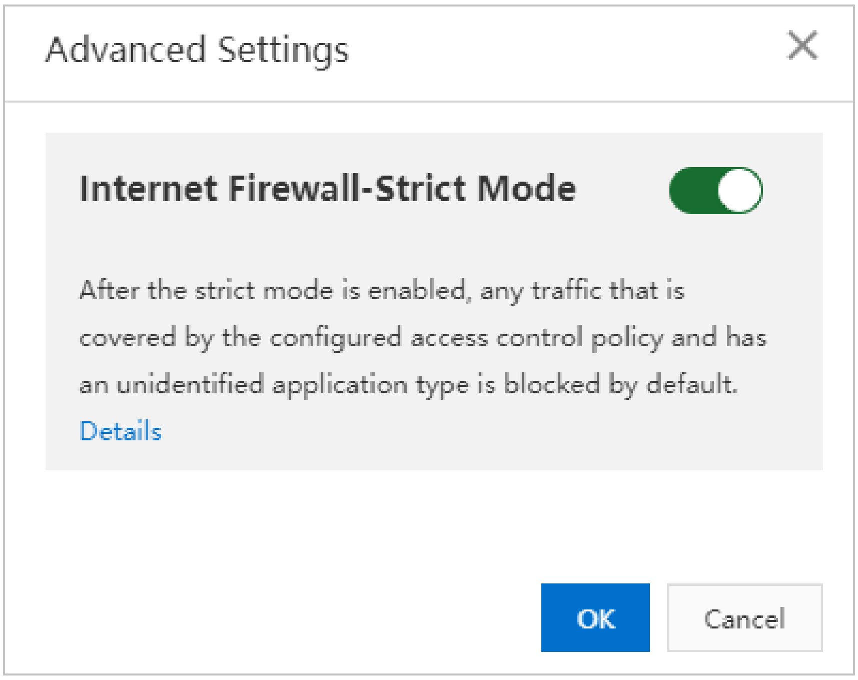
Before you enable the strict mode on the Internet firewall, we recommend that you configure access control policies. For more information, see Outbound and inbound traffic control on the Internet firewall.

Enable or disable the strict mode

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.
3. In the upper-right corner of the **Internet Firewall** tab, click **Advanced Settings**.



4. In the **Advanced Settings** dialog box that appears, enable or disable **Internet Firewall-Strict Mode** and click **OK**.



Advanced Settings

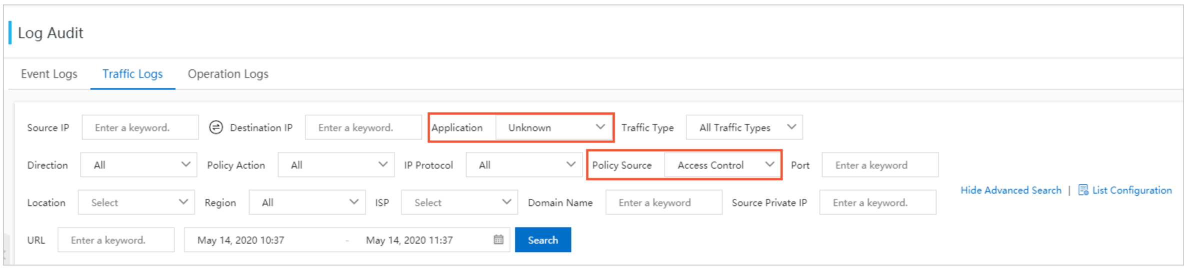
Internet Firewall-Strict Mode

After the strict mode is enabled, any traffic that is covered by the configured access control policy and has an unidentified application type is blocked by default.

After the strict mode is enabled, all traffic that matches an access control policy and contains unknown applications is discarded. You can view logs of discarded traffic on the Log Audit page.

View logs of discarded traffic

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Logs** > **Log Audit**.
3. Navigate to **Traffic Logs** > **Internet Firewall** and click **Show Advanced Search**. Then, set **Application** to **Unknown** and **Policy Source** to **Access Control** and click **Search**.



Log Audit

Source IP: Enter a keyword. | Destination IP: Enter a keyword. | Application: Unknown | Traffic Type: All Traffic Types

Direction: All | Policy Action: All | IP Protocol: All | Policy Source: Access Control | Port: Enter a keyword

Location: Select | Region: All | ISP: Select | Domain Name: Enter a keyword | Source Private IP: Enter a keyword.

URL: Enter a keyword. | May 14, 2020 10:37 - May 14, 2020 11:37

4. View the logs of traffic discarded in strict mode. The policy names of these logs are **unknown_app_deny_all**. You can view the time, source IP addresses, destination IP addresses, and destination ports of the discarded traffic.

   If normal traffic is discarded, we recommend that you add the application information to the request packets or disable the strict mode.

1.4 Access control on an internal firewall between ECS instances

Cloud Firewall uses internal firewalls to control inbound and outbound traffic between ECS instances. You can configure access control policies to restrict unauthorized access between ECS instances. The access control policies you configure and publish in the Cloud Firewall console are synchronized to ECS security groups.

Context

Compared with creating security group rules for ECS instances, creating access control policies on an internal firewall has the following advantages:

- You can publish multiple policies at a time.
- You can create policy groups by using templates to allow or deny all traffic by default.
- Cloud Firewall automatically creates security group rules based on application groups.

For more information about the differences between internal firewalls and ECS security groups, see #unique_9.

Before you configure access control policies on an internal firewall, you must create a policy group, which contains default access control policies. Then, you can configure fine-grained inbound and outbound access control policies in the policy group. After you configure access control policies in the policy group, you must publish the policies, so they can be synchronized to ECS security groups and take effect. The procedure is as follows:

1. Create a policy group
2. Create an access control policy
3. Publish policies in a policy group

By default, you can create up to 100 policy groups and 100 policies in each group. The policies include both those synchronized from ECS security groups to Cloud Firewall and those created in the Cloud Firewall console. If you want to create more than 100 policies, delete unnecessary policies or submit a ticket.

Policy group types

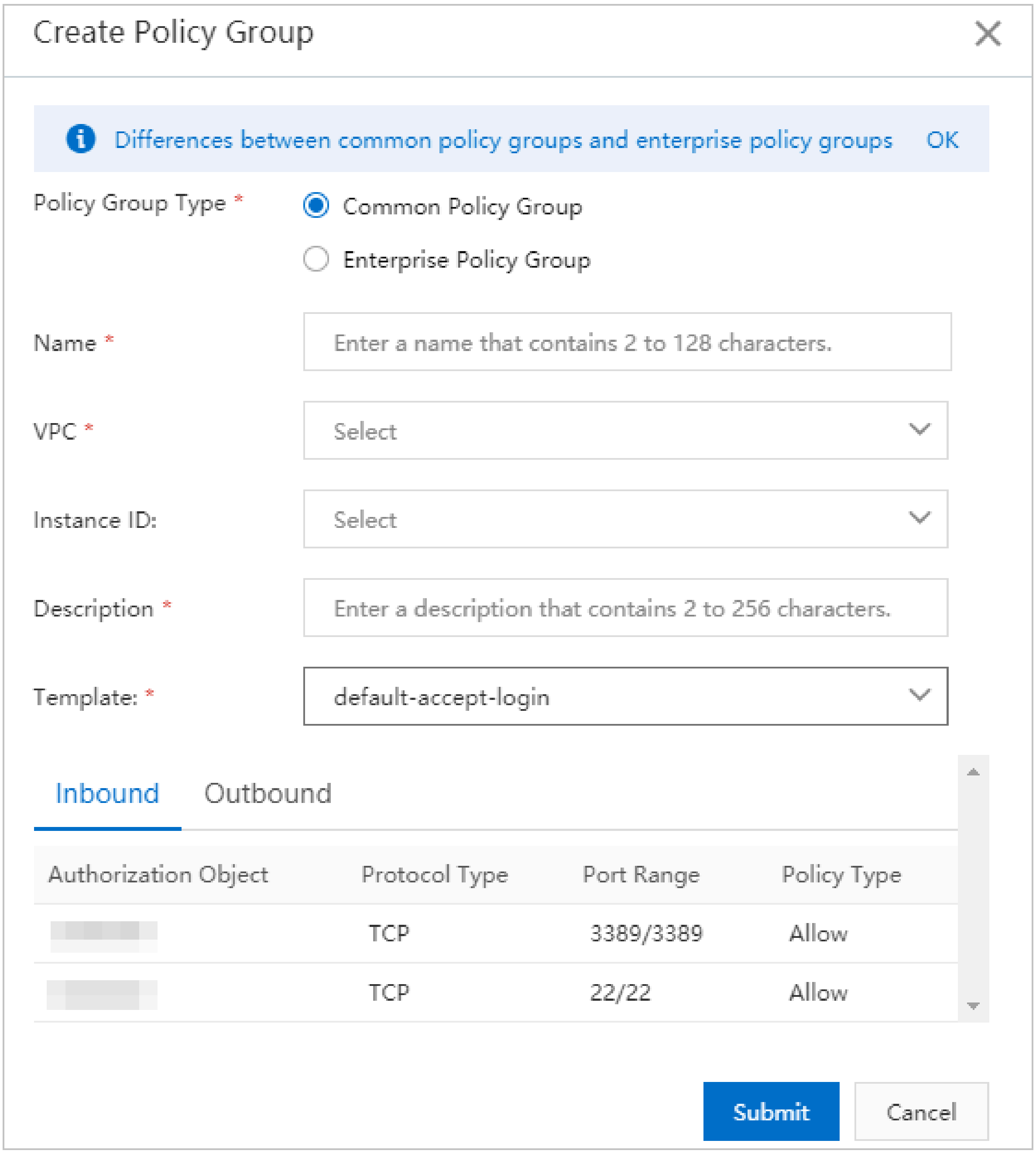
Policy groups are classified into common and enterprise policy groups. The following table lists the differences between the two types of policy groups.

Policy group type	Policy type	Policy priority	Inbound policy	Outbound policy	Scenario
Common policy group	Default policy	Determined by the policy group template.	Allows or denies traffic based on the policy group template.	Allows or denies traffic based on the policy group template.	Businesses that require fine-grained network control on a moderate number of network connections.
	Custom policy	A value within the range of 1 to 100. A smaller value indicates a higher priority.	Allows or denies traffic based on your business needs.	Allows or denies traffic based on your business needs.	
Enterprise policy group	Default policy	The value is 1 and cannot be changed.	Allows traffic based on the policy group template.	Allows traffic based on the policy group template.	Businesses that require efficient O&M.
	Custom policy		Allows traffic based on your business needs.	Allows traffic based on your business needs.	

Create a policy group

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.
3. On the **Access Control** page, click the **Internal Firewall** tab. Then, click **Create Policy Group** in the upper-right corner.

4. In the **Create Policy Group** dialog box that appears, configure policy group parameters.



Create Policy Group

Differences between common policy groups and enterprise policy groups OK

Policy Group Type * ● Common Policy Group ○ Enterprise Policy Group

Name * Enter a name that contains 2 to 128 characters.

VPC * Select

Instance ID: Select

Description * Enter a description that contains 2 to 256 characters.

Template: * default-accept-login

Inbound Outbound

Authorization Object	Protocol Type	Port Range	Policy Type
[redacted]	TCP	3389/3389	Allow
[redacted]	TCP	22/22	Allow

Parameter	Description
Policy Group Type	Valid values: • **Common Policy Group**: suitable for businesses that require fine-grained network control on a moderate number of network connections. • **Enterprise Policy Group**: suitable for businesses that require efficient O&M.
Name	Enter a name that helps identify the policy group.

Parameter	Description
VPC	Select a VPC to which you want to apply the policy group from the **VPC** drop-down list. **Note:** A policy group can be applied to only one VPC.
Instance ID	Select one or more ECS instances to which you want to apply the policy group from the **Instance ID** drop-down list. **Note:** The Instance ID drop-down list only contains ECS instances within the selected **VPC**.
Description	Enter a description for the policy group.
Template	Select a template from the **Template** drop-down list. • **default-accept-login**: allows inbound traffic destined for TCP ports 22 and 3389 and all outbound traffic. • **default-accept-all**: allows all inbound and outbound traffic. • **default-drop-all**: denies all inbound and outbound traffic. **Note:** Enterprise policy groups do not support the **default-drop-all** template.

5. Click **Submit**.

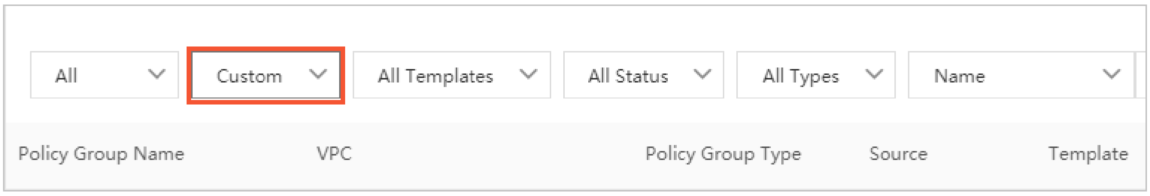
   The created policy group is displayed on the Internal Firewall tab. You can perform the following operations on the policy group:

   - **Configure Policy**: Configure fine-grained access control policies in the policy group.
   - **Publish**: Synchronize the access control policies in the policy group to ECS security groups.
   - **Modify**: Change the ECS instances to which the policy group is applied and modify the group description.
   - **Delete**: Delete the policy group.

   Warning:

After you delete a policy group, its access control policies are also deleted. Exercise caution when you perform this operation.

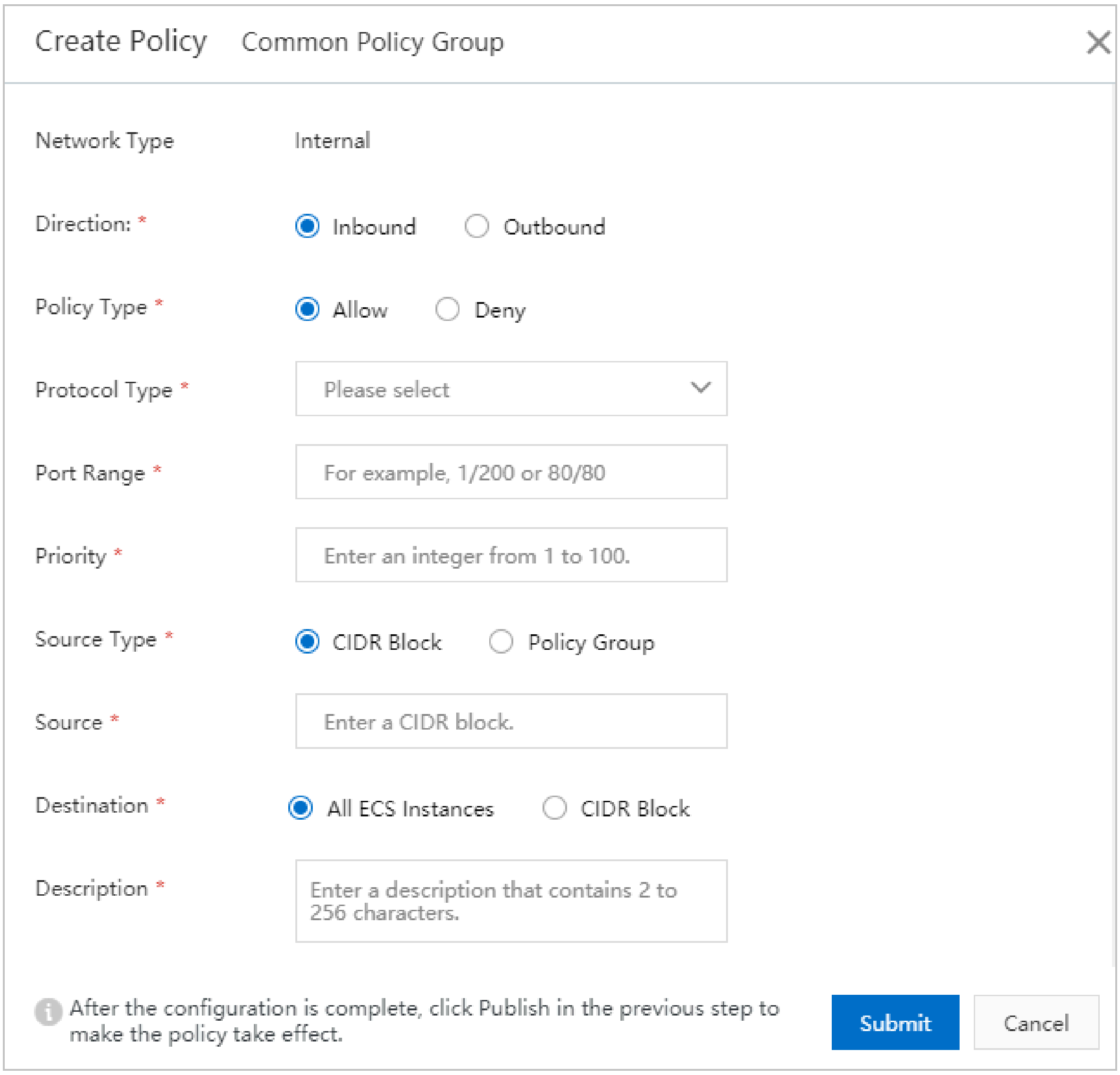
If you want to delete policy groups that are no longer needed, set the source to **Custom** and click Search to view all custom policy groups and determine whether to delete them.



Create an access control policy

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.
3. On the **Access Control** page, click the **Internal Firewall** tab, find the target policy group, and click **Configure Policy** in the Actions column.
4. On the **Policies** page, click **Create Policy**.

5. In the **Create Policy** dialog box that appears, configure the policy parameters.



Create Policy Common Policy Group

Network Type: Internal

Direction: * ● Inbound ○ Outbound

Policy Type * ● Allow ○ Deny

Protocol Type * Please select

Port Range * For example, 1/200 or 80/80

Priority * Enter an integer from 1 to 100.

Source Type * ● CIDR Block ○ Policy Group

Source * Enter a CIDR block.

Destination * ● All ECS Instances ○ CIDR Block

Description * Enter a description that contains 2 to 256 characters.

After the configuration is complete, click Publish in the previous step to make the policy take effect.

Parameter	Description
Network Type	The default value is **Internal** and cannot be changed. This value indicates that the policy is applied to an internal network.
Direction	Valid values: - **Inbound**: traffic from other ECS instances to the ECS instances specified in the policy group. - **Outbound**: traffic from the ECS instances specified in the policy group to other ECS instances.

Parameter	Description
Policy Type	Valid values: - **Allow**: allows traffic that matches the policy. - **Deny**: denies traffic that matches the policy. If the traffic is denied, data packets are discarded without responses. If two policies have the same configuration but different policy types, the **deny** policy takes effect, and the **allow** policy does not. **Note:** Enterprise policy groups do not support the **Deny** policy type.
Protocol Type	Select the traffic protocol from the **Protocol Type** drop-down list. - **TCP** - **UDP** - **ICMP** - **ANY** (You can select ANY if you do not know which protocol is used.)
Port Range	The destination port of traffic controlled by the policy, for example, 22/22.
Priority	Enter the priority of the policy. The priority must be an integer within the range of 1 to 100. A smaller value indicates a higher priority. Different policies can have the same priority. If an allow policy and a deny policy have the same priority, the deny policy takes precedence. **Note:** The priorities of policies in an enterprise policy group are fixed to **1** and cannot be changed. The value 1 indicates the highest priority.

Parameter	Description
Source Type and **Source**	For an **inbound** policy, configure the source type and source of traffic. Valid source types: • **CIDR Block** If you select this type, you can enter only one CIDR block as the traffic source. • **Policy Group** If you select this type, you must select a policy group. All ECS instances in the policy group are the traffic sources. **Note:** Enterprise policy groups do not support the **Policy Group** option.
Destination	For an **inbound** policy, select the destination of traffic. • **All ECS Instances**: All ECS instances under your Alibaba Cloud account are the traffic destinations. • **CIDR Block**: Enter a destination CIDR block.
Select Source	For an **outbound** policy, select the source of the traffic. • **CIDR Block**: Enter a source CIDR block. • **All ECS Instances**: All ECS instances under your Alibaba Cloud account are the traffic sources.

Parameter	Description
Destination Type and **Destination**	For an **outbound** policy, configure the destination type and destination of traffic. Valid destination types: • **CIDR Block** If you select this type, you can enter only one CIDR block as the traffic destination. • **Policy Group** If you select this type, you must select a policy group. All ECS instances in the policy group are the traffic destinations. **Note:** Enterprise policy groups do not support the **Policy Group** option.
Description	Enter a description for the policy.

6. Click **Submit**.

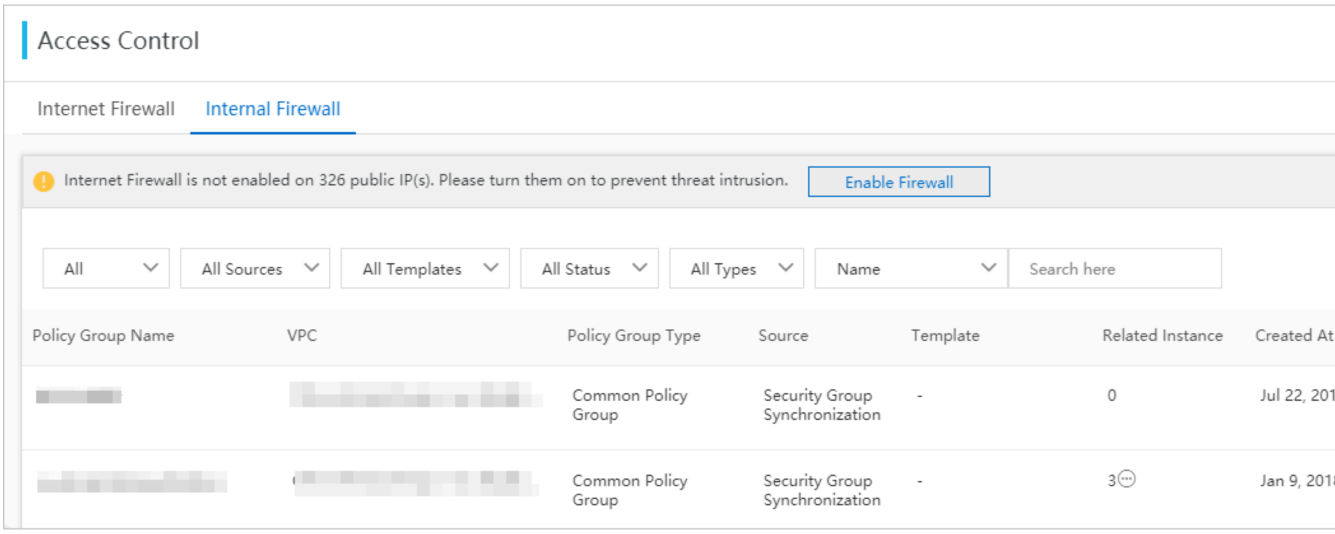
   The created policy is displayed in the policy list. You can **edit** or **delete** policies in the list.

> **Warning:**
>
> After you delete a policy, its access control configuration becomes invalid. Exercise caution when you delete a policy. A deleted policy is retained in the list, but you cannot perform operations on it.

Publish policies in a policy group

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.

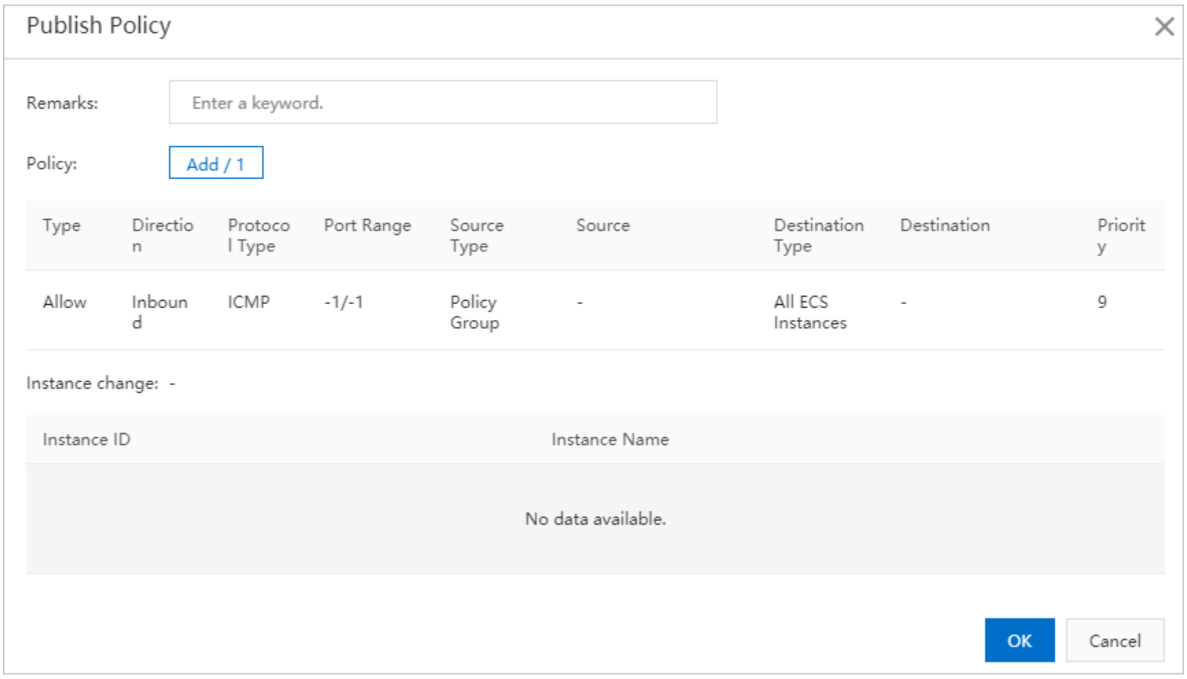
3. On the **Access Control** page, click the **Internal Firewall** tab, find the target policy group, and click **Publish** in the Actions column.



Internet Firewall is not enabled on 326 public IP(s). Please turn them on to prevent threat intrusion.

Policy Group Name	VPC	Policy Group Type	Source	Template	Related Instance	Created At
[redacted]	[redacted]	Common Policy Group	Security Group Synchronization	-	0	Jul 22, 201
[redacted]	[redacted]	Common Policy Group	Security Group Synchronization	-	3	Jan 9, 201

4. In the **Publish Policy** dialog box that appears, confirm the content of the policies, enter remarks, and click **OK**.



Remarks: Enter a keyword.

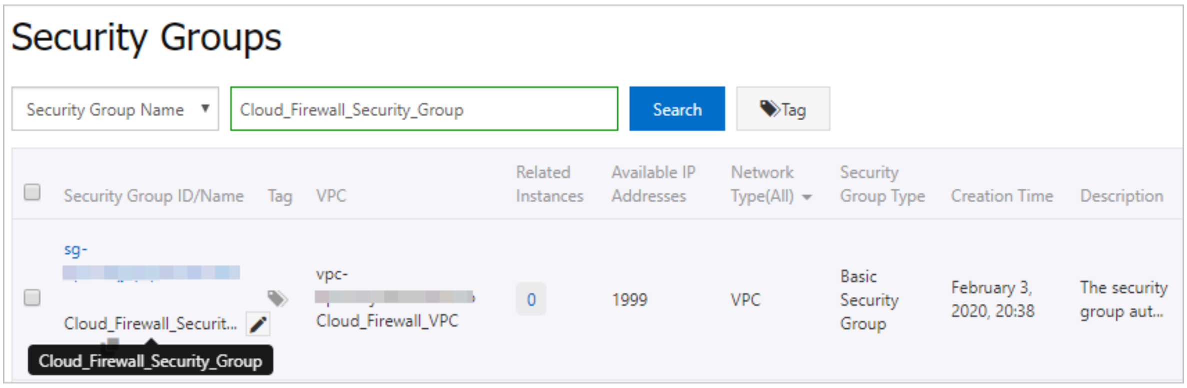
Policy: Add / 1

Type	Direction	Protocol Type	Port Range	Source Type	Source	Destination Type	Destination	Priority
Allow	Inbound	ICMP	-1/-1	Policy Group	-	All ECS Instances	-	9

Instance change: -

Instance ID	Instance Name
No data available.	

The policies take effect on ECS security groups after you publish them. You can log on to the ECS console and navigate to **Network & Security** > **Security Groups** to view the policies you have published in the Cloud Firewall console. The default policy name is **Cloud_Firewall_Security_Group**.



Security Groups

Security Group Name ▾ | Cloud_Firewall_Security_Group | Search | Tag

□	Security Group ID/Name	Tag	VPC	Related Instances	Available IP Addresses	Network Type(All)	Security Group Type	Creation Time	Description
□	sg-[redacted] Cloud_Firewall_Securit...		vpc-[redacted] Cloud_Firewall_VPC	0	1999	VPC	Basic Security Group	February 3, 2020, 20:38	The security group aut...

Cloud_Firewall_Security_Group

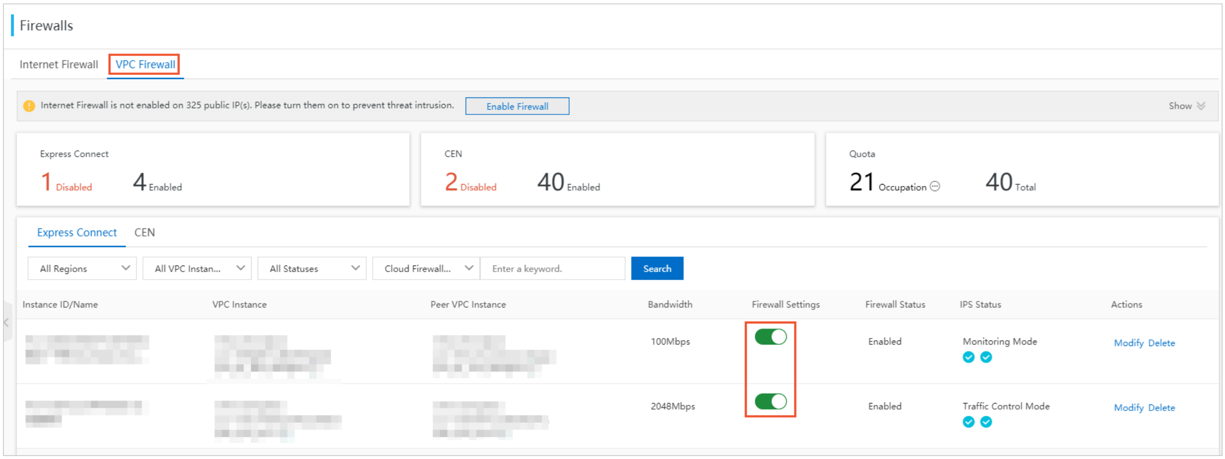
1.5 Access control on VPC firewalls

This topic describes how to configure access control policies on VPC firewalls. Cloud Firewall uses VPC firewalls to detect and control traffic between VPCs.

Prerequisites

VPC firewalls are not enabled by default. Before you configure access control policies for VPCs, you must create and enable a VPC firewall.

Access control policies take effect only after you enable the VPC firewall.



Firewalls

Internet Firewall | VPC Firewall

Internet Firewall is not enabled on 325 public IP(s). Please turn them on to prevent threat intrusion. Enable Firewall Show

Express Connect: 1 Disabled, 4 Enabled

CEN: 2 Disabled, 40 Enabled

Quota: 21 Occupation, 40 Total

Express Connect | CEN

All Regions | All VPC Instan... | All Statuses | Cloud Firewall... | Enter a keyword. | Search

Instance ID/Name	VPC Instance	Peer VPC Instance	Bandwidth	Firewall Settings	Firewall Status	IPS Status	Actions
[redacted]	[redacted]	[redacted]	100Mbps	●	Enabled	Monitoring Mode ✓ ✓	Modify Delete
[redacted]	[redacted]	[redacted]	2048Mbps	●	Enabled	Traffic Control Mode ✓ ✓	Modify Delete

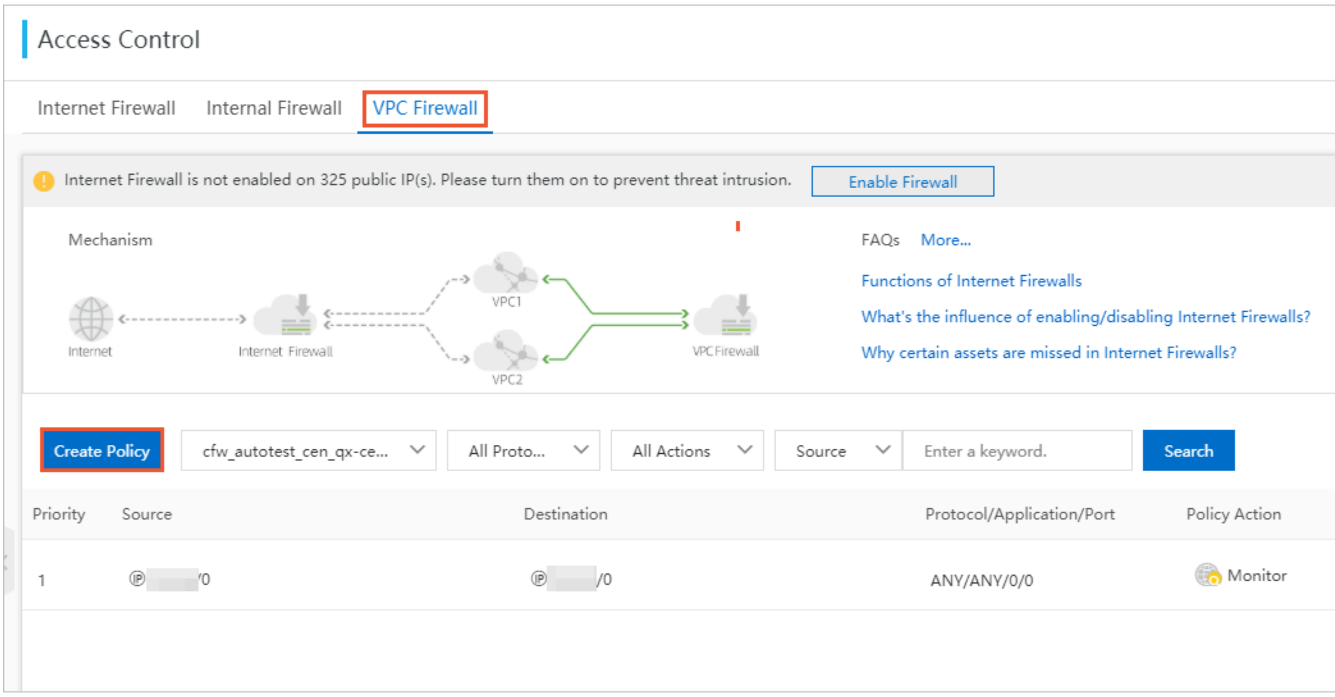
How it works

A VPC firewall allows all traffic by default. If you want to control traffic between VPCs, you can configure access control policies to deny traffic from untrusted sources. You can also allow traffic from trusted sources and deny traffic from all other sources.

Procedure

1. Log on to the Cloud Firewall console.

2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.
3. On the **VPC Firewall** tab, click **Create**.



Access Control

Internet Firewall Internal Firewall VPC Firewall

Internet Firewall is not enabled on 325 public IP(s). Please turn them on to prevent threat intrusion. Enable Firewall

Mechanism

FAQs More...

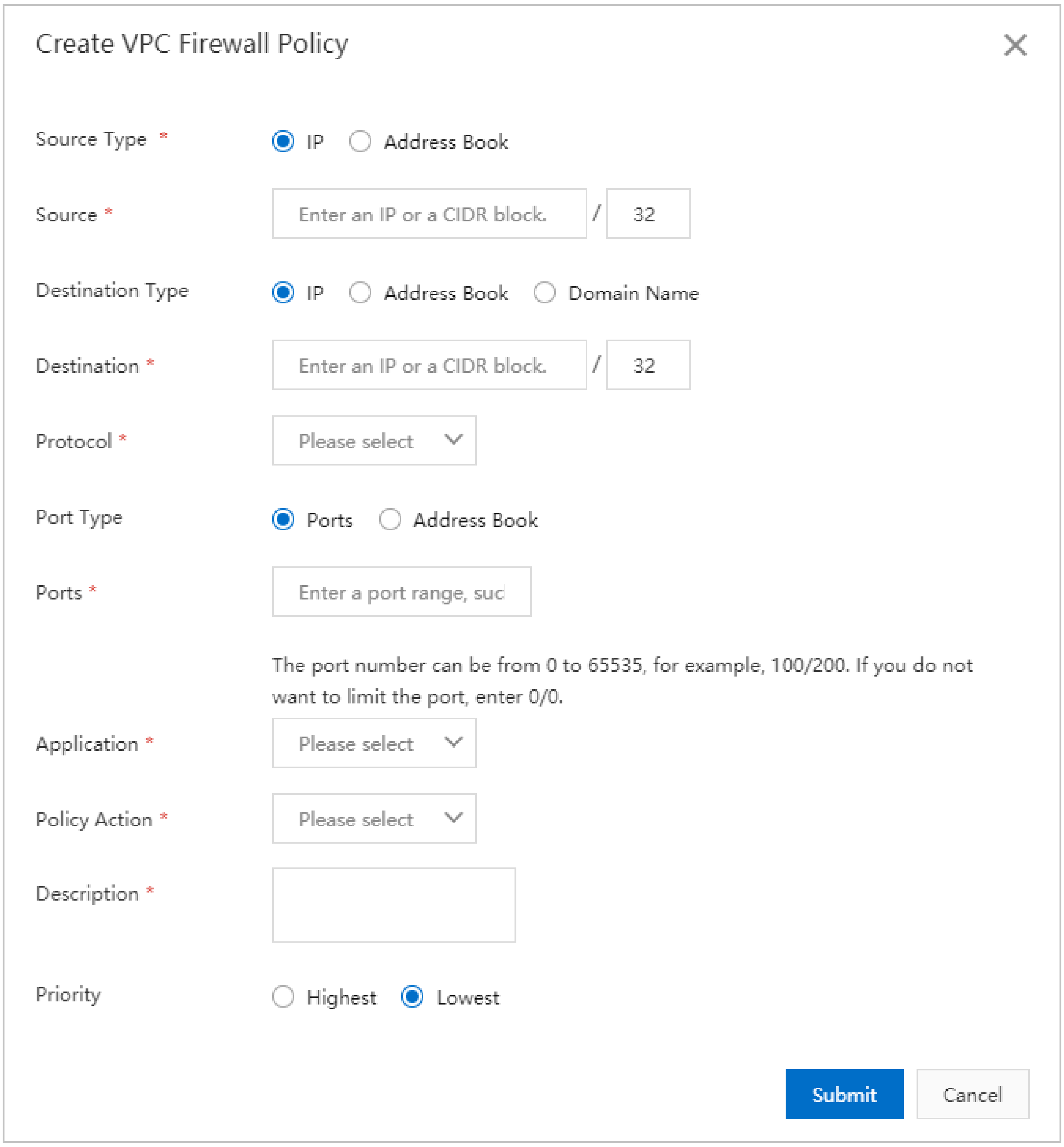
Functions of Internet Firewalls

What's the influence of enabling/disabling Internet Firewalls?

Why certain assets are missed in Internet Firewalls?

Priority	Source	Destination	Protocol/Application/Port	Policy Action
1	[redacted]/0	[redacted]/0	ANY/ANY/0/0	Monitor

4. In the **Create VPC Firewall Policy** dialog box, configure the policy. For information about parameters in a policy, see the Policy parameters table in this topic.



Create VPC Firewall Policy ×

Source Type * ● IP ○ Address Book

Source * Enter an IP or a CIDR block. / 32

Destination Type ● IP ○ Address Book ○ Domain Name

Destination * Enter an IP or a CIDR block. / 32

Protocol * Please select

Port Type ● Ports ○ Address Book

Ports * Enter a port range, suc

The port number can be from 0 to 65535, for example, 100/200. If you do not want to limit the port, enter 0/0.

Application * Please select

Policy Action * Please select

Description *

Priority ○ Highest ● Lowest

You can choose one of the following configuration methods based on your needs:

- Create a policy to **deny** traffic from untrusted sources.
- Create a policy to **allow** traffic from trusted sources, and then create another to **deny** traffic from all other sources. Make sure that the **allow** policy has a higher priority than the **deny** policy. For more information about policy priorities, see Change the priority of an access control policy.

Note:

A VPC firewall allows all traffic by default.

Policy parameters

Parameter	Description
Source Type	The type of the traffic source. You can select IP or Address Book. • If you select **IP**, enter a CIDR block in the **Source** field. • If you select **Address Book**, select a pre-configured address book in the **Source** field. **Note:** You can add multiple IP addresses to an address book to simplify policy configuration.
Source	The source CIDR block of the traffic. **Note:** You can enter only one CIDR block, for example, 1.1.1.1/32. If you set **Source Type** to **Address Book**, select a pre-configured address book.
Destination Type	• **IP**: Set the destination to a CIDR block. • **Address Book**: Set the destination to an address book. • **Domain Name**: Set the destination to a domain name. Wildcard domain names are supported, for example, *.aliyun.com. **Note:** By default, if an HTTP header does not contain the host field or an HTTPS request does not contain the Server Name Indication (SNI), Cloud Firewall **allows** the traffic.
Destination	The destination of the traffic. You can enter only one CIDR block. If you set **Destination Type** to Domain Name, enter a domain name. Wildcard domain names are supported, for example, *.aliyun.com.
Protocol	• ANY (All protocols are matched.) • TCP • UDP • ICMP

Parameter	Description
Port Type	You can select Ports or Address Book. • **Ports**: Specify only one port range. • **Address Book**: Select a pre-configured **port address book**. A port address book contains multiple ports, which simplifies policy configuration.
Ports	You can specify a port range. 0/0 indicates all ports can be matched. **Note:** If you set Protocol to ICMP, the destination ports are not required. If you set Protocol to ANY, the destination ports you specify do not take effect in ICMP traffic control.
Application	You can set the application to ANY, HTTP, HTTPS, Memcache, MongoDB, MQTT, MySQL, RDP, Redis, SMTP, SMTPS, SSH, or VNC. If **Protocol** is set to TCP, multiple applications are available. Otherwise, you can only set the application to ANY. **Note:** Cloud Firewall identifies applications based on packet characteristics, instead of port numbers. If Cloud Firewall fails to identify the application in a packet, it **allows** the packet.
Policy Action	Specify whether the VPC firewall allows or denies traffic. • **Allow**: Matched traffic is allowed. • **Deny**: Matched traffic is denied and no notifications are sent. • **Monitor**: Matched traffic is monitored but allowed. After you observe the traffic for a period of time, you can change the policy action to Allow or Deny.
Description	Enter a description to identify the policy.
Priority	The priority of a policy, which defaults to Lowest. • **Lowest**: The policy takes effect in the last priority. • **Highest**: The policy takes effect in the first priority.

1.6 Access control policies with DNS-resolved addresses

If the type of destination addresses is set to **Domain Name** in an access control policy for Internet Firewall, Cloud Firewall resolves the destination domain name and allows you to view IP addresses after the resolution. This topic describes how to configure access control policies for outbound traffic using the resolved addresses.

Context

Since the release of the access control function, you can set the destination address type to **Domain Name** when configuring an access control policy for outbound traffic in the Cloud Firewall console. If you select **Domain Name**, the policy takes effect only on HTTP, HTTPS, SSL, SMTP, or SMTPS application packets transmitted using the TCP. (The TCP is the default protocol and cannot be changed.)

Now, Cloud Firewall updates the access control policies for **outbound** traffic by using dynamic DNS resolution, enhancing domain name-based access control. If the destination address type is set to **Domain Name**, Cloud Firewall automatically resolves the domain name and use the resolved address for access control. You can view the IP address after a resolution in real time and manually update it when it changes.

Note:

- When the application type is HTTPS or SMTP, the host field is used for domain name-based access control.
- When the application type is HTTPS, SMTP, or SSL, the SNI field is used for domain name-based access control.
- You can view the IP addresses resolved from domains and use the IP addresses for access control only if the application protocol is not HTTP, HTTPS, SSL, SMTP, or SMTPS.

How the protection feature works

For an access control policy for outbound traffic (except HTTP, HTTPS, SSL, SMTP, or SMTPS traffic transmitted using the TCP), DNS resolves the domain name into an IP address. After the policy is created, Cloud Firewall protects the IP address resolved from the domain name.

Limits

Access control policies based on DNS-resolved addresses are not supported for the following scenarios:

- Inbound traffic.

  Only access control policies for outbound traffic support this feature.

- The domain name of the destination address is **Wildcard domain name**, such as *.alibabacloud.com.
- The destination address type is set to **Address Book**.
- Users of Alibaba Gov Cloud, Alibaba Finance Cloud, and international site (alibabacloud.com).

  Only public cloud accounts at the China site support this feature.

Notice:

Pay attention to the following tips when you configure access control policies based on DNS resolution:

- When you access external domain names from an ECS instance, you cannot change the default DNS server (the ADNS) configured for the instance. If you change the DNS server , the access control policy becomes invalid.
- The access control policy may not meet your business needs if multiple domain names are resolved to the same IP address.

  For example, assume that you want to configure a policy to allow FTP traffic to access a.test.com. If the DNS resolution result of a.test.com based on the A record is 1.1.1.1, the rule issued to the engine allows FTP traffic to access the IP address 1.1.1.1. If b.test.com is also resolved to 1.1.1.1 based on the A record, FTP traffic bound to b.test.com is allowed.
- Change of the DNS resolution result

  If the resolution result of domain name a.test.com changes from 1.1.1.1 to 2.2.2.2, the periodic resolution task of Cloud Firewall detects the change of the IP address in real time and automatically updates the access control policy. Cloud Firewall automatically refreshes the resolved IP address, ensuring that the real-time IP address corresponding to the domain name that you want to block or allow is included in the access control policy. The automatic update interval of a policy is 30 minutes. After the resolved address in a policy changes, the policy takes effect 30 minutes later.

  If you want to update your access control policy based on the dynamically changing resolved address, click **DNS** on the policy editing page to manually trigger DNS resolution and obtain the latest IP address, and then click **OK** to save the policy updates.

Procedure

1. Create an access control policy for **outbound** traffic.

   The following table describes the configuration items and methods of access control policies.

Item	Description	How to configure
Source Type	The type of the source address of data packets to which you want to apply the access control policy. Valid values: • **IP**: Specify one CIDR block. • **Address Book**: Select a CIDR block from the IP address book that you have configured. The address book contains multiple CIDR blocks. This allows you to manage multiple IP addresses in policy configuration.	Select IP or Address Book. If **Source Type** is set to IP, manually specify the CIDR block. If **Source Type** is set to Address Book, select a CIDR block from the address book that you have configured.
Source	The source address of data packets to which you want to apply the access control policy.	Enter the source address. **Note:** You can specify only one CIDR block, for example, 1.1.1.1/32.
Destination Type	The type of the destination address of the data packets to which you want to apply the access control policy. Valid values: IP Address, Address Book , Domain Name, and Region.	Select **Domain Name**.
Destination	The destination address of the data packets to which you want to apply the access control policy.	Enter the domain name to which you want to apply the access control policy. **Note:** Only non-wildcard domain names support dynamic DNS resolution.

Item	Description	How to configure
DNS	Cloud Firewall automatically resolves destination domain names and controls access to the obtained IP addresses.	Click **DNS** to view the IP address resolved from the domain name in real time.
Protocol	The protocol of the data packets to which you want to apply the access control policy. Valid values: - ANY: indicates any protocol. - TCP - UDP - ICMP	Select a protocol from the drop-down list.
Port Type	You can select Ports or Address Book.	Select Ports.
Ports	The ports that allow or block the outbound traffic.	Enter a port range. 0/0 indicates any port.
Application	You can set the application to ANY, HTTP, HTTPS, Memcache, MongoDB, MQTT, MySQL, RDP, Redis, SMTP, SMTPS, SSH, or VNC. If **Protocol** is set to TCP, multiple application types are supported. If it is set to other values, you can only set the application type to ANY. **Note:** Applications are identified based on the characteristics of application packets (protocol identification is not based on ports). If application identification fails, the packets are **allowed**.	Select the application type from the drop-down list.

Item	Description	How to configure
Policy Action	Indicates whether Internet firewall allows or denies the traffic. • **Allow**: The traffic is allowed. • **Deny**: The traffic is denied without any notification. • **Monitor**: The traffic is allowed. After you monitor the traffic for a period of time, you can change Policy Action to **Allow** or **Deny** based on your business needs.	Select an action type from the drop-down list.
Description	The description or note about a policy. Enter the description of the policy so that you can distinguish the policies later.	Enter the description.
Priority	The priority of an access control policy. The default priority is Lowest. • **Lowest**: indicates that the access control policy takes effect at last. • **Highest**: indicates that the access control policy takes effect first.	Select **Highest** or **Lowest**.

2. Click **Submit** to complete the configuration of the access control policy.

   After the policy is submitted, you can view, edit, delete, copy, or change its priority by choosing **Internet Firewall** > **Outbound Policies**.

What's next

You can check whether the policy takes effect by choosing **Firewall Settings** > **Internet Firewall** in the Cloud Firewall console.

1.7 Default allow policies for security groups

You can apply the default allow policies to security groups with a few clicks, so you do not need to configure a policy for each ECS instance. This topic describes how to apply the default allow policies to security groups associated with an ECS IP address.

Context

By default, security group rules deny inbound traffic from the Internet to ECS instances. Cloud Firewall provides default allow policies so you can quickly change the default action from deny to allow. This way, you do not have to configure a security group rule for each ECS instance.

How it works

Cloud Firewall issues four access control policies (security group rules) with the lowest priority (priority 100) to a security group associated with the public IP address of an ECS instance. These policies allow traffic between the ECS instance and the Internet. The four policies are automatically created. You only need to confirm and save them for the security groups.

Note:

The default allow policies take effect only on traffic **allowed** by security group rules and do not take effect on **denied** traffic.

Limits

- Advanced security groups do not support default allow policies. For more information, see #unique_13. If a VPC contains an advanced security group, default allow policies are also not supported for other security groups in the VPC.
- Default allow policies can be configured only for security groups associated with public IP addresses or EIPs of ECS instances. They cannot be configured for Internet SLB instances.
- To better protect your assets, we recommend that you do not apply default allow policies to IP addresses with the Internet firewall disabled. You must enable the firewall for IP addresses to which you have applied default allow policies. Otherwise, these IP addresses may be exposed to the Internet.

Apply default allow policies

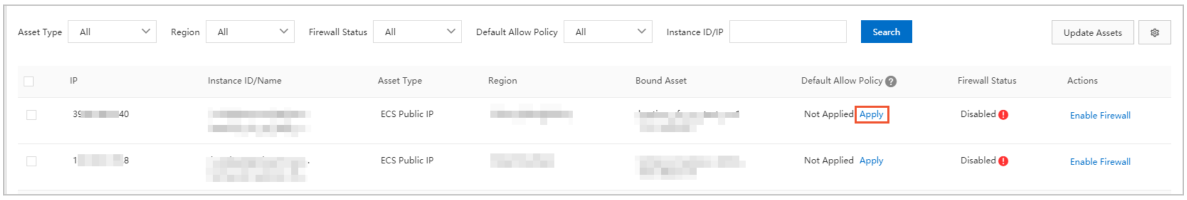
Follow these steps:

Warning:

To avoid serious security risks to your business, take note of the following:

- Do not apply the default allow policies to IP addresses not protected by the Internet firewall.
- If no traffic distribution component (for example, an Internet SLB instance) is configured for the public IP address of an ECS instance, do not apply the default allow policies to that IP address.
- If your Cloud Firewall service has expired and you plan not to renew it, go to the Security Groups page in the ECS console to delete the four policies added by Cloud Firewall.

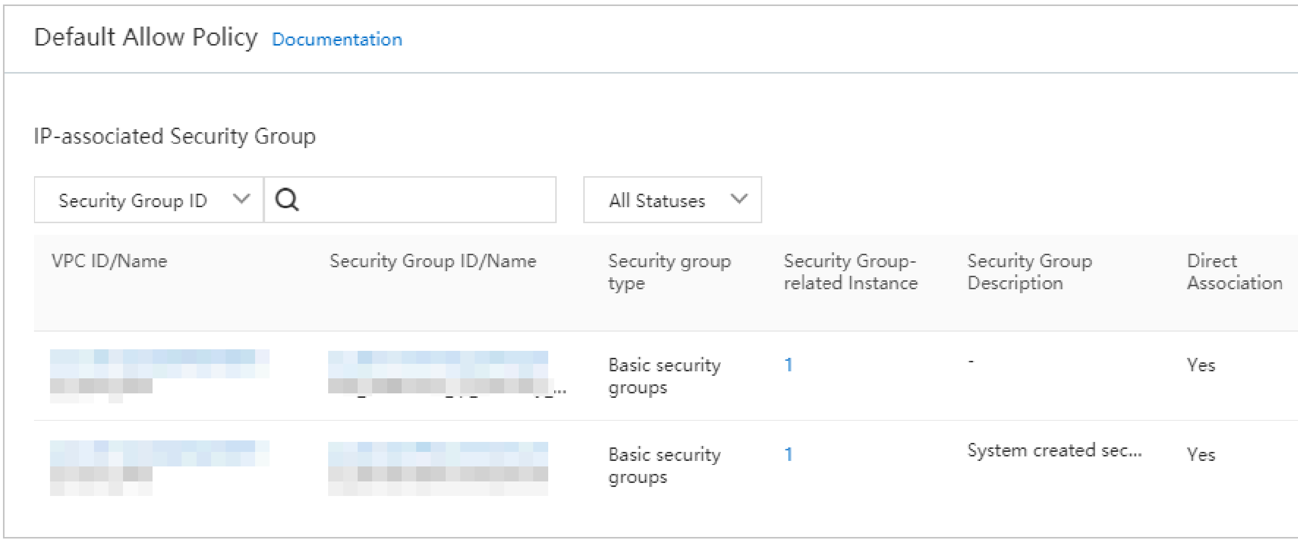
1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, click **Firewall Settings**.
3. On the **Internet Firewall** page, find the security group you want to configure and click **Apply**.



□	IP	Instance ID/Name	Asset Type	Region	Bound Asset	Default Allow Policy	Firewall Status	Actions
□	39[redacted]40	[redacted]	ECS Public IP	[redacted]	[redacted]	Not Applied Apply	Disabled	Enable Firewall
□	1[redacted]8	[redacted]	ECS Public IP	[redacted]	[redacted]	Not Applied Apply	Disabled	Enable Firewall

4. In the **Default Allow Policy** dialog box that appears, find the target security group.

- If the existing rules do not conflict with the default allow policies, click **One-click Apply** and go to step 5.
- If there are configuration conflicts, the **One-click Apply** button is unavailable.



Default Allow Policy Documentation

IP-associated Security Group

Security Group ID | All Statuses

VPC ID/Name	Security Group ID/Name	Security group type	Security Group-related Instance	Security Group Description	Direct Association
[redacted]	[redacted]	Basic security groups	1	-	Yes
[redacted]	[redacted]	Basic security groups	1	System created sec...	Yes

The following table lists solutions to the conflicts.

Scenario	Description	Solution
The conflicts can be resolved.	The security group has rules with priorities greater than or equal to 100, which conflict with the default allow policies. Cloud Firewall increases the priorities of the existing rules to resolve the conflicts.	In the **Default Allow Policy** dialog box, click **Adjust with One Click** and **OK**. Cloud Firewall then adjusts the priorities of the existing rules, and the **One-click Apply** button becomes available in the **Actions** column in the **IP-associated Security Group** list.
The conflicts cannot be resolved.	The security group has rules with priorities greater than or equal to 100, which conflict with the default allow policies. However, Cloud Firewall cannot adjust the priorities of the existing rules to resolve the conflicts.	In this case, the **Adjust with One Click** button is unavailable. Adjust the priorities of the security group rules on the Security Group pages in the ECS console, or contact Cloud Firewall technical support on DingTalk.

5. In the dialog box that appears after you click **One-click Apply**, check the four policies added by Cloud Firewall. Confirm them and click **OK** and **Submit**. Traffic between the security group and the Internet is allowed.

   > **Note:**
   >
   > All traffic between ECS instances in the security group and the Internet is allowed. Therefore, we recommend that you check the public IP addresses of the ECS instances. Make sure that appropriate access control policies are configured for these IP addresses in Cloud Firewall.

   After you click **One-click Apply** for all security groups associated with an IP address, the policies take effect, and the status in the Default Allow Policy becomes **Applied**. Click **View** to view details of the associated security groups.

   > **Notice:**
   >
   > After you apply the default allow policies, take note of the following:
   >
   > - Enable the firewall for the IP address in the Cloud Firewall console and add inbound policies on the **Internet Firewall** tab of the Access Control page.
   > - Configure ECS instances in the security groups to limit the number of IP addresses exposed to the Internet.
   > - If your Cloud Firewall service has expired, the security groups to which you have applied the default allow policies are no longer protected. Renew your Cloud Firewall service after you receive an expiration reminder. Otherwise, re-configure security group rules to protect your ECS instances. After you apply the default allow policies, Cloud Firewall adds four inbound rules to the security groups. The rules continue to work even after your Cloud Firewall service expires. If you do not want to renew your Cloud Firewall service, go to the Security Groups page in the ECS console and delete these rules.

What's next

Check the status of the default allow policies

Navigate to **Firewall Settings** > **Internet Firewall**. Check the status of the default allow policies to determine whether they are applied to the security groups of your ECS instance.

The status may be the following:

- **Applied**: The policies have been applied to all security groups associated with the IP address of the ECS instance. Inbound traffic between all ECS instances in these security groups and the Internet is allowed. If an ECS instance is added to multiple security groups, you must **apply** the default allow policies to all of them so that the policies can take effect.
- **Not Applied**: The policies have not been applied to all security groups associated with the IP address of the ECS instance. Inbound traffic between all ECS instances in these security groups and the Internet is still denied. In this case, there may be configuration conflicts among security group rules, or you have not performed the **One-click Apply** operation.
- **-**: This type of asset does not support default allow policies. Only EIP and ECS Public IP are supported. Other asset types, such as SLB EIP, ENI EIP, NAT EIP are not supported.

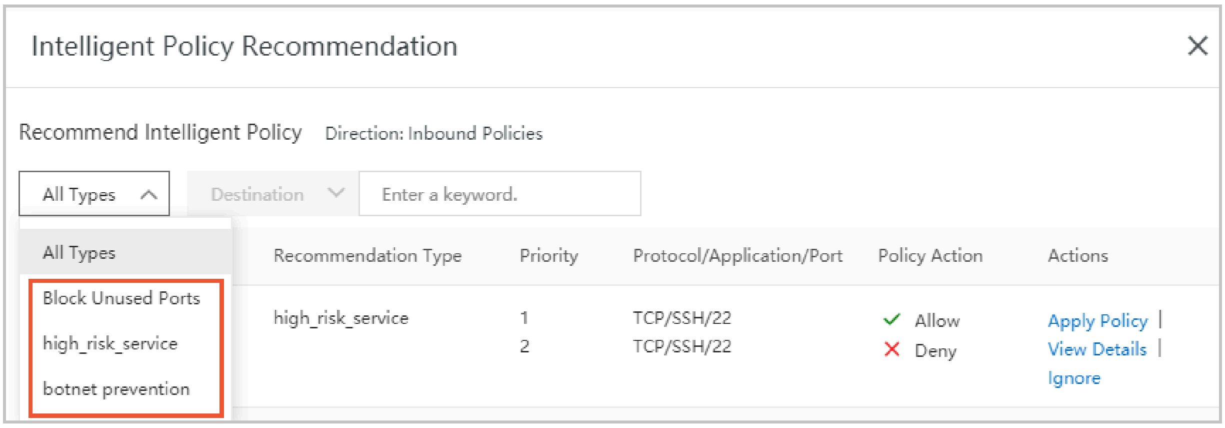
1.8 Intelligent policies

Cloud Firewall uses machine learning to analyze traffic passing through the Internet firewall. Cloud Firewall recommends intelligent policies for destination IP addresses or domain names based on your IP address assets, access history, and external connections. You can apply the intelligent policies based on your business needs. Intelligent policies help you control the exposure of assets to the Internet and block outbound traffic to malicious IP addresses and domain names. This reduces your business risks.

Context

Cloud Firewall automatically generates intelligent policies only for assets protected by the Internet firewall.

Cloud Firewall offers three types of intelligent policies: **high_risk_service**, **Block Unused Ports**, and **botnet prevention**.



Intelligent Policy Recommendation

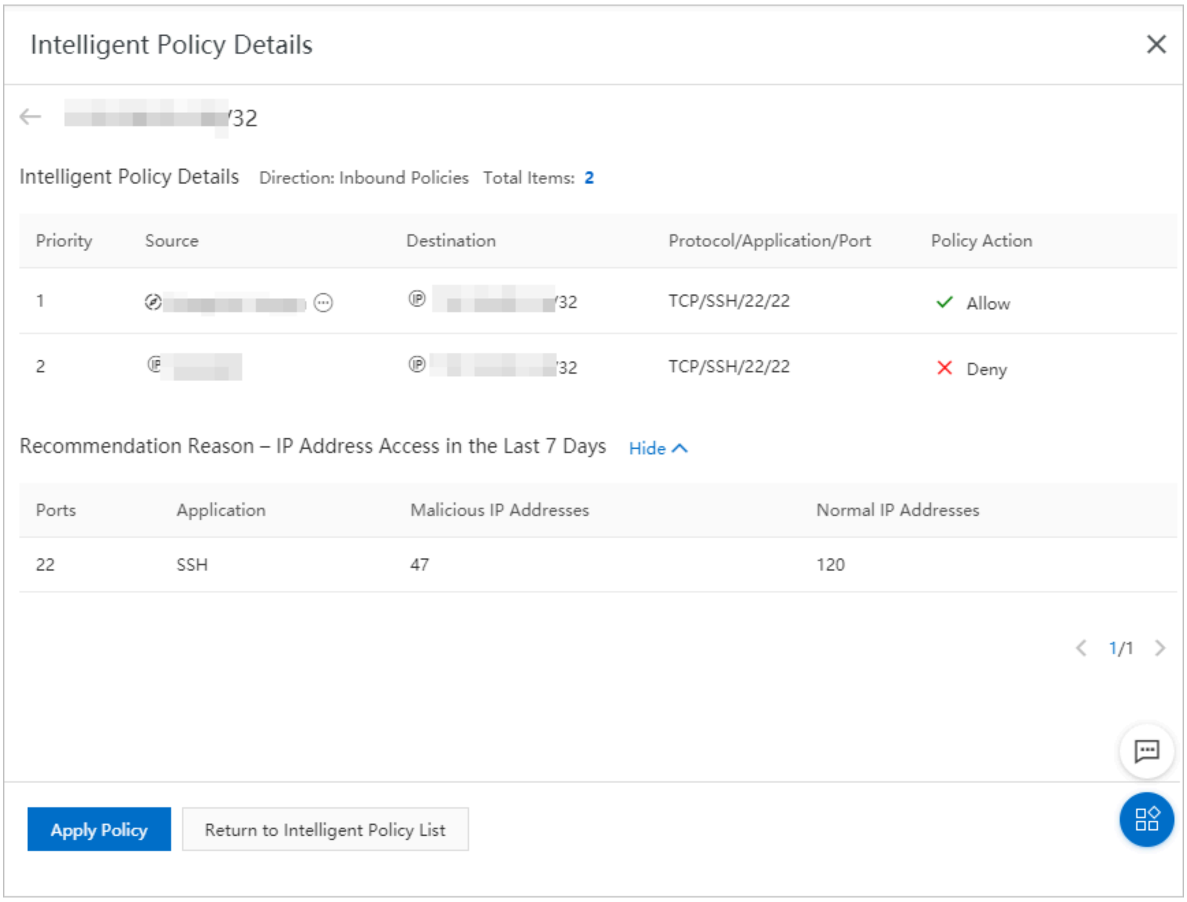
Recommend Intelligent Policy Direction: Inbound Policies

Recommendation Type	Priority	Protocol/Application/Port	Policy Action	Actions
high_risk_service	1 2	TCP/SSH/22 TCP/SSH/22	✓ Allow ✕ Deny	Apply Policy View Details Ignore

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose**Security Policies** > **Access Control**.
3. On the **Internet Firewall** tab, click **Outbound Policies** or **Inbound Policies**.
4. Click **Intelligent Policy**.

   The **Intelligent Policy Recommendation** page appears, which displays the inbound and outbound policies recommended for the public IP address.



Intelligent Policy Details

[redacted]/32

Intelligent Policy Details Direction: Inbound Policies Total Items: 2

Priority	Source	Destination	Protocol/Application/Port	Policy Action
1	[redacted]	[redacted]/32	TCP/SSH/22/22	✓ Allow
2	[redacted]	[redacted]/32	TCP/SSH/22/22	✕ Deny

Recommendation Reason – IP Address Access in the Last 7 Days

Ports	Application	Malicious IP Addresses	Normal IP Addresses
22	SSH	47	120

5. Optional: View policy details.

   a) On the **Intelligent Policy Recommendation** page, find the target policy, and click **View Details** in the Actions column.

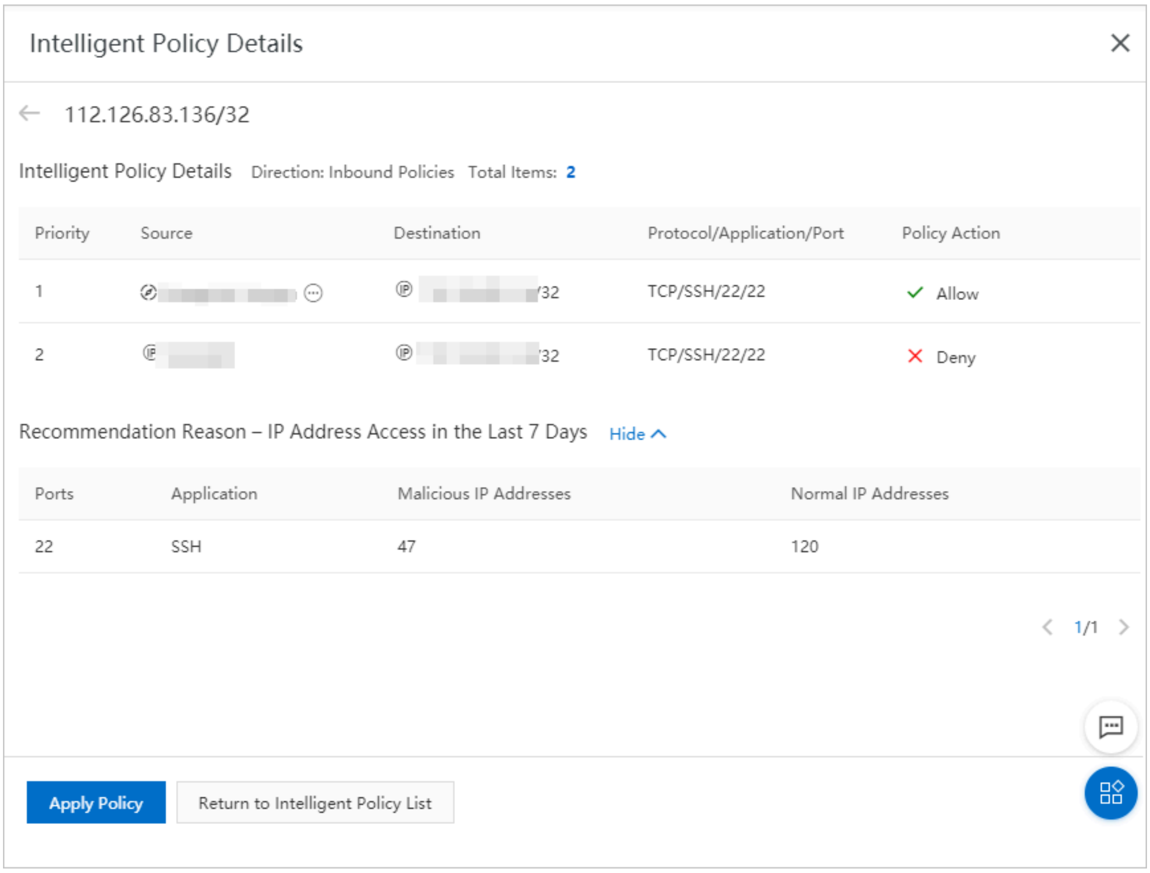
   Note:

If there are too many recommended policies, you can filter them based on **Recommendation Type** and **Destination**.

b) On the **Intelligent Policy Details** page, view all policies recommended by Cloud Firewall for the public IP address and the reasons why these policies are recommended.

Note:

To reduce the exposure of your assets to the Internet, we recommend that you allow access to the open ports that provide services for an open public IP address on the Internet firewall and deny access to other ports.



Intelligent Policy Details

← 112.126.83.136/32

Intelligent Policy Details Direction: Inbound Policies Total Items: 2

Priority	Source	Destination	Protocol/Application/Port	Policy Action
1	[redacted]	[redacted]/32	TCP/SSH/22/22	✓ Allow
2	[redacted]	[redacted]/32	TCP/SSH/22/22	✗ Deny

Recommendation Reason – IP Address Access in the Last 7 Days Hide

Ports	Application	Malicious IP Addresses	Normal IP Addresses
22	SSH	47	120

6. Use one of the following methods to apply an intelligent policy:

Notice:

Before you apply a policy, make sure that you understand its meaning and possible service impacts.

- In the list of recommended intelligent policies, select one or more policies and click **Apply Selected**.
- In the list of recommended intelligent policies, find the target policy and click **Apply Policy** in the Actions column.
- On the **Intelligent Policy Details** page, click **Apply Policy**.

Result

An intelligent policy takes effect after it is applied. On the **Access Control** page, you can view, modify, and delete applied access policies. For more information, see Outbound and inbound traffic control on the Internet firewall.

1.9 Manage address books

An address book is a collection of IP addresses, ports, or domain names. You can configure address books in the Cloud Firewall console to simplify the configuration of access control policies. You can add trusted or untrusted addresses to the same address book. This topic describes how to add, view, and modify an address book.

Context

Cloud Firewall synchronizes malicious IP addresses and domain names detected across Alibaba Cloud to cloud address books. It also adds the back-to-origin addresses of Anti-DDoS and WAF instances under your Alibaba Cloud account to cloud address books. You can configure fine-grained access control policies for these cloud address books.

When you configure access control policies, you can:

- Allow traffic of IP addresses and domain names in trusted address books.
- Deny traffic of IP addresses and domain names in untrusted address books.

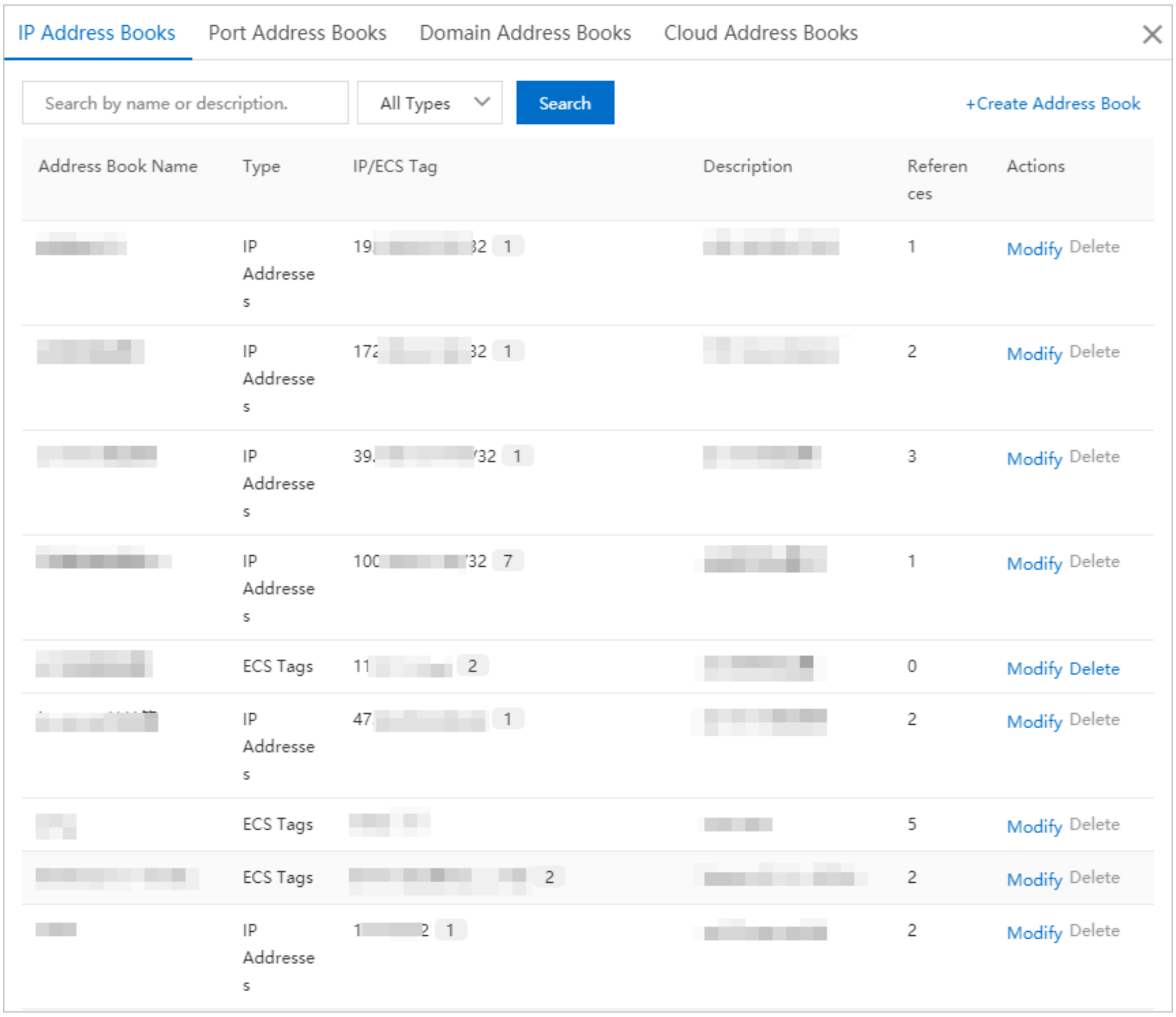
Note:

- One IP address or port number can be added to multiple address books.
- Cloud Firewall provides default global address books that you cannot modify or delete.
- You cannot modify or delete cloud address books.
- If you change the IP addresses, domain names, or ports in an address book, the changes are automatically updated in the policies that reference this address book.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.
3. In the upper-right corner of the **Internet Firewall** tab, click **Address Books**.

4. In the dialog box that appears, manage address books.



Address Book Name	Type	IP/ECS Tag	Description	References	Actions
[redacted]	IP Addresses	[redacted] 1	[redacted]	1	Modify Delete
[redacted]	IP Addresses	[redacted] 1	[redacted]	2	Modify Delete
[redacted]	IP Addresses	[redacted] 1	[redacted]	3	Modify Delete
[redacted]	IP Addresses	[redacted] 7	[redacted]	1	Modify Delete
[redacted]	ECS Tags	[redacted] 2	[redacted]	0	Modify Delete
[redacted]	IP Addresses	[redacted] 1	[redacted]	2	Modify Delete
[redacted]	ECS Tags	[redacted]	[redacted]	5	Modify Delete
[redacted]	ECS Tags	[redacted] 2	[redacted]	2	Modify Delete
[redacted]	IP Addresses	[redacted] 1	[redacted]	2	Modify Delete

You can perform the following operations:

- **Add an address book.**

  You can add both trusted and untrusted address books based on the access control policies you want to configure. Cloud Firewall allows you to add **IP**, **port**, and **domain name** address books. For more information, see Add an address book.

- **Modify an address book.**

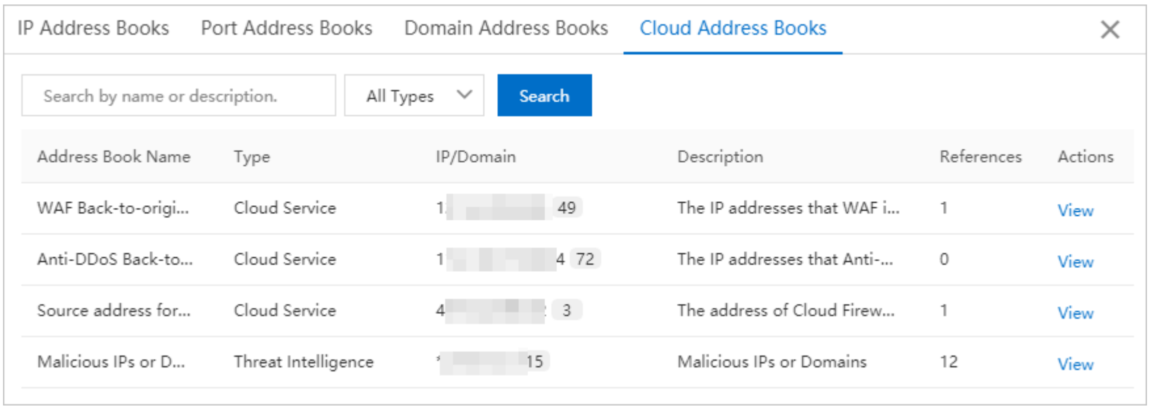
  On the **IP Address Books**, **Port Address Books**, or **Domain Address Books** tab, find the target address book. Click **Modify** in the **Actions** column to modify the address book.

  Note:

You cannot change the **type** or **name** of an address book.

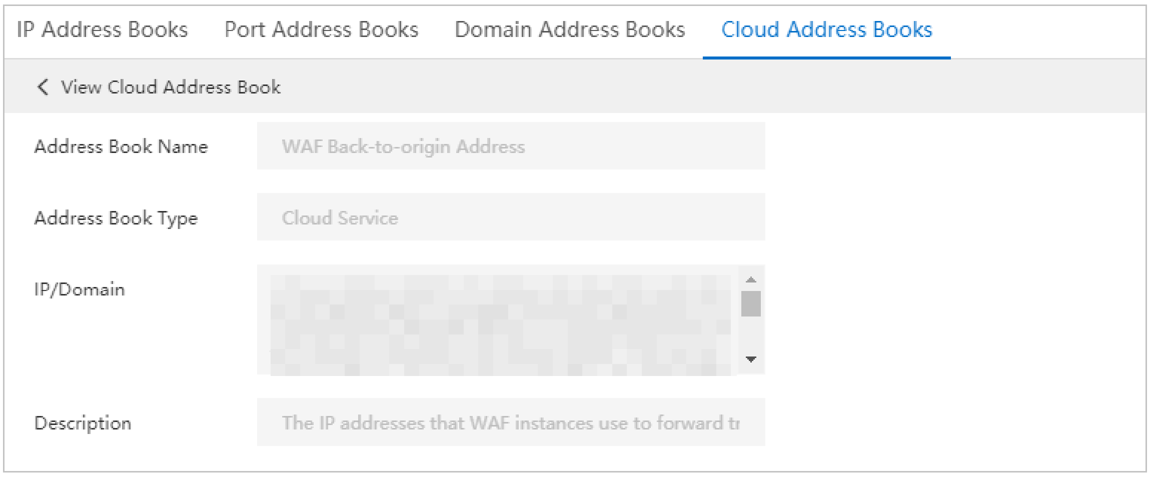
- **View cloud address books.**

  On the **Cloud Address Books** tab, view the names, types, IP addresses (domain names) and their quantity, numbers of references, and descriptions of cloud address books.



Address Book Name	Type	IP/Domain	Description	References	Actions
WAF Back-to-origi...	Cloud Service	1[redacted] 49	The IP addresses that WAF i...	1	View
Anti-DDoS Back-to...	Cloud Service	1[redacted]4 72	The IP addresses that Anti-...	0	View
Source address for...	Cloud Service	4[redacted] 3	The address of Cloud Firew...	1	View
Malicious IPs or D...	Threat Intelligence	[redacted] 15	Malicious IPs or Domains	12	View

  Click **View** in the **Actions** column to view the configuration of a cloud address book.



Address Book Name	WAF Back-to-origin Address
Address Book Type	Cloud Service
IP/Domain	[redacted]
Description	The IP addresses that WAF instances use to forward tı

- **Delete an address book.**

  On the **IP Address Books**, **Port Address Books**, or **Domain Address Books** tab, find the target address book. Click **Delete** in the **Actions** column. In the dialog box that appears, and click **OK**.

Note:

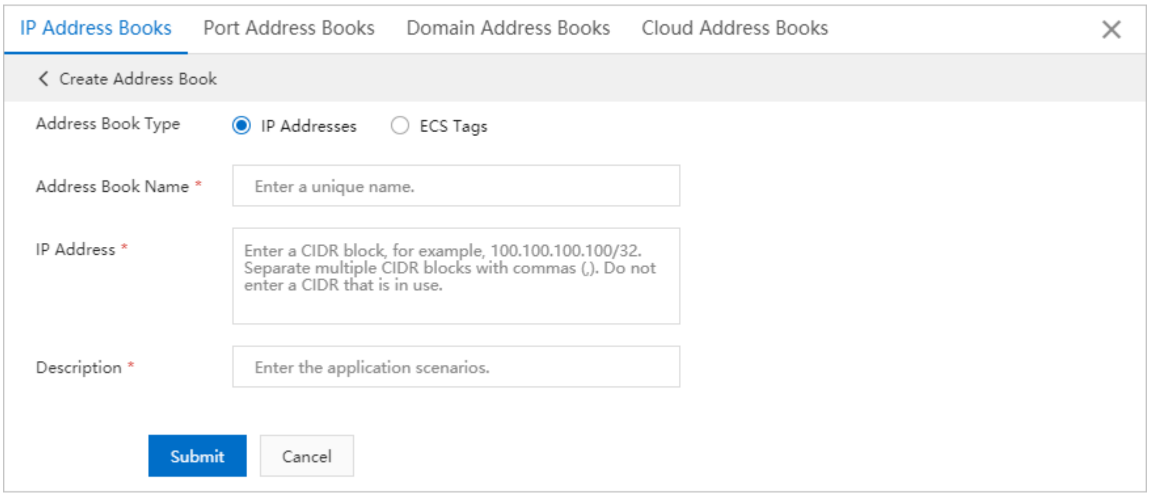
You cannot delete an address book that is being referenced by access control policies.

Add an address book

1. In the upper-right corner of the **IP Address Books**, **Port Address Books**, or **Domain Address Books** tab, click **Create Address Book**.

2. In the **Create Address Book**, **Create Port Address Book**, or **Create Domain Address Book** dialog box, configure the following parameters.

- **IP address book**



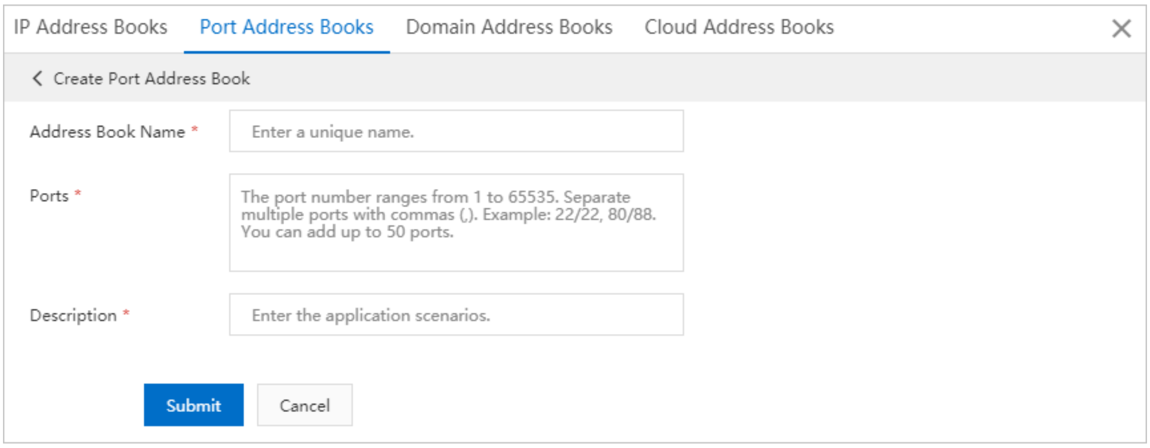
Address Book Type ● IP Addresses ○ ECS Tags

Address Book Name * Enter a unique name.

IP Address * Enter a CIDR block, for example, 100.100.100.100/32. Separate multiple CIDR blocks with commas (,). Do not enter a CIDR that is in use.

Description * Enter the application scenarios.

- **Port address book**

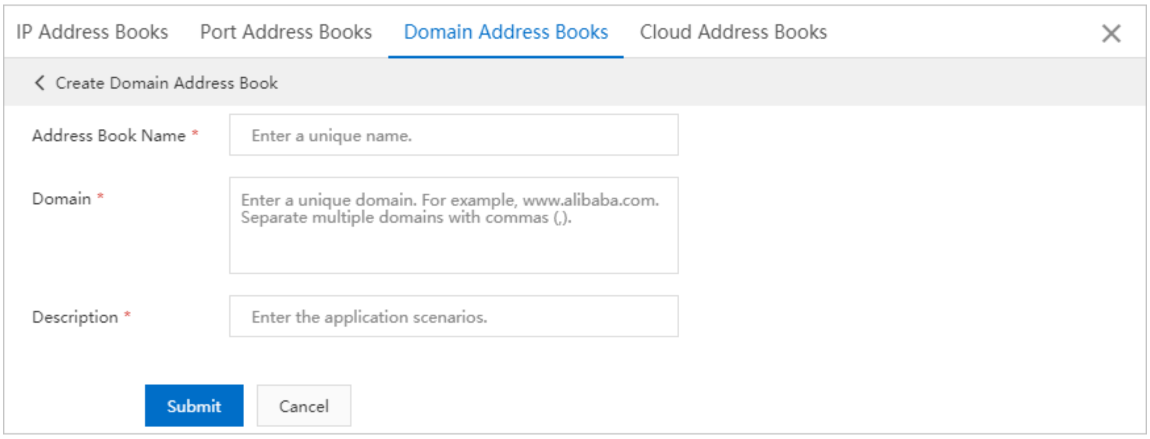


Address Book Name * Enter a unique name.

Ports * The port number ranges from 1 to 65535. Separate multiple ports with commas (,). Example: 22/22, 80/88. You can add up to 50 ports.

Description * Enter the application scenarios.

- **Domain address book**



Address Book Name * Enter a unique name.

Domain * Enter a unique domain. For example, www.alibaba.com. Separate multiple domains with commas (,).

Description * Enter the application scenarios.

Type	Parameter	Description
IP address book	Address Book Type	Select the type of the IP address book, which can be the following: • **IP Addresses** • **ECS Tags**
	IP Address	Enter one or more CIDR blocks. **Note:** Separate CIDR blocks with commas (,). This parameter is available when you set **Address Book Type** to **IP Addresses**.
	Add ECS of Specified Tags	Automatically add ECS instances that have specific tags to this address book. This function is enabled automatically and cannot be disabled. **Note:** This parameter is available when you set **Address Book Type** to **ECS Tags**.
	ECS Tags	Select ECS tags created under your Alibaba Cloud account. Cloud Firewall automatically adds public IP addresses of ECS instances that have the tags you specify to an address book. Click **Add Tag** to specify more ECS tags. After you select an ECS tag, information about the ECS instance is displayed under **ECS Tags**, including the VPC name and IP address.
Port address book	Ports	Enter one or more port ranges and separate them with commas (,).
Domain address book	Domain	Enter one or more domain names and separate them with commas (,). Each domain name must be unique.
Common parameters	Address Book Name	Enter a name for the address book. You can use the name to identify the address book.
	Description	Enter an application scenario for the address book.

3. Click **Submit**.

   The new address book is displayed in the list. You can view its name, number of references, and description, and delete or modify it.

References

Outbound and inbound traffic control on the Internet firewall

Access control on VPC firewalls

Intrusion prevention policies

1.10 Change the priority of an access control policy

Each access control policy configured in Cloud Firewall is assigned a default priority. You can click **Move** in the Actions column to change the priority of a policy.

Context

The priorities determine the order in which the policies take effect. Each access control policy has a unique priority. Number 1 indicates the highest priority.

A larger number indicates a lower priority.

The maximum number of policies allowed depends on the edition of Cloud Firewall. Therefore, the priority range is also different in each edition.

- In the Pro Edition, you can configure up to 1,000 access control policies. The priority ranges from 1 to 1000.
- In the Enterprise Edition, you can configure up to 2,000 policies. The priority ranges from 1 to 2000.
- In the Flagship Edition, you can configure up to 5,000 policies. The priority ranges from 1 to 5000.

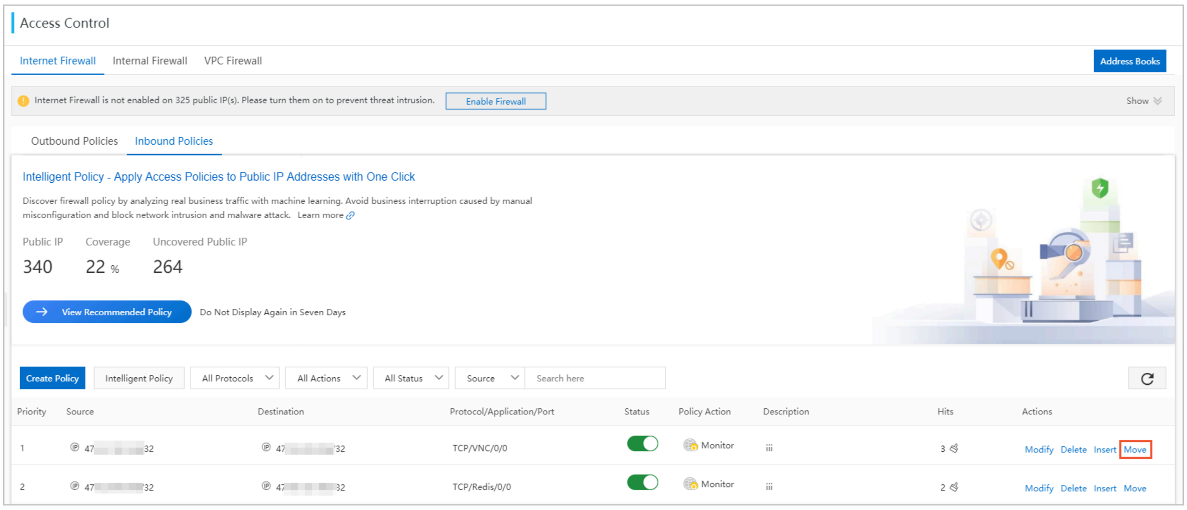
Note:

By default, a new policy is assigned the lowest priority.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.

3. On the **Internet Firewall** tab, click **Outbound Policies** or **Inbound Policies**. Find the policy whose priority you want to change and click **Move** in the **Actions** column.



Access Control

Internet Firewall Internal Firewall VPC Firewall Address Books

Internet Firewall is not enabled on 325 public IP(s). Please turn them on to prevent threat intrusion. Enable Firewall Show

Outbound Policies Inbound Policies

Intelligent Policy - Apply Access Policies to Public IP Addresses with One Click

Discover firewall policy by analyzing real business traffic with machine learning. Avoid business interruption caused by manual misconfiguration and block network intrusion and malware attack. Learn more

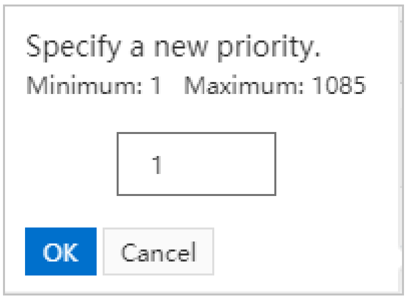
Public IP	Coverage	Uncovered Public IP
340	22 %	264

View Recommended Policy Do Not Display Again in Seven Days

Create Policy Intelligent Policy All Protocols All Actions All Status Source Search here

Priority	Source	Destination	Protocol/Application/Port	Status	Policy Action	Description	Hits	Actions
1	47[redacted]32	47[redacted]32	TCP/VNC/0/0		Monitor	iii	3	Modify Delete Insert Move
2	47[redacted]32	47[redacted]32	TCP/Redis/0/0		Monitor	iii	2	Modify Delete Insert Move

4. In the box that appears, enter a new priority.



Specify a new priority.
Minimum: 1 Maximum: 1085

1

OK Cancel

5. Click **OK**.

Note:

After you change the priority of a policy, the priorities of policies with lower priorities decrease.

2 Intrusion prevention

2.1 Intrusion prevention policies

Cloud Firewall uses a built-in threat detection engine to defend against intrusions and common cyber attacks. It provides virtual patches against vulnerabilities to intelligently block intrusion attempts.

Context

On the Intrusion Prevention page in the Cloud Firewall console, you can configure the mode of the threat detection engine, basic protection, and virtual patches to accurately identify and block intrusions.

Modes of the threat detection engine

The threat detection engine supports the following modes:

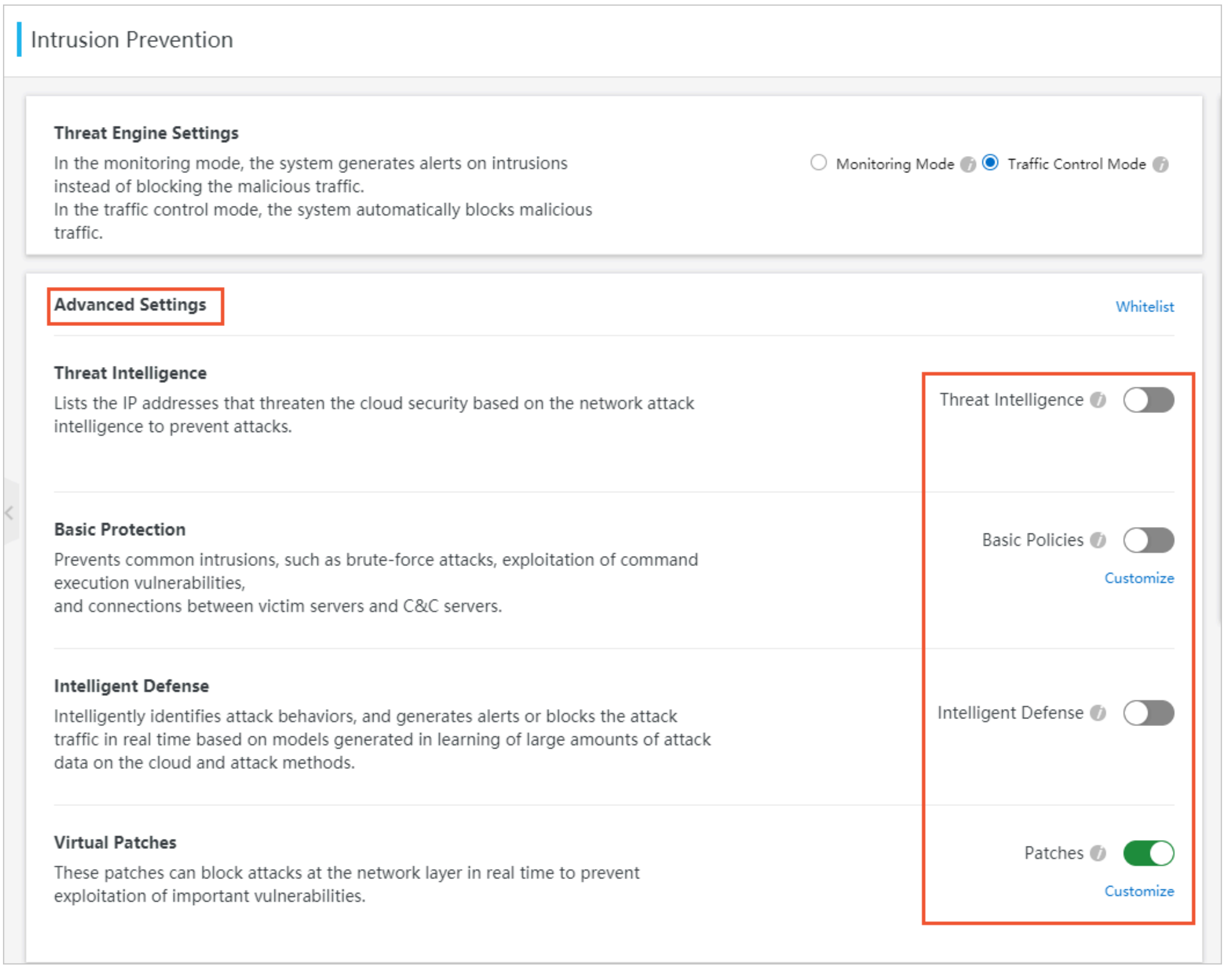
- **Monitoring Mode**: The engine only sends alerts after it detects malicious traffic.

  > **Note:**
  > **Monitoring Mode** is selected by default after you activate Cloud Firewall.

- **Traffic Control Mode**: The engine blocks malicious traffic to prevent intrusions.

Advanced settings

In the **Advanced Settings** section, you can configure a whitelist, threat intelligence, intelligent defense, basic protection, and virtual patches to achieve precise intrusion prevention.



Intrusion Prevention

Threat Engine Settings

In the monitoring mode, the system generates alerts on intrusions instead of blocking the malicious traffic.
In the traffic control mode, the system automatically blocks malicious traffic.

○ Monitoring Mode ● Traffic Control Mode

Advanced Settings

Whitelist

Threat Intelligence

Lists the IP addresses that threaten the cloud security based on the network attack intelligence to prevent attacks.

Threat Intelligence: off

Basic Protection

Prevents common intrusions, such as brute-force attacks, exploitation of command execution vulnerabilities,
and connections between victim servers and C&C servers.

Basic Policies: off
Customize

Intelligent Defense

Intelligently identifies attack behaviors, and generates alerts or blocks the attack traffic in real time based on models generated in learning of large amounts of attack data on the cloud and attack methods.

Intelligent Defense: off

Virtual Patches

These patches can block attacks at the network layer in real time to prevent exploitation of important vulnerabilities.

Patches: on
Customize

- Whitelist

  Cloud Firewall trusts the source and destination IP addresses in a whitelist and does not block their traffic.

- Threat intelligence

  The threat intelligence feature synchronizes malicious IP addresses detected across Alibaba Cloud to Cloud Firewall. Malicious IP addresses include IP addresses that initiate malicious traffic, scanning, or brute-force attacks. This feature provides up-to-date information about threat sources.

- Basic protection

  The basic protection feature defends your network against common intrusions, such as brute-force attacks and command execution vulnerabilities, and manages connections from infected hosts to a command-and-control (C&C) server.

- Intelligent defense

  The intelligent defense feature learns from a massive amount of data about attacks on the cloud. It identifies attacks and generates alerts in real time.

- Virtual patches

  Virtual patches are installation-free. You can use them to defend against high-risk vulnerabilities.

Procedure

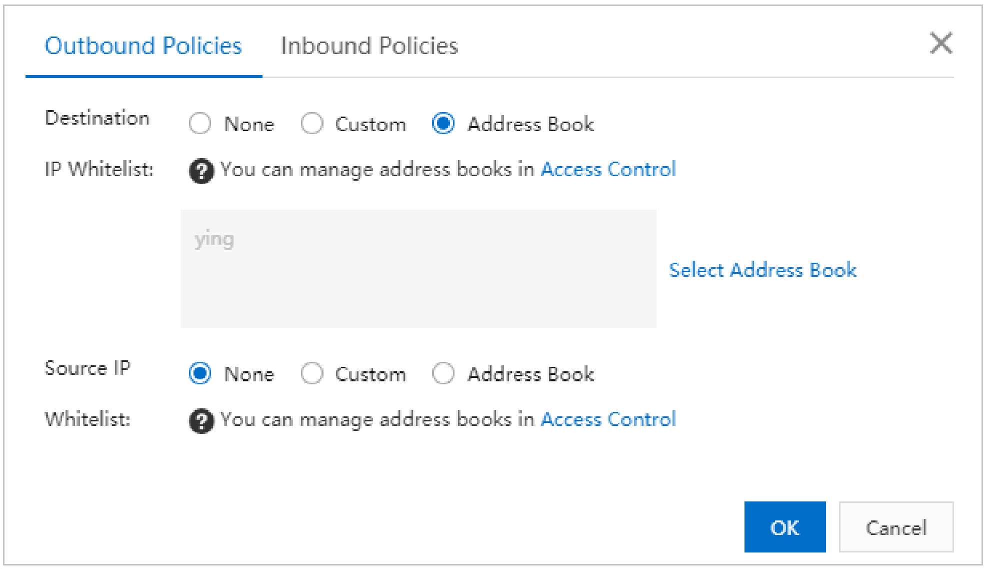
1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Intrusion Prevention**.
3. On the **Intrusion Prevention** page, perform the following operations to protect your network:
   - In the **Threat Engine Settings** section, select **Monitoring Mode** or **Traffic Control Mode**.

     Note:

Monitoring Mode is selected by default. In this mode, Cloud Firewall only sends alerts after it detects malicious traffic (but does not block it). After you select **Traffic Control Mode**, Cloud Firewall blocks malicious traffic it detects.

- In the **Advanced Settings** section, click **Whitelist** to add trusted IP addresses to a whitelist. Cloud Firewall allows traffic of IP addresses in the whitelist.

  You can add the trusted source IP addresses, destination IP addresses, or address books of both inbound and outbound traffic to the whitelist.



Destination IP Whitelist: ○ None ○ Custom ● Address Book

You can manage address books in Access Control

ying

Source IP Whitelist: ● None ○ Custom ○ Address Book

You can manage address books in Access Control

- Configure **Threat Intelligence**. This feature scans for signs of threats and blocks traffic to C&C servers.

Note:

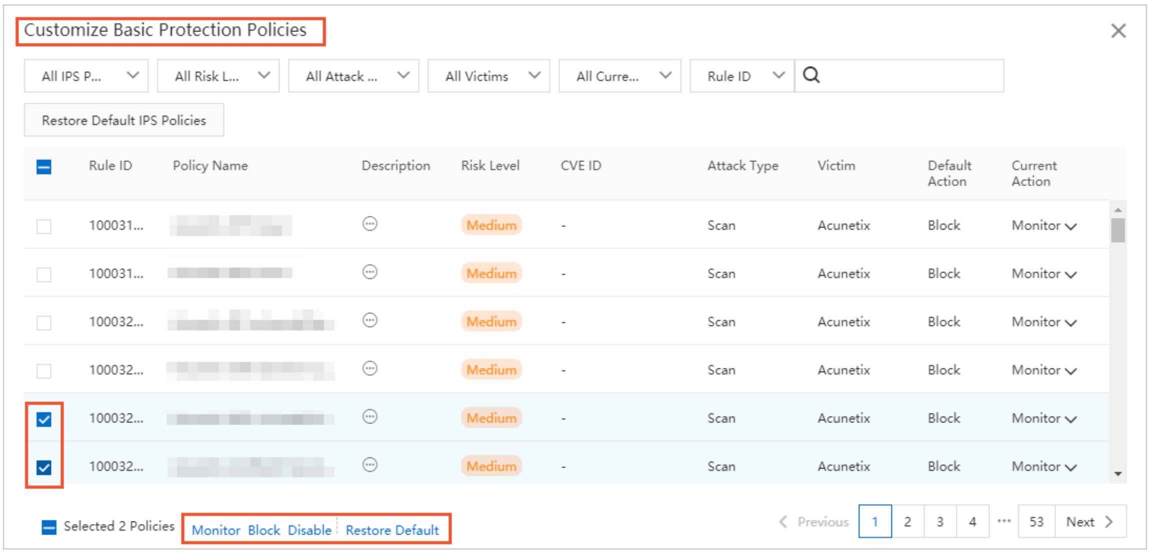
We recommend that you enable threat intelligence.

- Configure **Basic Protection**. This feature defends against common intrusions such as brute-force attacks and command execution vulnerabilities.

Note:

We recommend that you enable basic protection.

In the **Basic Protection** section, click **Customize**. In the **Customize Basic Protection Policies** dialog box that appears, configure one or more basic protection policies.



Customize Basic Protection Policies

☐	Rule ID	Policy Name	Description	Risk Level	CVE ID	Attack Type	Victim	Default Action	Current Action
☐	100031...	[redacted]	⊙	Medium	-	Scan	Acunetix	Block	Monitor
☐	100031...	[redacted]	⊙	Medium	-	Scan	Acunetix	Block	Monitor
☐	100032...	[redacted]	⊙	Medium	-	Scan	Acunetix	Block	Monitor
☐	100032...	[redacted]	⊙	Medium	-	Scan	Acunetix	Block	Monitor
☑	100032...	[redacted]	⊙	Medium	-	Scan	Acunetix	Block	Monitor
☑	100032...	[redacted]	⊙	Medium	-	Scan	Acunetix	Block	Monitor

Selected 2 Policies
Monitor Block Disable Restore Default
Previous 1 2 3 4 ... 53 Next

- Configure **Intelligent Defense**. This feature learns from a massive amount of data about attacks on the cloud. It identifies attacks and generates alerts in real time.

Note:

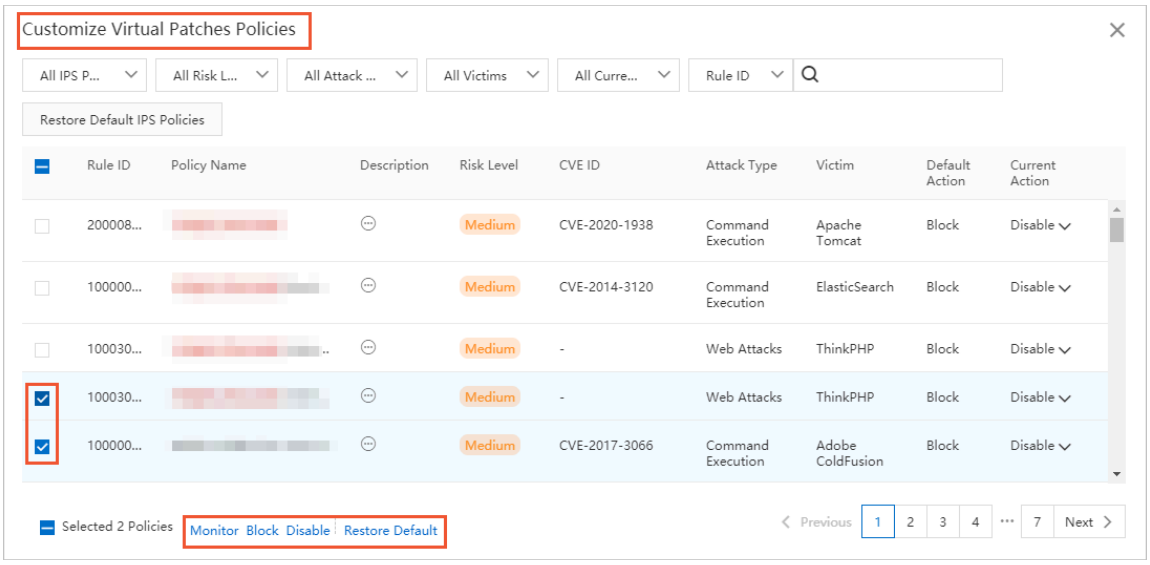
We recommend that you enable intelligent defense.

- Configure **Virtual Patches**. After this feature is enabled, Cloud Firewall provides installation-free patches against common vulnerabilities in real time.

Note:

If this feature is disabled, Cloud Firewall does not automatically update patches for your assets. We recommend that you enable all virtual patches.

In the **Virtual Patches** section, click **Customize**. In the **Customize Virtual Patches Policies** dialog box that appears, configure one or more basic virtual patch policies.



Customize Virtual Patches Policies

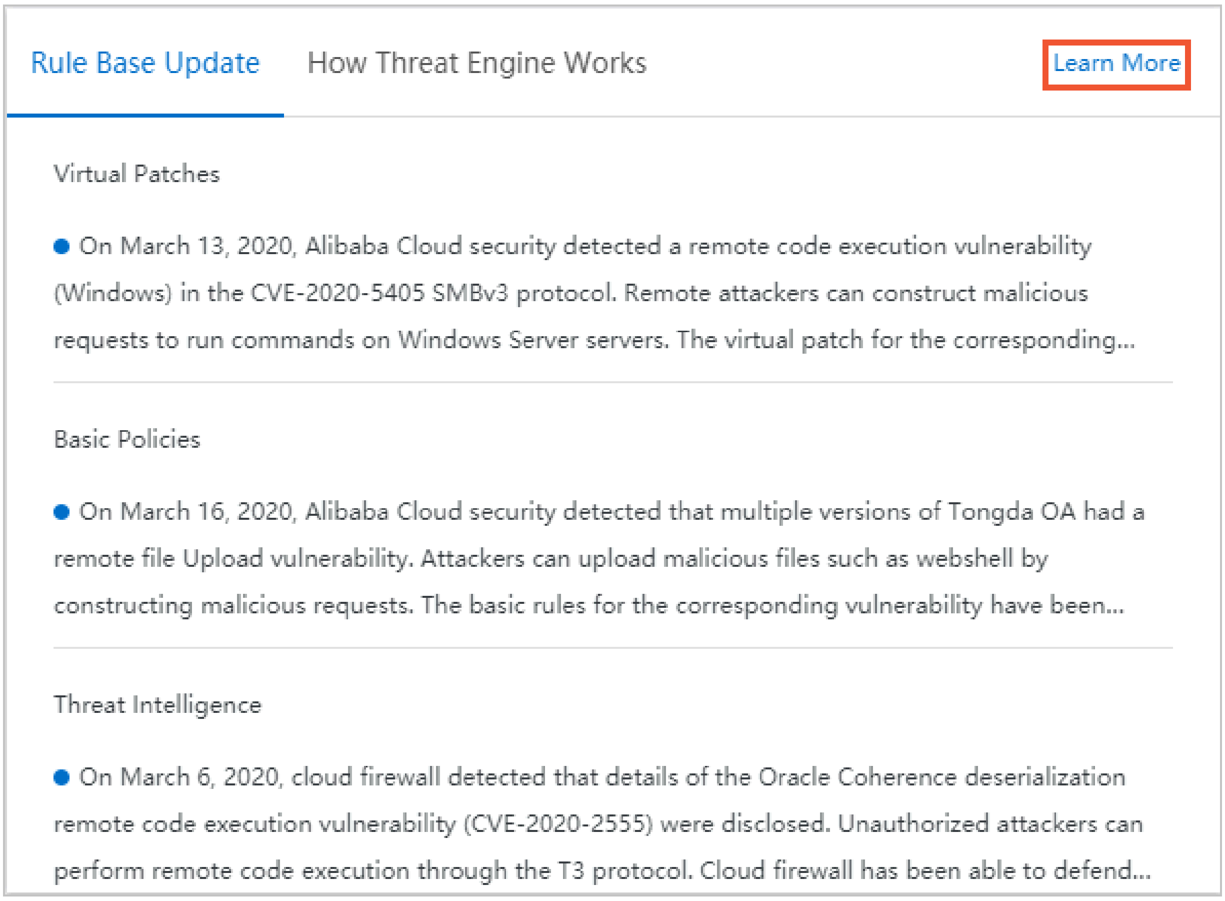
	Rule ID	Policy Name	Description	Risk Level	CVE ID	Attack Type	Victim	Default Action	Current Action
□	200008...	[redacted]	⋯	Medium	CVE-2020-1938	Command Execution	Apache Tomcat	Block	Disable
□	100000...	[redacted]	⋯	Medium	CVE-2014-3120	Command Execution	ElasticSearch	Block	Disable
□	100030...	[redacted]	⋯	Medium	-	Web Attacks	ThinkPHP	Block	Disable
☑	100030...	[redacted]	⋯	Medium	-	Web Attacks	ThinkPHP	Block	Disable
☑	100000...	[redacted]	⋯	Medium	CVE-2017-3066	Command Execution	Adobe ColdFusion	Block	Disable

Selected 2 Policies
Monitor Block Disable Restore Default
Previous 1 2 3 4 ⋯ 7 Next

Rule base update

The **Rule Base Update** tab displays information about the updates of security intelligence, virtual patches, and basic IPS policies.

In the upper-right corner of the **Rule Base Update** tab, click **Learn More** to view all updates.



Virtual Patches

- On March 13, 2020, Alibaba Cloud security detected a remote code execution vulnerability (Windows) in the CVE-2020-5405 SMBv3 protocol. Remote attackers can construct malicious requests to run commands on Windows Server servers. The virtual patch for the corresponding...

Basic Policies

- On March 16, 2020, Alibaba Cloud security detected that multiple versions of Tongda OA had a remote file Upload vulnerability. Attackers can upload malicious files such as webshell by constructing malicious requests. The basic rules for the corresponding vulnerability have been...

Threat Intelligence

- On March 6, 2020, cloud firewall detected that details of the Oracle Coherence deserialization remote code execution vulnerability (CVE-2020-2555) were disclosed. Unauthorized attackers can perform remote code execution through the T3 protocol. Cloud firewall has been able to defend...