ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall

Product Introduction

Document Version: 20201013

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 is the first Firewall as a Service (FWaaS) solution that is provided by Alibaba Cloud for public clouds. Cloud Firewall allows you to centrally manage the access control policies that are used to control north-south traffic from the Internet to your ECS instances and the microsegmentation policies that are used to control east-west traffic between ECS instances. Cloud Firewall provides a built-in intrusion prevention system (IPS). IPS allows you to view networkwide traffic and inter-business access relationships. Cloud Firewall is the primary infrastructure used to secure your business that have been migrated to Alibaba Cloud.

Protection scope of Cloud Firewall

Cloud Firewall can protect the following cloud assets or traffic:

- Internet traffic: traffic from public IP addresses of Elastic Compute Service (ECS), elastic IP addresses (EIPs) of Server Load Balancer (SLB), some public IP addresses of SLB, high-availability virtual IP addresses (HAVIP), EIPs, EIPs of ECS, EIPs of Elastic Network Interface (ENI), and EIPs of Network Address Translation (NAT) Gateway

  > **Note** Alibaba Cloud provides public and private SLB instances. Some public SLB instances cannot be protected by Cloud Firewall due to network architecture reasons. We recommend that you deploy private SLB instances and associate EIPs with the private SLB instances. For information about how to associate an EIP with an SLB instance, see Associate an EIP with an SLB instance.

- Traffic between VPCs: traffic between VPCs that are connected by using a CEN or Express Connect

Videos

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, CSA STAR, and PCI DSS.

References

Features

Billing

Traffic analysis overview

FAQ

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 layer4.

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

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.

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.Editions and regions

This topic describes the differences between Cloud Firewall editions and supported regions.

Differences in features and billing between Cloud Firewall editions

Feature or billing item	Trial Edition	Premium Edition	Enterprise Edition	Ultimate Edition
Basic price per month	Free of charge.	USD 420	USD 1,450	USD 3,900
Peak Internet bandwidth of protected traffic	Not supported.	Default value: 10 Mbit/s per month. You can increase the bandwidth. **Extra fee:** USD 7 per month for each increase of 1 Mbit/s of bandwidth.	Default value: 50 Mbit/s per month. You can increase the bandwidth. **Extra fee:** USD 7 per month for each increase of 1 Mbit/s of bandwidth.	Default value: 200 Mbit/s per month. You can increase the bandwidth. **Extra fee:** USD 7 per month for each increase of 1 Mbit/s of bandwidth.
Number of protected public IP addresses	Not supported.	Default value: 20. You can increase the quota. **Extra fee:** USD 7 per month for each additional public IP address that you want to protect.	Default value: 50. You can increase the quota. **Extra fee:** USD 7 per month for each additional public IP address that you want to protect.	Default value: 200. You can increase the quota. **Extra fee:** USD 7 per month for each additional public IP address that you want to protect.

Feature or billing item	Trial Edition	Premium Edition	Enterprise Edition	Ultimate Edition
Maximum number of access control policies Note If an access control policy involves multiple source CIDR blocks, destination CIDR blocks, or ports, this policy is counted as N policies. N = Number of source CIDR blocks × Number of destination CIDR blocks × Number of ports. If a policy involves only one source CIDR block, one destination CIDR block, and one port, this policy is counted as one policy.	Not supported.	4,000.	10,000.	20,000. You can submit a ticket to increase the quota.
Threat detection by using an intrusion prevention system (IPS) and installation of virtual patches	Not supported.	Supported.	Supported.	Supported.
IPS whitelist	Not supported.	Not supported.	Supported.	Supported.

Feature or billing item	Trial Edition	Premium Edition	Enterprise Edition	Ultimate Edition
Visualization of security group traffic	Not supported.	Not supported.	Supported.	Supported.
Synchronization of security group policies	Supported.	Not supported.	Supported.	Supported.
Isolation between VPCs	Not supported.	Not supported.	Supported.	Supported.
Number of protected VPCs	Not supported.	N/A.	Default value: 2. You can submit a ticket to increase the quota. **Extra fee**: USD 300 per month for each additional VPC that you want to protect.	Default value: 5. You can submit a ticket to increase the quota. **Extra fee**: USD 300 per month for each additional VPC that you want to protect.
Maximum inter-VPC traffic that can be protected	Not supported.	N/A.	100 Mbit/s	1 Gbit/s
Unified VPC protection across Alibaba Cloud accounts (with Cloud Enterprise Network enabled)	Not supported.	Not supported.	Not supported.	Supported.

Feature or billing item	Trial Edition	Premium Edition	Enterprise Edition	Ultimate Edition
Log audit (Logs are stored for seven days by default.) Note If you enable the log audit feature, Cloud Firewall stores the logs generated in the last six months and allows you to export the logs.	Not supported.	Provides quintuple logs. Note A quintuple log contains the information of a source IP address, a source port, a destination IP address, a destination port, and a transport layer protocol.	Provides quintuple logs.	Provides quintuple logs.
Expert service	Not supported.	Supported.	Supported.	Supported.
Cluster deployment	Not supported.	Uses shared resources.	Uses shared resources.	Uses dedicated resources. You can submit a ticket to change resource specifications.
Subscription mode	Free trial.	Shortest subscription period: six months.	Monthly subscription supported.	Monthly subscription supported.

Regions supported by Cloud Firewall

Log on to the Cloud Firewall console. In the left-side navigation pane, click Firewall Settings and then the Internet Firewall tab to view the supported regions.

Note Before you purchase Cloud Firewall, make sure that your cloud assets are deployed in the regions supported by Cloud Firewall. Cloud assets include public IP addresses of Elastic Compute Service (ECS), elastic IP addresses (EIPs) of Server Load Balancer (SLB), high-availability virtual IP addresses (HAVIP), EIPs, EIPs of ECS, EIPs of Elastic Network Interface (ENI), public IP addresses of SLB, and EIPs of Network Address Translation (NAT) Gateway. If your cloud assets are not deployed in regions supported by Cloud Firewall, Cloud Firewall cannot protect these assets even if you have purchased Cloud Firewall. In this case,submit a ticket to apply for a refund.

Alibaba Cloud account type	Supported region
Account registered on the International site (alibabacloud.com)	**Regions in China:** • China (Beijing) • China (Zhangjiakou-Beijing Winter Olympics) • China (Hangzhou) • China (Shanghai) • China (Shenzhen) • China (Hong Kong)
	Regions outside China: • Singapore (Singapore) • Malaysia (Kuala Lumpur) • Indonesia (Jakarta) • Germany (Frankfurt)

VPC firewall limits

A VPC firewall helps you detect and control the traffic between VPCs that are connected by using Express Connect or Cloud Enterprise Network (CEN). Different network environments have different limits for enabling VPC firewalls. For more information, see VPC firewall limits.

7.FAQ

Can Cloud Firewall protect public SLB instances?

Alibaba Cloud provides public and private SLB instances. Some public SLB instances cannot be protected by Cloud Firewall due to network architecture reasons. We recommend that you deploy private SLB instances and associate EIPs with the private SLB instances. For information about how to associate an EIP with an SLB instance, see Associate an EIP with an SLB instance.

> **Note** For a public SLB instance that is in use and is not protected by Cloud Firewall, we recommend that you do not change the network type of the instance by yourself. If you need any help, contact SLB technical support.

What are the protected bandwidth quotas of Cloud Firewall in different editions?

Cloud Firewall can protect your Internet traffic and traffic between VPCs. Cloud Firewall in different editions have different protected bandwidth quotas:

- For Internet traffic, the default protected bandwidth quota per month is 10 Mbit/s in Premium Edition, 50 Mbit/s in Enterprise Edition, and 200 Mbit/s in Ultimate Edition.
- For traffic between VPCs, the default protected bandwidth quota per month is 100 Mbit/s in Enterprise Edition and 1 Gbit/s in Ultimate Edition. No protection is provided in Premium Edition.

For more information, see Features and billing items of each edition.

8.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.
- 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.