ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall
Product Introduction

Document Version: 20220630

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.What is Cloud Firewall?

Cloud Firewall of Alibaba Cloud is a cloud security solution that provides firewalls as a service. Cloud Firewall implements centralized security isolation and traffic control for your cloud assets at the Internet, virtual private cloud (VPC), and host boundaries. Cloud Firewall is the first line of defense to protect your services in Alibaba Cloud.

Compliance

Cloud Firewall complies with the following standards: ISO 9001, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 29151, ISO 27701, BS 10012, Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR), and Payment Card Industry (PCI) Data Security Standards (DSS).

Contact us

If you have any questions about the features, prices, and specifications of Cloud Firewall or if you want to apply for the trial use of Cloud Firewall, join the DingTalk group numbered 33081734 to obtain support from Cloud Firewall security experts.

Related information

- Functions and features
- 计费方式（包年包月）
- Protection scope of Cloud Firewall

2.Functions and features

Cloud Firewall is a cloud security solution that provides firewalls as a service. It manages both north-south and east-west traffic and provides features, such as traffic monitoring, precise access control, and real-time intrusion prevention, to deliver protection at the network boundaries. This topic describes Cloud Firewall features and the Cloud Firewall editions that support the features.

Cloud Firewall features

The following table describes Cloud Firewall features and the Cloud Firewall editions that support the features. For more information about the subscription billing method of Cloud Firewall, see 计费方式（包年包月）.

Note

- Cross (×): The feature is not supported by the edition.
- Tick (√): The feature is supported by the edition.

Scenario	Feature	Description	Free Edition	Premium Edition	Enterprise Edition	Ultimate Edition	Pay-as-you-go Edition	References
Access traffic analysis and attack detection of on-cloud networks	Overview	Provides an overview of defense features that are enabled and disabled and shows statistics on access traffic and detected security risks from the last seven days.	×	√	√	√	√	Overview

Scenario	Feature	Description	Free Edition	Premium Edition	Enterprise Edition	Ultimate Edition	Pay-as-you-go Edition	References
Access control	Internet Firewall	Supports domain name-based access control to strictly control the traffic of outbound connections and supports two-way access control over north-south IPv4 traffic.	×	√	√	√	×	Create access control policies for outbound and inbound traffic on the Internet firewall
	VPC Firewall	Controls traffic between virtual private clouds (VPCs).	×	×	√	√	×	Create an access control policy for a VPC firewall
	Internal Firewall	Controls east-west traffic among your Elastic Compute Service (ECS) instances on an internal network.	×	×	√	√	×	Access control on an internal firewall between ECS instances

Scenario	Feature	Description	Free Edition	Premium Edition	Enterprise Edition	Ultimate Edition	Pay-as-you-go Edition	References
	Policy Assistant	Checks for ECS security group rules whose risk level is High and provides suggestions to modify the rules. This allows you to use security groups in a more secure and efficient manner.	√	√	√	√	×	Check security group rules
Network traffic analysis	Outbound Connections	Monitors outbound connections of cloud assets in real time.	×	√	√	√	×	Outbound connections
	Internet Access	Collects and analyzes the statistics on access traffic of on-cloud networks.	×	√	√	√	×	Internet access
	VPC Access	Monitors the traffic between VPCs in real time, which allows you to dynamically obtain the VPC traffic data and identify and handle suspicious traffic at the earliest opportunity.	×	×	√	√	×	VPC access
	All Access Activities	Allows you to query traffic that passes through Cloud Firewall based on conditions.	×	√	√	√	×	All access activities
	Vulnerability Prevention	Detects vulnerabilities that can be exploited by attacks in real time and defends against these vulnerabilities.	×	√	√	√	√	Vulnerability protection
	Breach Awareness	Provides the details about intrusion events that are detected by the intrusion prevention system (IPS) and the solutions to handle the intrusion events.	×	√	√	√	√	Breach awareness

Scenario	Feature	Description	Free Edition	Premium Edition	Enterprise Edition	Ultimate Edition	Pay-as-you-go Edition	References
Attack prevention	Intrusion Prevention	Provides the details about protection for traffic between VPCs, inbound Internet traffic, and outbound Internet traffic.	×	√	√	√	√	Intrusion prevention
	Prevention Configuration	Provides the built-in threat detection engine that delivers the following capabilities: - Intelligently detects and blocks intrusions in real time. Analyzes the network traffic blocked by Cloud Firewall and IPS. - Synchronizes all malicious IP addresses detected across Alibaba Cloud and defends against potential threats, such as malicious visitors, scanners, and command-and-control servers. - Integrates the intrusion prevention policies used for attack and defense on Alibaba Cloud to ensure high accuracy in threat detection. - Supports installation-free virtual patches for business systems. Precisely defends against common vulnerabilities. **Notice** Cloud Firewall Pay-as-you-go Edition does not provide the details about existing intrusion prevention rules or support the creation of custom intrusion prevention rules.	×	√	√	√	√	防护配置

Scenario	Feature	Description	Free Edition	Premium Edition	Enterprise Edition	Ultimate Edition	Pay-as-you-go Edition	References
Log management	Log Audit	Provides log audit and behavior backtracking. • Provides the logs of events on the Internet firewall and VPC firewalls. • Provides the logs of the traffic that passes through Cloud Firewall. If a threat occurs, you can view traffic logs to analyze traffic, identify its source, and check whether configured access control policies are in effect. • Provides system operation logs to record all configurations and operations on Cloud Firewall.	×	√	√	√	×	Log audit
	Log Analysis	Automatically collects, stores, and analyzes both inbound and outbound traffic logs in real time and supports real-time monitoring and alerting based on specific metrics. This ensures timely responses if exceptions occur in critical business. The value of a log storage duration ranges from 7 to 365 days.	×	√	√	√	×	Enable the log analysis feature
		Allows you to back up and roll back access control policies of the Internet firewall and VPC firewalls.	×	×	√	√	×	Back up and roll back an access control policy
		Supports the packet capture feature, which helps you troubleshoot network failures and analyze attacks.	×	×	√	√	×	Create a packet capture task

Scenario	Toolbox Feature	Description	Free Edition	Premium Edition	Enterprise Edition	Ultimate Edition	Pay-as-you-go Edition	References
Common tools for network traffic detection		Supports the strict mode of the Internet firewall. After the strict mode is enabled, the Internet firewall blocks traffic that meets the following conditions: The traffic matches an access control policy, and the application type of the traffic is identified Unknown.	×	×	√	√	×	Strict mode of the Internet firewall
		Checks whether the requirements of classified protection are met.	√	√	√	√	×	None
Business visualization	Custom Groups	Allows you to create custom groups to build relationships between the applications of your cloud assets and application groups or business groups.	×	√	√	√	×	Custom groups
Centralized account management	Central Account Management	Allows you to add Alibaba Cloud accounts as members, which helps you manage the resources of the accounts in a centralized manner.	×	×	×	√	×	Use centralized account management

3.Benefits

Cloud Firewall is the first Firewall as a Service (FWaaS) solution on the cloud. It manages north-south and east-west traffic in a centralized manner to protect your network. The out-of-the-box feature of Cloud Firewall makes it easy to use. In addition, Cloud Firewall supports precise access control and network-wide traffic visualization.

Fully managed service

Cloud Firewall is the first FWaaS solution that is available on a public cloud platform, Alibaba Cloud. It adopts software-defined networking (SDN) technology. Cloud Firewall is a fully managed service that spares you from complex device deployment and system configurations, such as firewall image installation and routing configurations. In addition, you do not need to pay attention to disaster recovery, scale-out, or access issues.

Ease of use

After you purchase a Cloud Firewall edition and complete necessary configurations in the console, you can use Cloud Firewall immediately to defend your network. Cloud Firewall effectively reduces the cost of network security control and O&M.

Smooth scaling

Cloud Firewall is deployed in cluster mode and supports smooth scaling. It provides a defense capability of up to 2 Gbit/s for each IP address. You can customize the defense capability based on your business requirements.

Stability and reliability

Cloud Firewall is deployed in two availability zones (AZs) to achieve high availability. This way, Cloud Firewall does not break down if a server or AZ fails.

On-cloud in-depth integration

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

Cloud Firewall integrates access by Alibaba Cloud network service, such as Virtual Private Cloud (VPC), Cloud Enterprise Network (CEN), Elastic IP Address (EIP), and Server Load Balancer (SLB). Cloud Firewall controls access to common cloud assets at the network layer and exploits security capabilities of terminals to monitor and block suspicious access to cloud assets.

Real-time intrusion prevention

A built-in intrusion prevention system (IPS) allows Cloud Firewall to update network-wide threat intelligence in real time and monitors more than 5 million active malicious IP addresses and domain names. In this way, Cloud Firewall can detect and block threats from the Internet. In addition, Cloud Firewall provides a cyber kill chain to defend against critical cyberattacks.

Visualized business relationships

Cloud Firewall shows assets and their access relationships in topology views. After you activate Cloud Firewall, you can view your business groups, application groups, assets, and access relationships between assets in topologies, and perform clustering analysis of user traffic without any configurations. Cloud Firewall supports visualized analysis of traffic to ensure policy accuracy.

Compliance with classified protection requirements

Cloud Firewall meets classified protection requirements such as boundary protection and access control.

4.Common scenarios

Cloud Firewall is the infrastructure that you can deploy to ensure network security for your workloads migrated to Alibaba Cloud. Cloud Firewall provides core features such as network-wide traffic identification, centralized policy management, intrusion detection, and log-related features.

Cloud Firewall controls the traffic from the Internet to your Elastic Compute Service (ECS) instances, the traffic from ECS instances to the Internet, and the traffic between ECS instances.

Access control on the Internet firewall

Cloud Firewall controls inbound and outbound Internet traffic, and intercepts attacks and threats from the Internet. The attacks and threats include intrusions, mining activities, and malicious traffic.

Access control on internal firewalls

Cloud Firewall controls the traffic between ECS instances in an internal network and isolates workloads. This way, risks on a specific ECS instance do not pose security threats to other workloads in the cloud.

Access control on VPC firewalls

Cloud Firewall controls the traffic between virtual private clouds (VPCs).

Intrusion prevention

Cloud Firewall detects and analyzes outbound connections of cloud assets, Internet access traffic, and traffic between ECS instances in an internal network. This helps you monitor the network traffic in real time, determine which cloud assets are at risk, and stop abnormal activities in real time to prevent risks.

Traffic visualization

Cloud Firewall displays asset information and access relationships to help you identify unusual traffic in real time.

Classified protection compliance

Cloud Firewall stores the logs of cloud assets. This helps websites meet the requirements of classified protection.

> ? **Note** Cloud Firewall Premium Edition can store logs for up tp 180 days. Cloud Firewall Enterprise Edition and Ultimate Edition can store logs for 7 to 360 days.

5.FAQ

Can I temporarily increase the bandwidth of Cloud Firewall?

Yes, you can increase the bandwidth of Cloud Firewall on a daily basis. For more information, see Upgrade the bandwidth configuration.

Does Cloud Firewall support the feature of centralized account management?

Yes, Cloud Firewall Ultimate Edition supports the feature of centralized account management. However, Cloud Firewall Premium Edition and Cloud Firewall Enterprise Edition do not support the feature. For more information about the feature of centralized account management, see Use centralized account management.

Trial use and pre-sales consultation

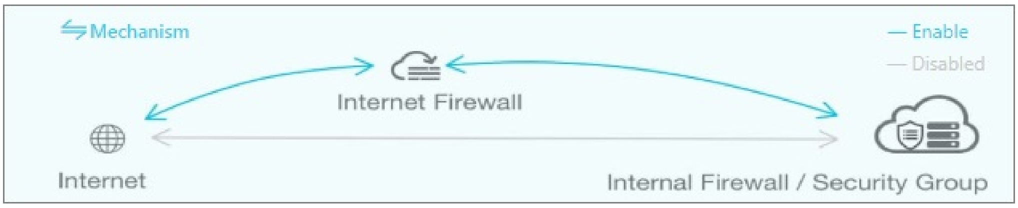
If you have questions about the features, prices, and specifications of Cloud Firewall, or if you want to apply for the trial use of Cloud Firewall, contact Cloud Firewall technical support by using DingTalk. You can search for group number 33081734 by using your DingTalk to join the Cloud Firewall DingTalk group and obtain support from Cloud Firewall security experts.

6.Terms

This topic introduces the common terms in Cloud Firewall.

Internet firewall

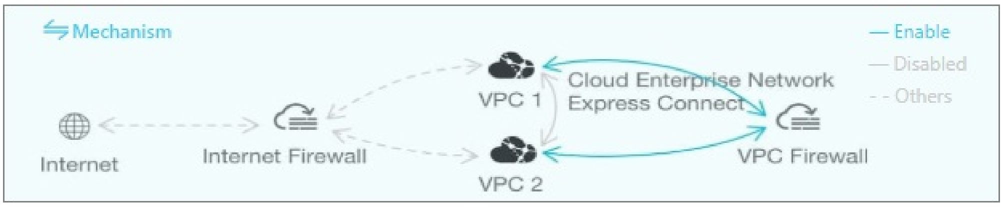
The Internet firewall monitors and manages the traffic between the Internet and your cloud assets in a centralized manner. The Internet firewall is deployed between the Internet and your servers. The following figure shows how the Internet firewall works.



The built-in intrusion prevention module of the Internet firewall allows you to detect compromised servers, block outbound connections initiated by your servers, and view the relationships among cloud services. You can enable the Internet firewall to protect your assets with a few clicks. You are not required to configure access to networks or install images. The Internet firewall is deployed in a cluster and can be smoothly scaled up and out.

VPC firewall

A VPC firewall is a distributed firewall that monitors the traffic between two virtual private clouds (VPCs). A VPC firewall is deployed between two VPCs. The following figure shows how a VPC firewall works.



A VPC firewall must be deployed between two VPCs that are connected by Express Connect or are bound to the same Cloud Enterprise Network (CEN) instance. VPC firewalls are not automatically created. You must specify two VPCs to create a VPC firewall.

security group and internal firewall

A security group is a distributed virtual internal firewall provided by Elastic Compute Service (ECS). It supports port status monitoring and packet filtering. You can use a security group to control access to ECS instances. A security group is a group of ECS instances in 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 for this instance.

An internal firewall implements the security group feature at the underlying layer. You can configure policies on the **Internal Firewall** tab of the **Access Control** page in the Cloud Firewall console or configure security groups in the **ECS console**. The configurations are automatically synchronized.

outbound connection

Cloud Firewall analyzes the outbound connections initiated by your servers in Alibaba Cloud to detect suspicious servers.

breach awareness

The breach awareness module monitors network traffic and detects suspicious events. The module sends alerts on or directly deals with the detected suspicious events. Cloud Firewall integrates the intrusion detection and prevention capabilities of Alibaba Cloud that are built over more than a decade. Cloud Firewall collects and analyzes the traffic that passes through Cloud Firewall in real time. You can use Cloud Firewall to detect compromised servers and block suspicious network activities.

open application, open port, and open public IP address

An open application is an application that is exposed to the Internet, such as an HTTP or SSH application.

An open port is a port that is exposed to the Internet, such as port 80 or 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:

- Elastic IP addresses (EIPs). EIPs can be associated with the ECS instances of the VPC type, internal-facing Server Load Balancer (SLB) instances of the VPC type, elastic network interfaces (ENIs), or Network Address Translation (NAT) gateways.
- Public NAT IP addresses of ECS instances.

application group

In the east-west business visualization module, an application group is a collection 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.

An application is the smallest unit of east-west business visualization in Cloud Firewall. By default, an application serves as a collection of all open ports on an ECS instance. You can create an application by cloning the application of a specific port.

business group

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

vulnerable application group and vulnerable business group

A vulnerable application group is a collection of applications that have open vulnerable ports, such as port 445. Each vulnerable port corresponds to a vulnerable application group.

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

You can use vulnerable business groups and application groups to identify the ECS instances that have open vulnerable ports or have accessed vulnerable ports.

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

independent business group and dependent business group

In the east-west traffic visualization module, these terms 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

First visit traffic refers to the traffic from a source IP address to a destination IP address during the first visit within a specific period of time. You can identify the cause of the first visit traffic based on information including the time of the first visit and the source and destination IP addresses. The first visit traffic can be generated by intrusions or applications that are newly published.

address book

Cloud Firewall allows you to create address books of IP addresses or port numbers. This allows you to implement flexible access control based on IP addresses or ports. When you configure an access control policy, you can use an address book to specify all the IP addresses or ports in the address book at a time.

Cloud Firewall supports the following types of address books:

- IP address book: allows you to specify a set of IP addresses.
- Port address book: allows you to specify a set of ports.
- Domain name address book: allows you to specify a set of domain names.
- Cloud address book: allows you to specify a set of IP addresses or domain names.

The following rules apply to address books:

- Cloud Firewall has built-in global address books. You cannot modify or delete these address books.
- One IP address or port number can be added to multiple address books.
- If you change the IP addresses or port numbers in an address book, the changes automatically take effect for access control policies.

7.Supported regions

This topic lists the regions in which the features of Cloud Firewall are supported.

The features are Internet Firewall, virtual private cloud (VPC) Firewall, network address translation (NAT) Firewall, and Domain Name System (DNS) Firewall.

Note In the following table, indicates that the feature is supported and indicates that the feature is not supported.

Region	Region ID	Internet Firewall		VPC Firewall		NAT Firewall	DNS Firewall
		IPv4	IPv6	CEN transit router (Basic Edition) and Express Connect	CEN transit router (Enterprise Edition)		
China (Qingdao)	cn-qingdao						
China (Beijing)	cn-beijing						
China (Zhangjiakou)	cn-zhangjiakou						
China (Hohhot)	cn-huhehaote						
China (Ulanqab)	cn-wulanchabu						
China (Hangzhou)	cn-hangzhou						
China (Shanghai)	cn-shanghai						
China (Shenzhen)	cn-shenzhen						

Region	Region ID	Internet Firewall		VPC Firewall		NAT Firewall	DNS Firewall
		IPv4	IPv6	CEN transit router (Basic Edition) and Express Connect	CEN transit router (Enterprise Edition)		
China (Heyuan)	cn-heyuan						
China (Guangzhou)	cn-guangzhou						
China (Chengdu)	cn-chengdu						
China (Hong Kong)	cn-hongkong				Submit a to enable the feature.		
Singapore (Singapore)	ap-southeast-1						
Australia (Sydney)	ap-southeast-2						
Malaysia (Kuala Lumpur)	ap-southeast-3						
Indonesia (Jakarta)	ap-southeast-5				Submit a to enable the feature.		
India (Mumbai)	ap-south-1						
Japan (Tokyo)	ap-northeast-1						
US (Silicon Valley)	us-west-1						
US (Virginia)	us-east-1						

Region	Region ID	Internet Firewall		VPC Firewall		NAT Firewall	DNS Firewall
		IPv4	IPv6	CEN transit router (Basic Edition) and Express Connect	CEN transit router (Enterprise Edition)		
Germany (Frankfurt)	eu-central-1						
UK (London)	eu-west-1						
UAE (Dubai)	me-east-1						

8.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 layer4.