

Alibaba Cloud Cloud Firewall

Product Introduction

Issue: 20190429

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 <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid <i>Instance_ID</i></code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

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

Legal disclaimer.....	I
Generic conventions.....	I
1 What is Cloud Firewall.....	1
2 Technical principles.....	2
3 Features.....	3
4 Benefits.....	5
5 Scenarios.....	7
6 Glossary.....	8

1 What is Cloud Firewall

Alibaba Cloud's Cloud Firewall is the industry's first firewall as a service (FWaaS) solution targeted for public clouds. It allows you to centrally manage the control policies for the access traffic from the Internet to your ECS instances (internet traffic), and provides micro-isolation policies for the access traffic between ECS instances (intranet traffic). With the built-in Intrusion Prevention Service (IPS), Cloud Firewall gives you full visibility of network-wide traffic and access relationships between ECS. Cloud Firewall is the primary infrastructure that you need to deploy to ensure network security of the businesses that you have migrated onto Alibaba Cloud.

2 Technical principles

Cloud Firewall is a network security product tailored by the Alibaba Cloud Security team for cloud users. With the advantages of easy deployment and smooth scaling, it integrates functions such as access control, business isolation, and traffic identification.

Cloud Firewall mainly consists of the following two control modules:

- **North-south traffic control module:** controls the access traffic from the Internet to your ECS instances. This module controls the access traffic through layer 4 to layer 7.
- **East-west traffic control module:** controls the access traffic between ECS instances through security groups. This module controls the access traffic through layer 4.

3 Features

Cloud Firewall supports centralized management of north-south and east-west traffic, and provides features including real-time traffic monitoring, precise access control, real-time intrusion prevention, and traffic logs to comprehensively protect your network.

Cloud Firewall supports the following features:

- Real-time traffic monitoring:
 - Monitors the external connection activities.
 - Analyzes the access traffic from the Internet to your ECS instances.
 - Analyzes the access traffic between ECS instances in your intranet.
 - Gives you full visibility of your assets and access relationships between assets, helping you detect abnormal traffic in a timely manner.
- Precise access control:
 - Controls the access traffic from the Internet to your ECS instances (north-south traffic).
 - Provides micro-isolation protection over the access traffic between ECS instances (east-west traffic) on your intranet.
 - Controls inbound and outbound traffic.
 - Performs domain name-based access control to strictly control the external connection traffic.
 - Analyzes external connections activities to help you detect abnormal activities on ECS instances.
- Real-time intrusion prevention:
 - Intelligently detects and blocks intrusions in real time. Analyzes the network access traffic blocked by Cloud Firewall and IPS.
 - Synchronizes malicious IP addresses (for example, those of malicious visitors , scanners, and command-and-control servers) detected on the entire Alibaba

Cloud network to Cloud Firewall to defend against threats and intrusions in advance.

- Embedded with intrusion prevention rules concluded in long-term attack and defense practices on cloud platforms, featuring a high threat recognition rate and a low false alarm rate.
- Supports recovery through virtual patches instead of patch installation in business systems, and precisely protects against popular vulnerabilities and high-risk 0-day and N-day exploitation.
- Behavior backtracking:
 - Provides event logs to show real-time threats or intrusions detected and blocked by IPS.
 - Provides traffic logs to show all the traffic that passes through Cloud Firewall . When a threat event occurs, you can view traffic logs to analyze the traffic, identify the visitors, and check whether the configured access control policies have taken effect.
 - Provides system operation logs to show all the configuration and operation records in Cloud Firewall.
 - Stores logs for a maximum of six months, which complies with network security regulations and classified protection requirements.

4 Benefits

This document introduces the benefits of Cloud Firewall, which is the industry's first FWaaS solution for cloud platforms. It manages north-south and east-west traffic in a centralized manner to comprehensively protect your network. Cloud Firewall's out-of-the-box features make it easy to use. In addition, it supports precise access control and network-wide traffic visibility.

FWaaS, which is easy to use

Cloud Firewall is the first FWaaS solution provided for public clouds based on software-defined networking (SDN) technology. Once you subscribe to the Cloud Firewall service in the console, you can use it after several simple steps of policy configurations. Cloud Firewall helps you get rid of the basic but complex system and network configurations such as image installation and routing setup that are required by traditional firewalls. In addition, you do not need to be concerned about issues such as disaster recovery, capacity expansion, and deployment.

Smooth scaling

Cloud Firewall is deployed in cluster mode and supports smooth scaling. It provides a defense capability of up to 2 Gbit/s per IP address, which is customizable.

High availability and reliability

Cloud Firewall is deployed in dual available zone (AZ) mode. The failure of any server or AZ does not affect Cloud Firewall's normal service.

Cloud Firewall supports easily bypassing a certain IP address, helping you rapidly diagnose faults during O&M.

Centralized policy management

Cloud Firewall provides complete north-south and east-west traffic control for your assets. You can fully control the access to your ECS instances and isolate ECS instances for security.

With Cloud Firewall, you can control access to common cloud assets such as ECS instances at the network level and fix the problems of abnormal accessing to the cloud assets.

Real-time intrusion prevention

With the built-in IPS, Cloud Firewall can receive simultaneous updates of network-wide threat intelligence, detect and block threats from the Internet in real time.

Business relationship visibility

Cloud Firewall shows assets and their access relationships in topology views. Once you subscribe to the Cloud Firewall service, you can gain instant visibility of your business regions, groups, assets, access relationships between assets, and clustering analysis of user traffic without any configurations. Cloud Firewall supports visual analysis of traffic to maximize the correctness of policies.

Compliance with classified protection requirements

Cloud Firewall meets the boundary protection, access control, and other requirements on classified protection.

5 Scenarios

Cloud Firewall is the primary infrastructure that you need to deploy to ensure network security of the businesses when you have migrated onto Alibaba Cloud. Cloud Firewall supports the functions including network-wide traffic identification, centralized policy management, intrusion detection, and logging.

Cloud Firewall controls the access traffic from the Internet to your ECS instances , external connection traffic from ECS instances to the Internet, and access traffic between ECS instances.

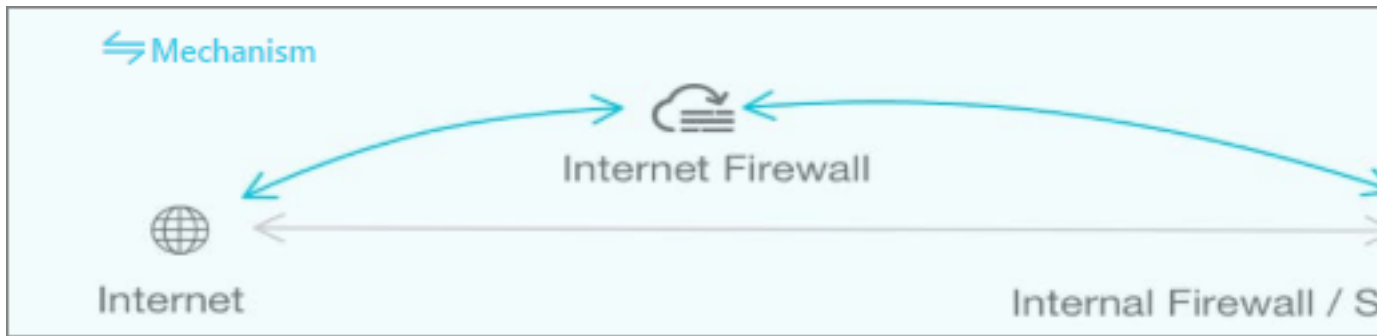
Cloud Firewall applies to the following scenarios:

- **Control the access traffic from the Internet to ECS instances:** For example, a financial company on Alibaba Cloud uses IPS to protect their HTTP and other businesses exposed on the Internet.
- **Prevent abnormal external connection activities:** For example, a government sector on Alibaba Cloud analyzes not only the access traffic from the Internet to ECS instances, but also the external connection traffic from ECS instances to the Internet. Based on the analysis, the government sector can determine which ECS instances are at risk and then block abnormal access in real time to avoid potential risks.
- **Protect the access traffic between ECS instances through micro-isolation:** For example, an e-commerce company on Alibaba Cloud runs businesses based on HTTP and uses Web Application Firewall (WAF) for business protection. To isolate the different businesses from each other, the company now deploys Cloud Firewall to comprehensively improve network control. This helps avoid threats to the company's cloud-based businesses due to security risks on a certain ECS instance.

6 Glossary

Internet Firewall

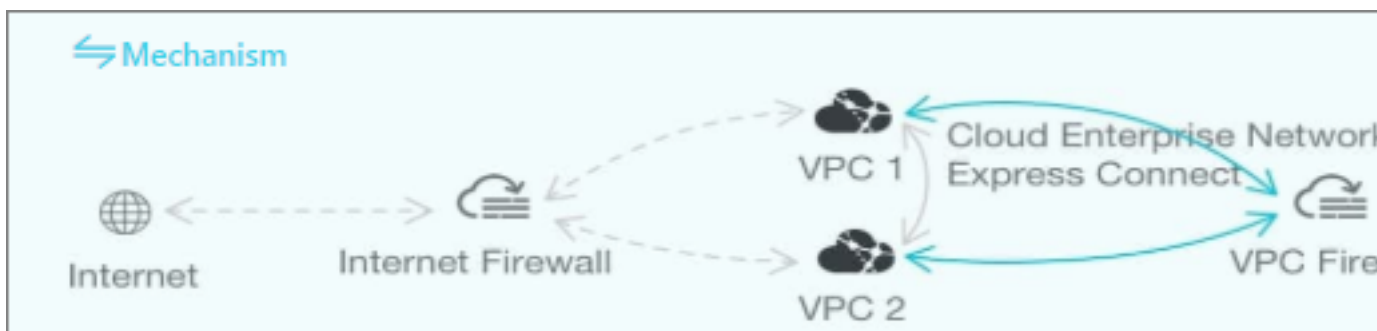
An Internet Firewall monitors and centrally manages the traffic between the Internet and your cloud assets. An Internet Firewall works as follows:



The built-in Intrusion Prevention module of an Internet Firewall allows you to detect victim servers, block external connections started by your servers, and view the connections among cloud services. An Internet firewall is delivered based on the SaaS model. You can quickly enable the firewall without complex network configurations or firewall installation using an image file. Internet Firewalls are deployed in a cluster by default and support smooth scale-up.

VPC Firewall

A VPC firewall is a distributed firewall that monitors the traffic between two VPC networks. A VPC firewall works as follows:



A VPC Firewall can be deployed between two VPC networks that are connected by Express Connect or are bound to the same CEN instance of the VPC network. A VPC Firewall is not created by default. You must specify two VPC networks to create a VPC Firewall.

Security Group/Internal Firewall

A Security Group is a distributed virtual internal firewall provided by ECS. It provides port status monitoring and packet filtering. You can use Security Group to configure access control among ECS instances. A Security Group is set for a group of ECS instances from the same region. These instances have the same security requirements and trust each other. When you create an ECS instance, you must specify at least one Security Group.

The Internal Firewall provided by Cloud Firewall IS based on Security Groups. To configure Internal Firewall policies, you can choose Cloud Firewall > Internal Firewall or go to the Security Group configuration page in the ECS console. The configurations are automatically synchronized between the two platforms.

External connections

Cloud Firewall analyzes the external connections started by your ECS instances. You can detect suspicious servers by monitoring the external connections data.

Intrusion detection

The intrusion detection module monitors the network traffic and detects suspicious events. The module sends alerts on or directly deals with the suspicious events. Cloud Firewall integrates the intrusion detection and prevention capabilities of Alibaba Cloud that have been built over the last ten years. Cloud Firewall performs real-time data collection and analysis on the traffic passing through the firewalls. You can detect victim servers and block suspicious network activities by using Cloud Firewall.

Open application, open port, and open public IP address

An open application is an application that is exposed to the Internet. For example, HTTP and SSH.

An open port is a port that is exposed to the Internet. For example, port 80 and port 22.

An open public IP address is the public IP address of an asset that is exposed to the Internet.

Cloud Firewall can identify the following types of public IP addresses:

- EIP addresses, which can be bound to ECS instances in VPC networks, SLB instances in VPC networks, ENI instances, or NAT gateways.

- NatPublicIp, the public IP addresses allocated to ECS instances.

Application group

In the east-west business visualization module, an application group is a set of applications that provide the same or similar services. For example, you can add all ECS instances that are deployed with MySQL to a database application group.

Business group

In the east-west business visualization module, a business group contains all application groups related to a specific business. For example, a Web portal business group contains the Web application groups and the database application groups.

Vulnerable application group, vulnerable business group

A vulnerable application group is a set of applications with a specific open vulnerable port, such as port 445. Each vulnerable port corresponds to a vulnerable application group.

A vulnerable business group is a set of vulnerable application groups.

You can use vulnerable business groups and application groups to find out which ECS instances have open vulnerable ports or have accessed vulnerable ports.

Cloud Firewall automatically creates vulnerable business groups and adds vulnerable businesses to the groups.

Independent business group, dependent business group

In the east-west traffic visualization module, these concepts reflect the access relationships between two business groups. For example, if business group A accesses the resources in business group B, business group B is the independent group, and business group A is the dependent group.

First visit traffic

The first visit traffic refers to the traffic from the source IP address to the destination IP address during the first visit within the specified period. You can analyze the cause of the first visit based on the time of the first visit, the source and destination IP addresses, and other information. The first visit traffic can be generated by intrusions or the activation of services.

Address book

Cloud Firewall allows you to create address books of IP addresses or port numbers. This enables more efficient firewall configuration. You can reference an address book to quickly configure all the IP addresses or ports in this address book.

Cloud Firewall supports the following types of address books:

- IP address books
- Port address books
- ECS tag address books. After you specify a group of ECS tags, Cloud Firewall automatically adds the public IP addresses of ECS instances with these tags to the specific ECS tag address book.

The following rules apply to address books:

- Cloud Firewall has built-in global address books. You cannot modify or delete these address books.

Address Book Name	Type	IP/ECS Tag	Description	References	Actions
[Redacted]	IP Address	[Redacted] 1	[Redacted]	1	Modify Delete
[Redacted]	IP Address	[Redacted]	[Redacted]	4	Modify Delete
[Redacted]	IP Address	[Redacted]	[Redacted]	1	Modify Delete
[Redacted]	IP Address	[Redacted] 1	[Redacted]	4	Modify Delete
[Redacted]	IP Address	[Redacted] 1	[Redacted]	6	Modify Delete
[Redacted]	IP Address	[Redacted]	[Redacted]	0	Modify Delete
Any	IP Address	[Redacted]	[Redacted]	2	Modify Delete

- An IP address or port number can be added to multiple address books.
- Changes of IP addresses or port numbers in address books automatically apply to the access control policies.