Alibaba Cloud
Cloud Firewall

Security Policy

Issue: 20190920

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 individuals 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

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:

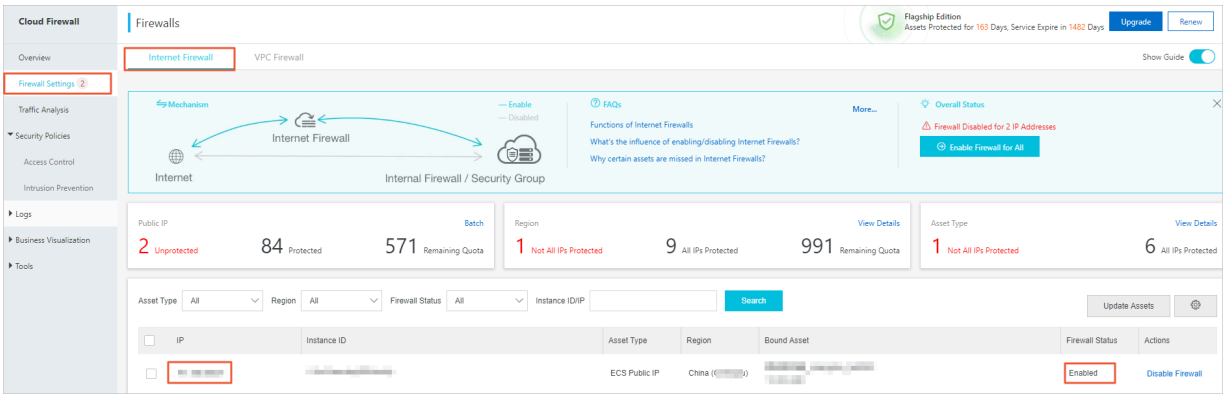
If you want to create more policies than allowed, we recommend that you delete unnecessary policies or submit a ticket for technical support.

2 Access control over the Internet firewall

Cloud Firewall supports access control over the Internet firewall. You can configure policies to control the traffic between the Internet and your servers.

Prerequisites

To make sure that the Internal firewall policies take effect on an instance, you must enable Internet firewall for this instance.

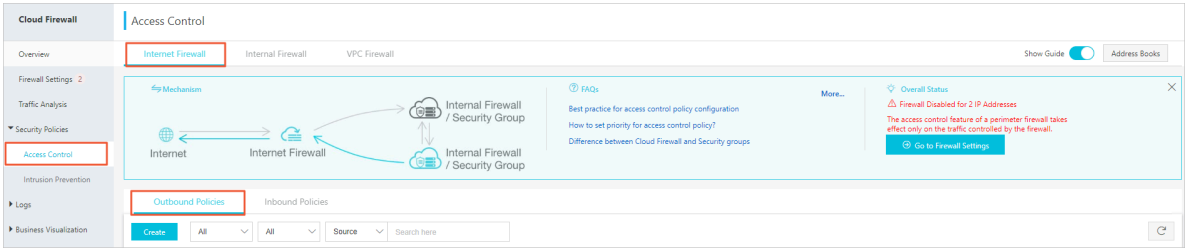


Context

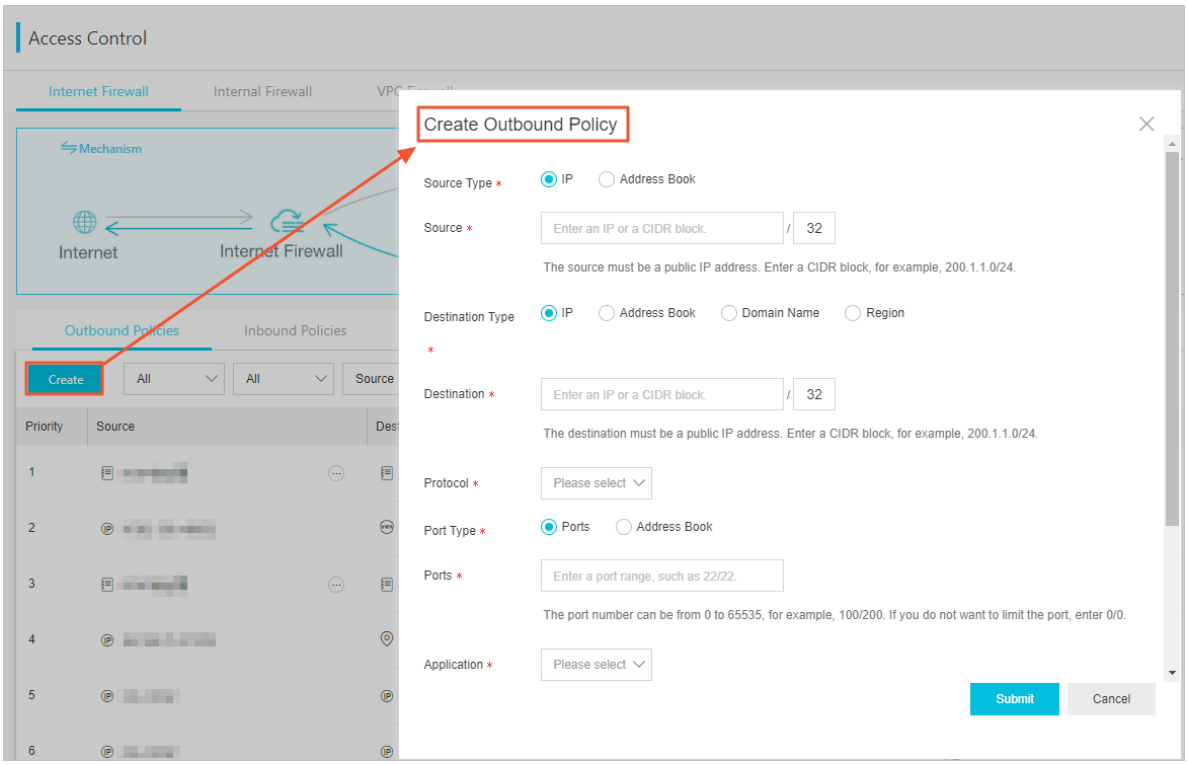
Internet firewall allows you to configure both outbound and inbound access policies.

Outbound traffic control

1. Log on to the Cloud Firewall console.
2. In the left pane, choose Security Policies > Access Control > Internet Firewall > Outbound Policies.



3. In the upper-left corner of the Outbound Policies tab page, click Create. The Create Outbound Policy dialog box is displayed.



4. Create an outbound access control policy.

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

      A. Configure the rule parameters according to the steps in the table.

Steps	Parameter name	Parameter configuration
1	Source Type	Select `IP` or `Address Book`. · IP: You can specify one CIDR block. · Address Book: You can select from the IP address books that you have configured. An IP address book is a set of CIDR blocks. This allows you to manage multiple IP addresses in policy configuration.

Steps	Parameter name	Parameter configuration
2	Source	The source address of the traffic. In this policy, set Source to internal IP addresses that can access the Internet. · If the source type is IP, you must set the source to a CIDR block. For example, 1.1.1.1/32. · If the source type is `Address Book`, click Select Address Book, and select an IP address book as the source.
3	Destination Type	You can select `IP`, `Address Book`, `Domain Name`, or `Region`. **Note:** If you select `Region`, you can select a destination from the seven continents and all regions in China, including 23 provinces, four municipalities, five autonomous regions, and two special administrative regions.
4	Destination	The destination of the traffic. In this policy, set Destination to a public IP address that can be accessed by an internal IP address.
5	Protocol	The protocol of the traffic. If you are not sure which protocol is used, select `ANY`.
6	Port Type	Select `Ports` or `Address Book`. · Ports: You can specify a port number or a port range. · Address Book: You can select from the port address books that you have configured. A port address book contains multiple ports.
7	Ports	The ports to which you want to apply this policy. If Port Type is Ports, specify a port number. You can also click Select Address Book to select a port address book that you have configured.

Steps	Parameter name	Parameter configuration
8	Application	The application where the traffic is bound to. Note: If Destination Type is set to `Domain Name`, you can set Application to `HTTP`, `HTTPS`, `SMTP`, or `SMTPS`.
9	Policy Action	Indicates whether Internet firewall allows or denies the traffic. Select `Allow` for this policy.
10	Description	Enter a description of the policy so that you can quickly distinguish the purpose of each policy when you view it later.
11	Priority	Select the priority of this policy, the default is the `Lowest`.

B. Click Submit.

Note:
The latest policy is displayed in the last row on the last page of the policy list.

b. In the second outbound policy, deny the traffic from all internal IP addresses to the Internet.

Set Source to `0.0.0.0/0` and Policy Action to Deny to prevent all unauthorized access activities. Configure the other parameters by referring to the preceding parameter descriptions.

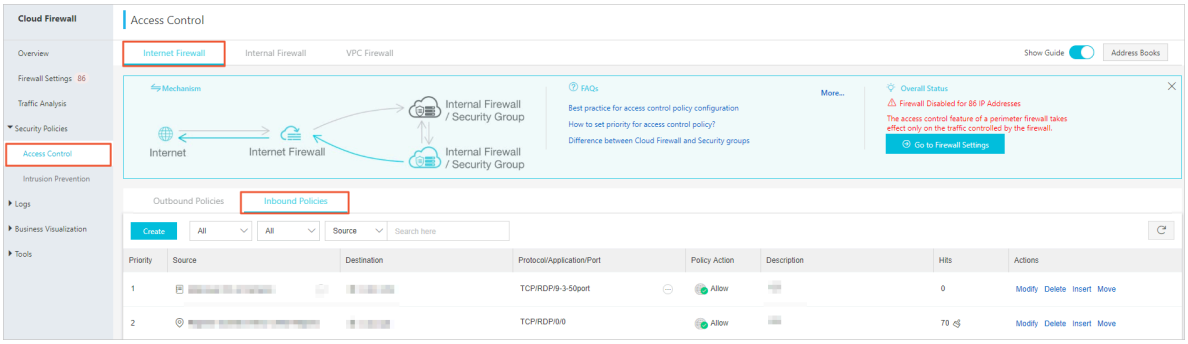
c. Make sure that the priority of the allow policy on the trusted IP addresses is higher than that of the deny policy.

Note:
Cloud Firewall assigns priorities to access control policies based on the policy creation time. A new policy has a lower priority than all existing policies. For more information about the policy priority, see #unique_5.

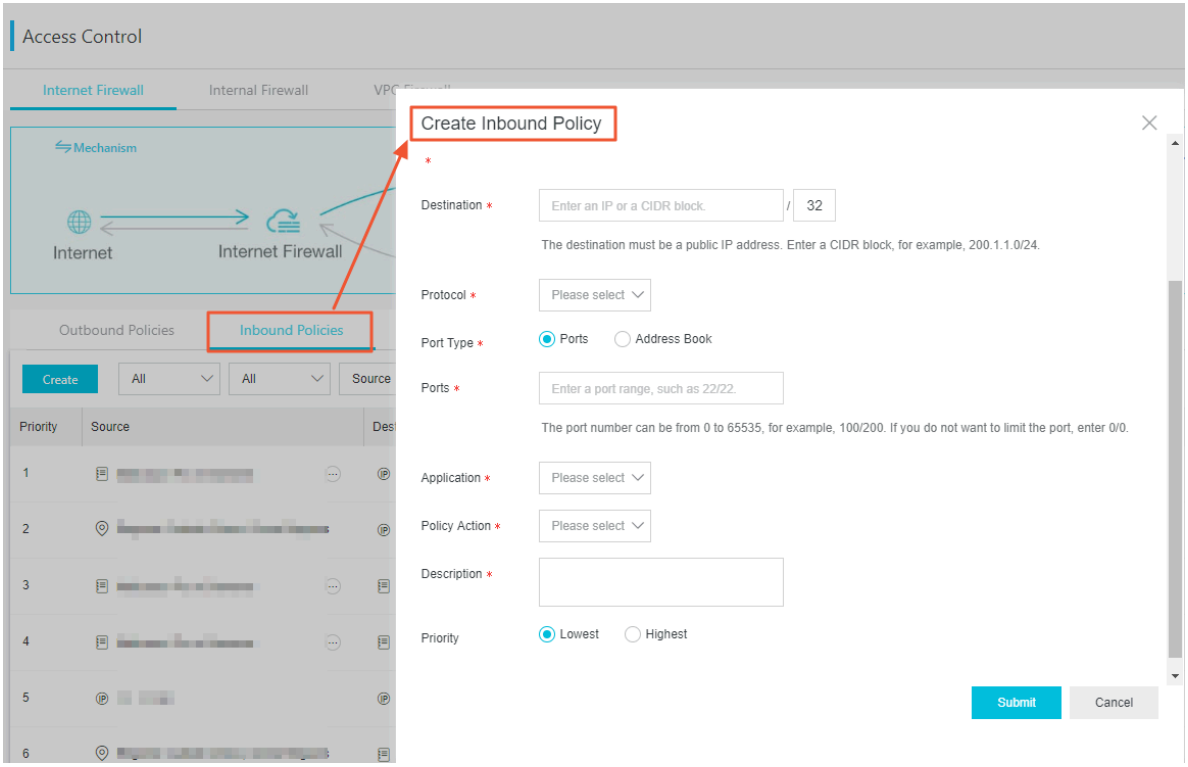
For more information about policy configuration parameters, seeParameters of an access control policy.

Inbound traffic control

1. Log on to the Cloud Firewall console.
2. In the left pane, choose Security Policies > Access Control > Internet Firewall > Inbound Policies.



3. In the upper-left corner of the Inbound Policies tab page, click Create. The Create Inbound Policy dialog box is displayed.



4. In the first inbound policy, allow traffic from trusted external IP addresses.

   Set Source to a trusted CIDR block or an IP `Address Book` that you have configured. Set Policy Action to Allow. For more information about configuring 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 a 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 the other external IP addresses to the internal network.

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

6. Make sure 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 newly created policy takes effect immediately by default. However, if the policy parameters are invalid or the Internet firewall is disabled, the policy may not take effect.

In the policy list, click the number in the Hits column of a policy. The Traffic Logs page is displayed. If the name of the policy is displayed in the Policy Name column on the Traffic Logs page, this policy has taken effect.

Note:
After you delete a policy, the allow or deny policy that you have configured becomes invalid. Exercise caution.

Parameters of 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 an existing address book. You can add multiple IP addresses to an address book to simplify policy configuration.

Parameter	Description
Source	The source IP address or CIDR block of the traffic.  Note: You can specify only one CIDR block, for example, 1.1.1.1/32. If you set Source Type to Address Book, select an exiting address book as the source.  Note: · In an outbound policy, the source address book can be an IP address book only, and the destination address book can be an IP address book, a domain address book, or a cloud address book. · In an inbound policy, the source address book can be an IP address book or a cloud address book, and the destination address book can be an IP address book only.
Destination type	· IP: Set the destination to an IP address. · Address Book: Set the destination to an address book. · Domain Name: Set the destination to a domain name. You can specify a wildcard domain, for example, `*. a . com` .  Note: - Only in an outbound policy can you set the destination type to IP, domain name, or region. - If an HTTP header does not contain the host field or an HTTPS request does not contain Server Name Indication (SNI), the policy action is set to Allow by default.

Parameter	Description
Destination	Set the destination to a CIDR block. If you set the destination type to domain name, set the destination to a domain or a wildcard domain. Note: · In an outbound policy, the source address book can be an IP address book only, and the destination address book can be an IP address book, a domain address book, or a cloud address book. · In an inbound policy, the source address book can be an IP address book or a cloud address book, and the destination address book can be an IP address book only.
Protocol	· ANY: Indicates any protocol. · TCP · UDP · ICMP
Destination ports	You can specify a port range. 0/0 indicates any port. Note: If you set the protocol to ICMP, the destination port configuration is not required. If you set the protocol to `ANY`, the destination port configuration does not take effect on ICMP traffic.
Application	You can set the application to ANY, HTTP, HTTPS, Mamcache, MongoDB, MQTT, MySQL, RDP, Redis, SMTP, SMTPS, SSH, or VNC. If Protocol is set to TCP, multiple applications are available. Otherwise, you can set the application to `ANY` only. Note: The identification application relies on the application message characteristics (the protocol identification is not based on the port); when the application identification fails, the session traffic is `Allow .`

Parameter	Description
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 monitoring the traffic for a period of time, you can change the policy action to Allow or Deny.
Description	A description or note about this policy. Enter a description of the policy so that you can distinguish the policies later.
Priority	Set the priority of the access control policy. The default priority is the `Lowest` .

3 Access control over the internal firewall between ECS instances

Cloud Firewall supports access control over the internal firewall. You can configure access control policies to restrict unauthorized access between ECS instances.

The internal firewall integrates the features of the ECS security group module. The access control policies that you configure on the Internal Firewall page in Cloud Firewall are automatically synchronized to the security group module of ECS.

 Note:
To view the policy groups that you have configured on the Internal Firewall page, specify Source as `Custom` , and click Search.

Benefits of internal firewall

- You can publish multiple policies at the same time.
- You can create policy groups based on templates.

  The templates are as follows:

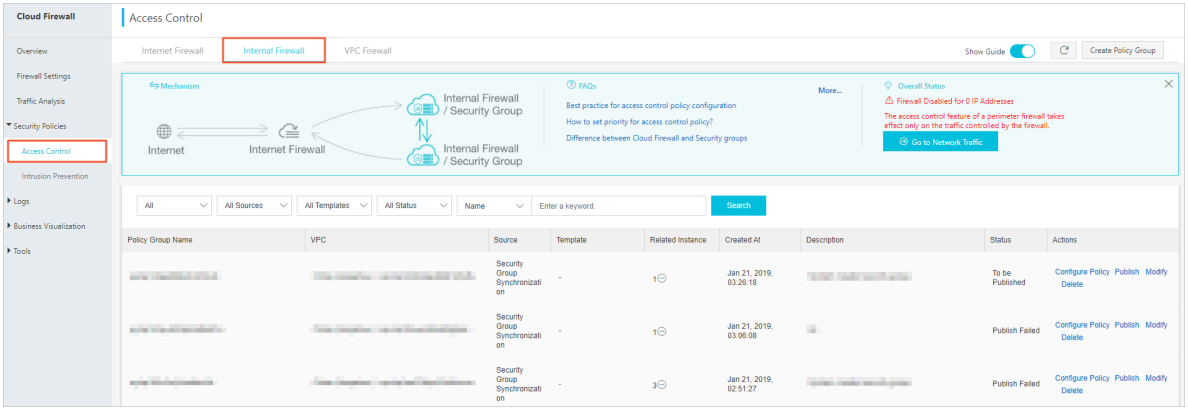
  - `default - accept - login` : Allow all inbound traffic that passes through port 22 and port 3389 by default.
  - `default - drop - all` : Deny all traffic in the policy group by default.
  - `default - accept - all` : Allow all traffic in the policy group by default.
- Security groups can be automatically created based on application groups.

 Note:
By default, you can create up to 100 policy groups and 100 policies between ECS instances. 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. If you want to create more policies than allowed, we recommend that you delete unnecessary policies or submit a ticket for technical support.

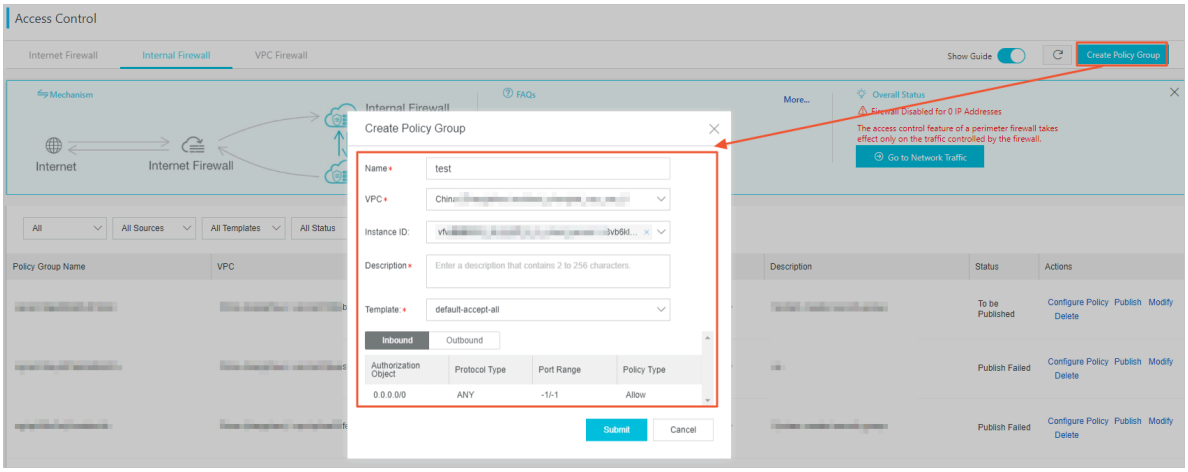
Procedure

Create a policy group, and then configure inbound or outbound access control policies.

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



3. In the upper-right corner, click Create Policy Group. In the Create Policy Group dialog box, configure the policy group.



The configuration items of a policy group are described as follows:

Item	Description	Configuration note
Name	The name of the policy group. The name must be from 1 to 128 characters in length.	Enter a policy group name.
VPC	The VPC network to which the policy group is applied.	In the VPC drop-down list, select a VPC network . Note: You can select only one VPC network.

Item	Description	Configuration note
Instance ID	The IDs of instances in the selected VPC network.	In the Instance ID drop-down list, select instance IDs. Note: You can select multiple instance IDs.
Description	A description of the policy group. The description must be from 2 to 256 characters in length.	Enter a description of the policy group.
Template	The policy group template.	In the Template drop-down list, select a template. The templates are as follows: · `default - accept - login` : Allow all inbound traffic that passes through port 22 and port 3389 by default. · `default - drop - all` : Deny all traffic in the policy group by default. · `default - accept - all` : Allow all traffic in the policy group by default.

4. Click Submit.

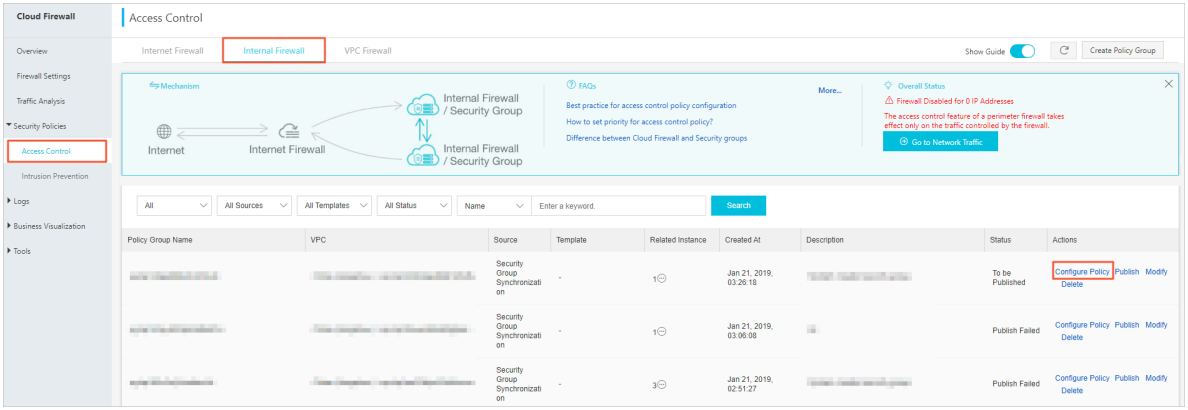
   You can locate the new policy group on the Internal Firewall page, and configure, publish, modify, or delete this policy group.

   Note:
   You can modify or delete a policy group. When you modify a policy group, you can only modify the related instances and the policy group description. After you delete a policy group, the access control policies between ECS instances in this policy group are automatically deleted and become invalid.

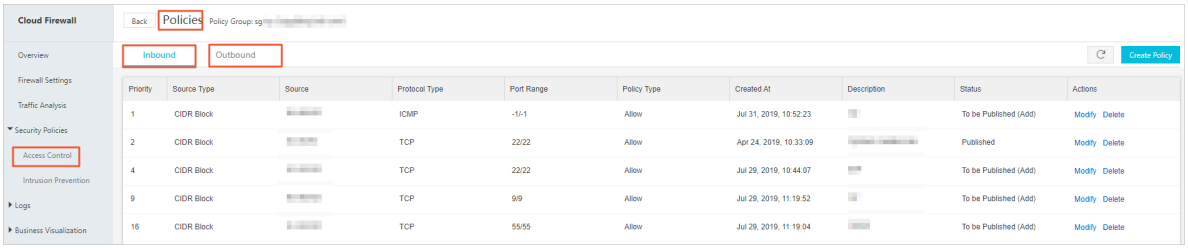
5. Click Configure Policy in the Actions column to create access control policies.

   Note:
   You can create multiple policies in a policy group. By default, you can create up to 100 policy groups and 100 policies. If you want to create more policies than

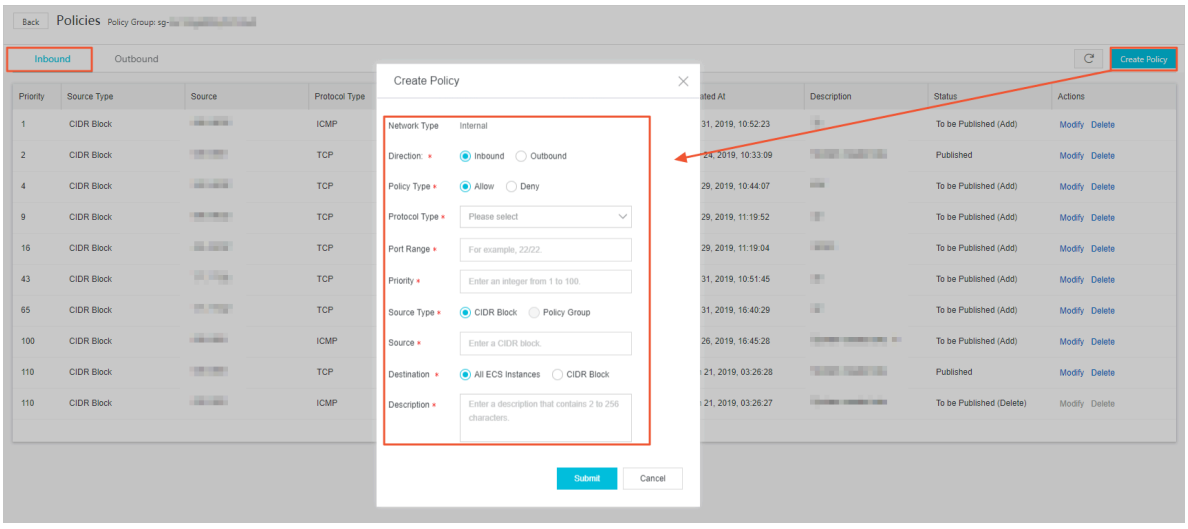
allowed, we recommend that you delete unnecessary policies or submit a ticket for technical support.



6. On the Policies page, click the Inbound or Outbound tab, and click Create Policy in the upper-right corner.



7. In the Create Policy dialog box, configure the policy.



The policy configuration items are as follows:

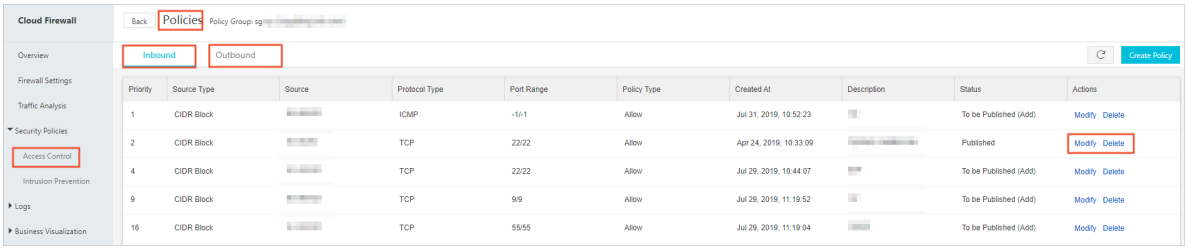
Item	Description	Configuration note
Network Type	The type of the network to which this policy is applied.	The default value is `Internal`, indicating that the policy is applied to traffic between ECS instances.

Item	Description	Configuration note
Direction	The direction of traffic controlled by this policy.	Options: · `Inbound` : Apply the policy to traffic from other instances to the specified instance. · `Outbound` : Apply the policy to traffic from the specified instance to other instances.
Policy Type	Indicates whether to allow or deny the traffic passing through the internal firewall.	Options: · `Allow` : Allow the traffic between ECS instances. · `Deny` : Deny the traffic between ECS instances.
Protocol Type	The protocol of the traffic.	In the Protocol Type dialog box, select a protocol. Options: · `TCP` · `UDP` · `ICMP` · `ANY` indicates any protocol. You can select `ANY` if you do not know which protocol is used.
Port Range	The ports that are controlled by this policy.	Enter a port range. For example, 22/22.
Priority	The priority of this policy.	Enter a priority number. Note: The priority number must be an integer from 1 to 100. If two policies have the same priority number, the Deny policy has the higher priority. If two Allow policies have the same priority number, both policies take effect at the same time.

Item	Description	Configuration note
Source Type	The type of the traffic source controlled by this policy.	Options: · CIDR Block : The policy controls the traffic from a CIDR block. · Policy Group : The policy controls the traffic from multiple ECS instances in a policy group. · Note: For a policy created in the ECS security group module, you cannot select Policy Group as the source type.
Source	The traffic source controlled by this policy. Enter a CIDR block or addresses of instances in a policy group.	Specify the traffic source based on the selected source type. · If the source type is set to CIDR Block , enter a CIDR block. You can specify only one CIDR block. · If the source type is set to Policy Group , click the Source drop-down list, and select a policy group. This sets multiple instances in the specified policy group as the traffic source. Note: You can select only one policy group as the source.
Destination	The destination of the traffic.	Options: · All ECS Instances : Apply this policy to all ECS instances. · CIDR Block : Specify an IP address or a CIDR block. The policy is applied to the traffic received by the specified addresses.
Description	A description of the policy.	Enter a policy description. The description must be from 2 to 256 characters in length.

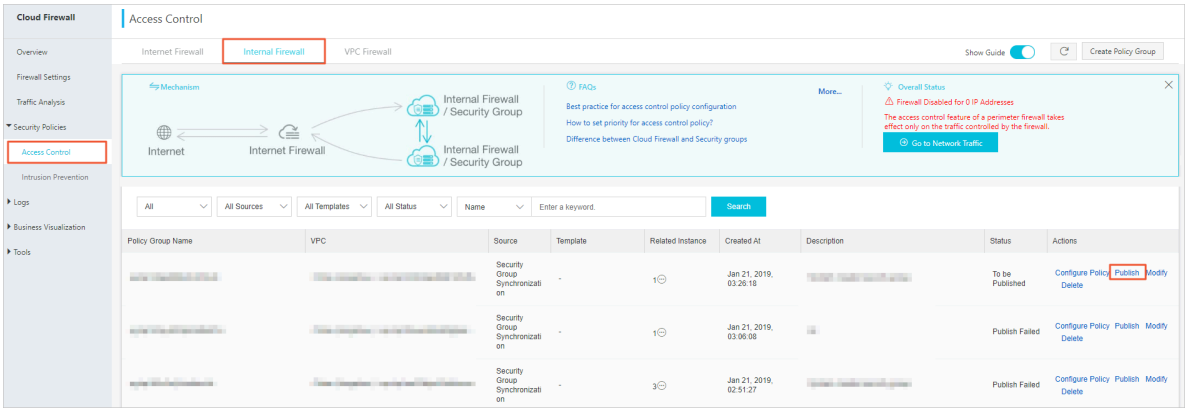
8. Click Submit.

   On the Policies page, you can view, modify, or delete the inbound or outbound policies.

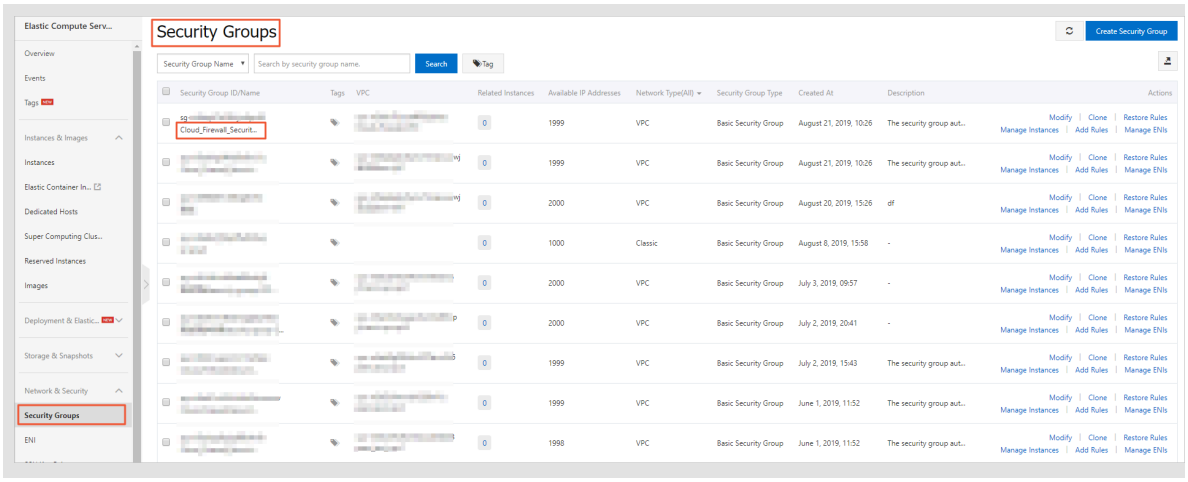


> **Note:**
> After you delete a policy, the traffic control rule specified in this policy becomes invalid. After you delete a policy, you can still view this policy in the list but cannot perform any operation on it.

9. On the Internal Firewall page, find the policy group to be applied. Click Publish in the Actions column. The policies take effect and are synchronized to the ECS security group module.



> **Note:**
> To apply a policy and synchronize it to the ECS security group module, you must publish it first. To view the policies that are created on the Internal Firewall page in Cloud Firewall and synchronized to the ECS security group module, log on to the ECS console, and choose Security Groups > Security Groups.



Differences between the internal firewall and ECS security groups

The internal firewall in Cloud Firewall can control the traffic between ECS instances.

For more information about the differences between the internal firewall and ECS security groups, see#unique_7

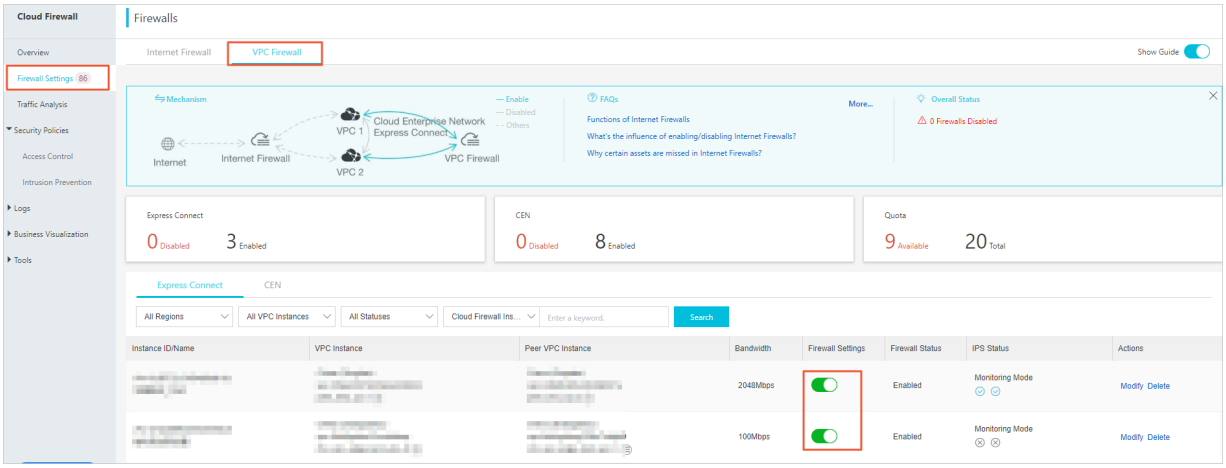
4 Access control over VPC firewalls

This topic describes access control over VPC firewalls.

Prerequisites

VPC firewalls are not automatically created. Before you create access control policies between two VPC networks, create and enable a VPC firewall first.

The access control policies take effect only after you have enabled the VPC firewall.



Context

Cloud Firewall supports access control over VPC firewalls. You can use a VPC firewall to detect and control the traffic between two VPC networks.

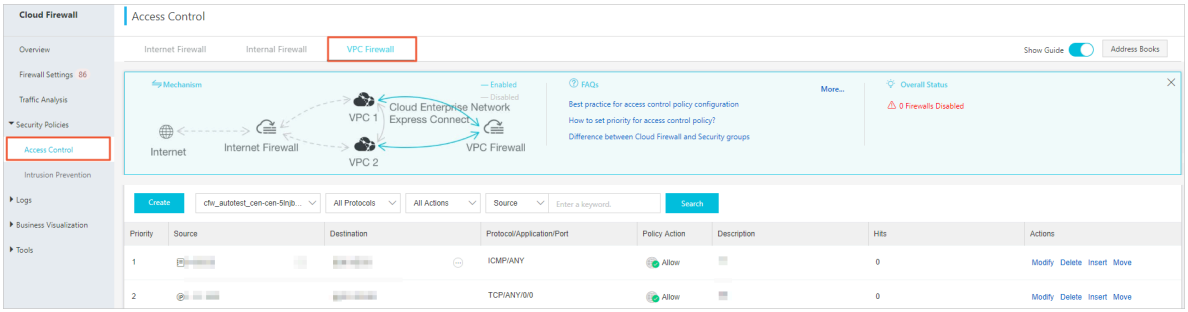
Configure an access control policy

A VPC firewall allows all traffic by default. To control the traffic between VPC networks, you can deny the traffic from untrusted sources. Or, you can allow the traffic from trusted sources and then deny the traffic from all other sources.

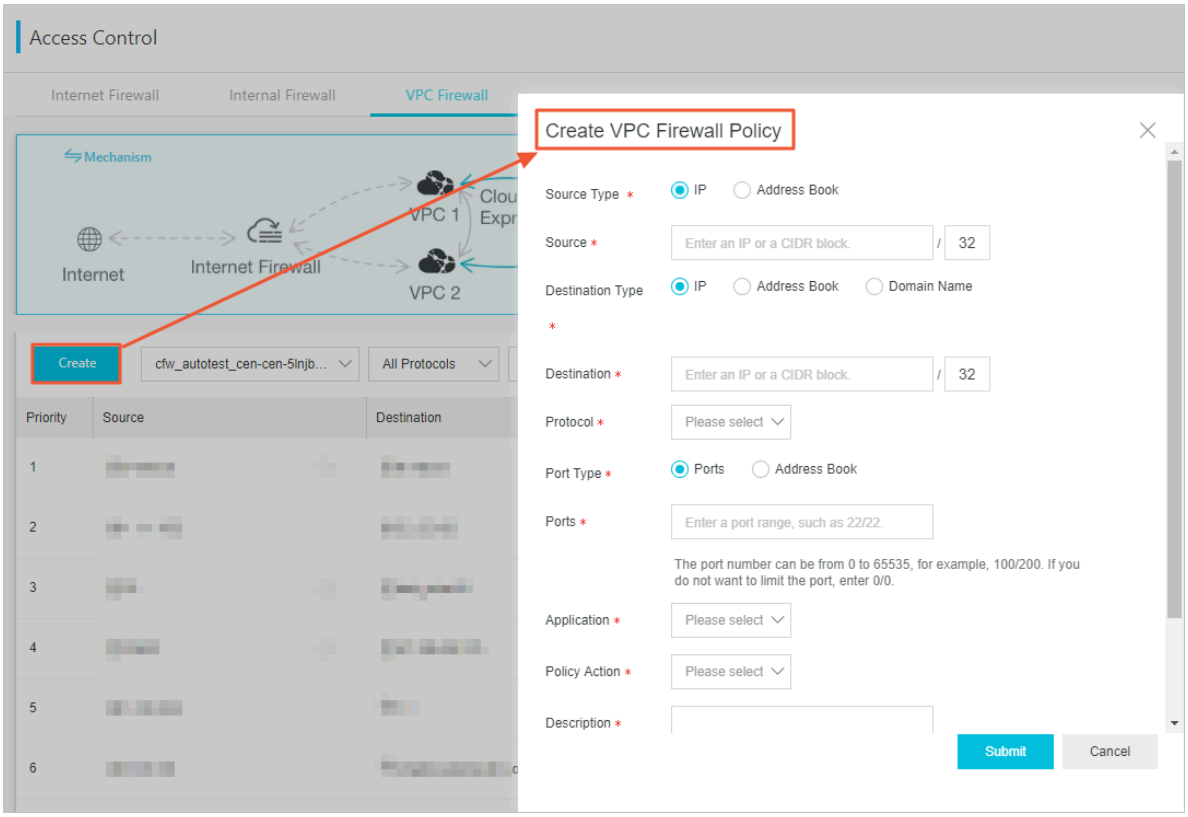
Procedure

1. Log on to the Cloud Firewall console.

2. In the left pane, choose Security Policies > Access Control > VPC Firewall.



3. Click Create.
4. In the Create VPC Firewall Policy dialog box, configure the access control policy.



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

- Create a policy to deny the traffic from untrusted sources.
- Create a policy to allow the traffic from trusted sources, and then create another policy to deny the traffic from all other sources. Make sure that the allow policy

has a higher priority than the deny policy. For more information on policy priority, see #unique_5.

For more information on the parameters in an access control policy, see the Policy parameters table in this topic.

 Note:
A VPC firewall allows all traffic by default.

Policy parameters

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 an existing address book. You can add multiple IP addresses to an address book to simplify policy configuration.
Source	The source IP address or CIDR block of the traffic.  Note: You can specify only one CIDR block, for example, 1.1.1.1/32. If you set Source Type to Address Book, select an existing address book as the source.
Destination type	· IP: Set the destination to an IP address. · Address Book: Set the destination to an address book. · Domain Name: Set the destination to a domain name. You can specify a wildcard domain, for example, `*.a.com`.  Note: If an HTTP header does not contain the host field or an HTTPS request does not contain Server Name Indication (SNI), the policy action is set to Allow by default.
Destination	Set the destination to a CIDR block. If you set the destination type to domain name, set the destination to a domain or a wildcard domain, for example, `*.a.com`.

Parameter	Description
Protocol	· ANY: Indicates any protocol. · TCP · UDP · ICMP
Destination ports	You can specify a port range. 0/0 indicates any port. Note: If you set the protocol to ICMP, the destination port configuration is not required. If you set the protocol to `ANY`, the destination port configuration does not take effect on ICMP traffic.
Application	You can set the application to ANY, HTTP, HTTPS, Memcached, MongoDB, MQTT, MySQL, RDP, Redis, SMTP, SMTPS, SSH, or VNC. If Protocol is set to `TCP`, multiple applications are available. Otherwise, you can set the application to `ANY` only. Note: The identification application relies on the application message characteristics (the protocol identification is not based on the port); when the application identification fails, the session traffic is `Allow`.
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 monitoring the traffic for a period of time, you can change the policy action to `Allow` or `Deny`.
Description	A description or note about this policy. Enter a description of the policy so that you can distinguish the policies later.
Priority	Set the priority of the access control policy. The default priority is the `Lowest`.

5 Set or modify the priority of an access control policy

Each access control policy in Cloud Firewall is automatically assigned with a default priority. You can click Move in the Actions column to modify the priority of a policy.

Context

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

The larger the priority number, the lower the priority.

The maximum number of policies varies with the edition of Cloud Firewall. Therefore, the priority number range also changes with the Cloud Firewall edition.

- In Pro Edition, you can configure up to 1,000 access control policies. The priority ranges from 1 to 1,000.
- In Enterprise Edition, you can configure up to 2,000 access control policies. The priority ranges from 1 to 2,000.
- In Ultimate Edition, you can configure up to 5,000 access control policies. The priority ranges from 1 to 5,000.

 Note:
A new policy has the lowest priority by default. That is, this policy is assigned with the largest priority number.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose Security Policies > Access Control > Internet Firewall.
3. On the Outbound Policies or Inbound Policies tab page, locate the access control policy of which the priority needs to be modified. Click Move in the Actions column.

4. Modify the priority in the displayed dialog box.

5. Click OK.

 Note:
After you modify the priority of a policy, the priorities of policies with lower priorities decrease accordingly.

6 Intrusion prevention policies

With the built-in IPS, Cloud Firewall defends against intrusions and common attacks in real time, and provides virtual patches for precise threat detection to intelligently block intrusions.

Cloud Firewall supports the following intrusion prevention features:

- Threat Intelligence: Cloud Firewall scans for and detects threat intelligence, and blocks malicious behavior from command-and-control servers in advance based on received threat intelligence.
- Basic Rules: Cloud Firewall detects malware and intercepts communication with command-and-control servers or backdoors.
- Virtual Patching: Cloud Firewall provides virtual patches to defend against exploits of popular high-risk vulnerabilities in real time.

IPS running mode

IPS supports the following running modes:

- Observation Mode: If you select this option, IPS monitors for malicious traffic and sends alarms when detecting it.

  
  Note:
  By default, IPS runs in Observation Mode mode once you subscribe to the Cloud Firewall service.

- Interception Mode: If you select this option, IPS intercepts malicious traffic to block intrusions.

Basic defense

IPS provides basic intrusion prevention capabilities to intercept password cracking , command execution vulnerabilities, and connections from infected servers to command-and-control servers.

IPS supports the following basic intrusion prevention modes:

- Basic Rules: If this mode is enabled, IPS provides basic intrusion prevention based on built-in intrusion prevention rules.

- Threat Intelligence: If this mode is enabled, IPS can perceive threat sources across the entire Alibaba Cloud network in advance. IPS learns malicious IP addresses (for example, those of malicious visitors, scanners, and crackers) on the entire network and precisely intercepts their intrusions. [DO NOT TRANSLATE]

Virtual patching

You can use virtual patches to defend against popular high-risk vulnerabilities without installing the patches in your system.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose Security Policies > Intrusion Prevention. The Intrusion Prevention page is displayed.
3. In the Mode Selection area, click Observation Mode or Interception Mode.

    Note:
   We recommend that you click Interception Mode.
4. In the Basic Defense area, turn on or off the Basic Rules or Threat Intelligence switch.

    Note:
   We recommend that you turn on both the Basic Rules and Threat Intelligence switches.
5. In the Virtual Patching, enable or disable the virtual patching function.

    Note:
   We recommend that you enable the virtual patching function.
6. Select the required virtual patches as follows: Click Custom in the Virtual Patching area to go to the Virtual Patch Management dialog box.
7. Click Enable or Disable to enable or disable a specified patch.

    Note:
   Disabled patches cannot be automatically updated. We recommend that you enable all virtual patches.