ALIBABA CLOUD

Alibaba Cloud

云防火墙

产品简介

文档版本：20220706

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是云防火墙？

阿里云云防火墙是一款云平台SaaS（Software as a Service）化的防火墙，可针对您云上网络资产的互联网边界、VPC边界及主机边界实现三位一体的统一安全隔离管控，是您业务上云的第一道网络防线。

云防火墙支持防护的范围

云防火墙可以防护以下云资产或流量：

- 互联网方向：ECS公网IP、SLB EIP、SLB公网IP、HAVIP、EIP、ECS EIP、ENI EIP、NAT EIP。
- VPC到VPC之间：已使用云企业网或高速通道实现两个VPC之间的互通。
- VPC和本地数据中心（IDC）之间：已使用VBR实现VPC和IDC之间互通。

合规认证

云防火墙已通过ISO 9001、ISO 20000、ISO 22301、ISO 27001、ISO 27017、ISO 27018、ISO 29151、ISO 27701、BS 10012、CSA STAR、PCI DSS认证。

联系我们

如果您在购买云防火墙时遇到产品功能、产品价格、产品选型等售前问题，或期望试用云防火墙产品，可通过钉钉与阿里云联系。使用钉钉加入阿里云云防火墙问题答疑群聊（群号：33081734），您将可以得到阿里云云防火墙安全专家的指导建议。

相关文档

- 功能特性
- 计费方式（包年包月）
- 云防火墙支持防护的范围

2.功能特性

阿里云云防火墙是一款云平台SaaS（Software as a Service）化的防火墙，可统一管理南北向和东西向的流量，提供流量监控、精准访问控制、实时入侵防御等功能，全面防护您的网络边界。本文介绍了云防火墙的功能特性及不同功能特性在不同版本中的支持情况。

功能列表

下表介绍了云防火墙的功能特性和支持的版本信息。关于包年包月云防火墙的计费方式详情，请参见计费方式（包年包月）。

> **说明**
>
> - ×：表示指定版本的云防火墙不支持该功能。
> - ✓：表示指定版本的云防火墙支持该功能。

应用场景	功能名称	描述	免费版	高级版	企业版	旗舰版
云上网络访问流量分析与攻击感知	概览	提供已开启和未开启的防御能力总览，并为您展示最近7天访问流量统计数据和已检测出的安全风险统计数据。	×	✓	✓	✓
访问控制	互联网边界防火墙	支持互联网通信协议为IPv4的入方向和出方向流量进行访问控制（南北向）；支持基于域名的访问控制，严格控制主动外联的出流量。	×	✓	✓	✓
	VPC边界防火墙	支持VPC间流量访问控制。	×	×	✓	✓
	主机边界防火墙	支持内网ECS之间的访问控制（东西向）。	×	×	✓	✓
	安全组检查	支持检查ECS服务器安全组中存在高危风险的规则，并提供修复建议，帮助您更安全、更高效地使用安全组功能。	✓	✓	✓	✓
网络流量分析	主动外联活动	实时监控云资产主动外联的行为。	×	✓	✓	✓
	互联网访问活动	支持云上网络访问流量统计和分析。	×	✓	✓	✓
	VPC访问活动	实时监控VPC专有网络之间的流量情况，帮助您实时获取VPC网络流量数据，及时发现和排查异常流量。	×	×	✓	✓
	全量活动搜索	支持基于过滤条件对经过云防火墙的访问流量进行搜索。	×	✓	✓	✓

应用场景	功能名称	描述	免费版	高级版	企业版	旗舰版
攻击防护	漏洞防护	实时检测可被攻击利用的漏洞，并提供针对此类漏洞的攻击防御能力。	×	✓	✓	✓
	失陷感知	由威胁检测引擎实时检测入侵活动及其详细信息，并提供对应的处置方案。	×	✓	✓	✓
	入侵防御	展示了云防火墙对互联网出方向、入方向的流量和VPC间流量防护的详细信息。	×	✓	✓	✓
	防护配置	内置威胁检测引擎，详细介绍如下： • 支持入侵防御功能并同步进行智能阻断。支持被阻断访问分析，识别被云防火墙和IPS阻断的网络流量。 • 支持威胁情报联动功能，同步阿里云全网的恶意IP（如恶意访问源、扫描源、中控服务等），对威胁和入侵做到提前防御。 • 内置云平台攻防实战中积累的入侵防御规则，威胁识别率高、误报率小。 • 支持虚拟补丁，无需在业务系统上安装补丁即可实时修复。可对热门漏洞进行精准防护。 注意 按量付费版不支持威胁情报功能，也不支持查看规则明细和自定义规则。	×	✓	✓	✓
日志分析	日志审计	提供日志审计和行为回溯功能，详细介绍如下： • 提供事件日志，可实时查看经过互联网边界防火墙和VPC边界防火墙的流量相关的事件日志。 • 提供流量日志，可查看经过云防火墙的所有流量数据。您可在威胁事件发生的时候通过查看流量日志进行流量和访问源分析，并查看配置的访问控制策略是否生效。 • 提供系统操作日志，可查看云防火墙所有的配置和操作记录。	×	✓	✓	✓
	日志分析	实时地自动采集并存储（存储时长可自定义7~365天）出、入方向的流量日志，并进行分析；支持基于特定指标，定制实时的监测与告警，确保在关键业务发生异常时您能及时响应。	×	✓	✓	✓

应用场景	功能名称	描述	免费版	高级版	企业版	旗舰版
常用网络流量检测工具	工具箱 涉及的文档如下： • 策略备份与回滚 • 网络抓包 • 互联网边界防火墙-严格模式	提供互联网边界防火墙和VPC边界防火墙的访问控制策略备份及回滚功能。	×	×	✓	✓
		支持网络抓包功能，帮助您定位网络故障和分析攻击行为。	×	×	✓	✓
		支持互联网边界防火墙-严格模式。该模式对命中访问控制策略，但应用类型未被云防火墙识别（Unknown）的流量提供一键拦截功能。	×	✓	✓	✓
		支持等保合规检测。	✓	✓	✓	✓
业务可视	自定义分组	支持通过自定义分组建立云资产的应用和应用组、业务区之间的关系。	×	✓	✓	✓
多账号管控	统一账号管理	支持添加其他阿里云成员账号，帮助您实现资源的统一管理。	×	×	×	✓

3.产品优势

阿里云云防火墙是一款云平台SaaS化的防火墙，可统一管理南北向和东西向的流量，保护您的网络安全。阿里云云防火墙操作简便、即开即用，支持精准访问控制和全网流量可视化。

全托管方式

云防火墙服务采用SDN技术，提供SaaS化的防火墙方案。服务由阿里云托管提供，无需您部署任何设备（传统防火墙的镜像安装、路由设置等复杂基础系统和网络配置操作），也无需您关注容灾、扩容或接入等问题。

简单易用

您购买了云防火墙、在控制台完成简单的设置后，可立即使用、秒级接入、即刻防御，同时有效降低网络安全管控运维成本。

支持平滑扩展

云防火墙采用了集群部署的模式，支持性能的平滑扩展，针对单个IP的防护流量可达2 Gbps；防护流量超过2 Gbps时云防火墙支持定制。

系统稳定可靠

默认高可用，采用双可用区部署，任意一台服务器或者任意一个可用区故障时都不会导致云防火墙故障。

云上深度集成

云防火墙为您的资产提供了完整的南北向和东西向访问控制能力，帮助您的业务建立完整的访问控制和安全隔离能力。

原生整合阿里云各类网络服务（如VPC、CEN、EIP、SLB等），通过在网络层面控制对常用云资产的访问，联动终端安全能力，解决对云资产的异常访问问题，实现响应闭环。

实时入侵防御

内置威胁检测引擎，可同步更新全网威胁情报，对超过500万的活跃恶意IP与域名条目进行监控，实现对来自互联网的威胁进行实时检测和阻断。同时，提供基于网络杀伤链，在重要的网络攻击阶段进行针对性的网络防御。

业务关系可视

云防火墙通过拓扑图直观地展现资产以及资产的访问关系。无需配置，开通服务后就可了解业务的分区、分组、资产、资产间的访问关系，以及用户流量的聚类分析。支持流量可视分析，最大程度保证策略的正确性。

满足等保合规2.0要求

满足《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》（简称“等保合规2.0”）的边界防护和访问控制等要求。

4.应用场景

云防火墙是用户上云后的安全组件，支持全网流量识别、统一策略管控、入侵检测、日志等核心功能。

云防火墙不仅可以防护从互联网到业务的访问流量，同时还能控制业务到互联网的主动外联访问，并对业务和业务间的访问进行控制。

互联网边界访问控制

对出、入互联网的访问流量进行管控，拦截来自互联网的攻击和威胁，例如黑客入侵、挖矿和恶意流量等。

内网访问控制

对内网中ECS服务器之间的访问流量进行管控，对不同的业务进行安全隔离，避免因某个ECS存在安全风险从而对整个云上业务产生安全威胁。

VPC边界访问控制

对VPC间的访问流量进行管控，实现VPC的分区防御。

入侵防御

对云资产主动外联的行为、互联网访问流量和内网ECS互访流量进行检测和分析，帮助您实时了解网络流量动态，以判断哪些云资产已经处于风险状态，并对这些异常行为进行实时阻断，防御潜在的风险。

流量可视化

让您全面了解资产的信息和访问关系，从而及时发现异常流量。

等保合规

存储云资产的访问日志，助力网站符合等保合规要求。

> **说明** 高级版支持存储180天的访问日志；企业版和旗舰版支持存储7~360天的访问日志。

5.常见问题

云防火墙支持防护的范围

云防火墙可以防护以下云资产或流量：

- 互联网方向：ECS公网IP、SLB EIP、SLB公网IP、HAVIP、EIP、ECS EIP、ENI EIP、NAT EIP。
- VPC到VPC之间：已使用云企业网或高速通道实现两个VPC之间的互通。
- VPC和本地数据中心（IDC）之间：已使用VBR实现VPC和IDC之间互通。

云防火墙提供的防护带宽流量是多少？

云防火墙可以对您公网方向的流量和VPC之间的流量进行防护，您可根据需要扩展防护流量带宽。根据您购买的服务版本的不同，云防火墙提供不同规格的防护带宽：

- 公网方向的流量：高级版默认10 Mbps/月，企业版默认50 Mbps/月，旗舰版默认200 Mbps/月。
- VPC间流量：高级版不提供防护，企业版默认100 Mbps/月，旗舰版默认1 Gbps/月。

详细内容，请参见云防火墙功能与计费表。

云防火墙带宽是否支持临时升级？

支持。云防火墙带宽支持按天进行升级。详细内容，请参见带宽升级（临时升级）。

云防火墙是否支持跨账号（多账号）统一管理？

云防火墙旗舰版支持跨账号统一管理，高级版和企业版不支持。有关跨账号统一管理的详细介绍，请参见统一账号管理。

产品试用与售前咨询

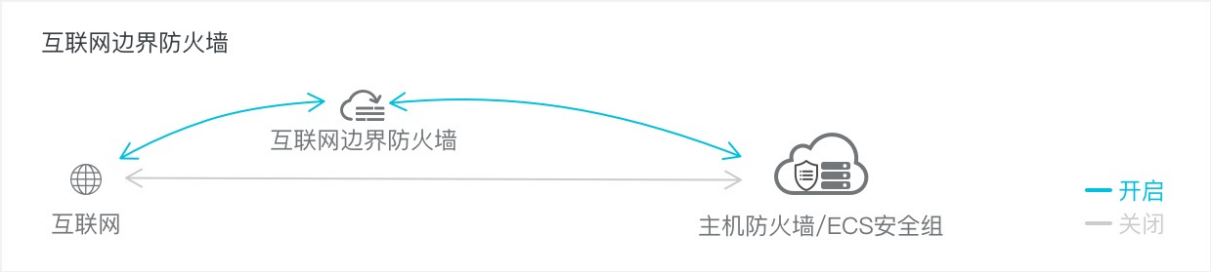
如果您在购买云防火墙时遇到产品功能、产品价格、产品选型等售前问题，或期望试用云防火墙产品，可通过钉钉与阿里云联系。

6.基本概念

本文主要介绍了云防火墙相关的基本概念。

互联网边界防火墙

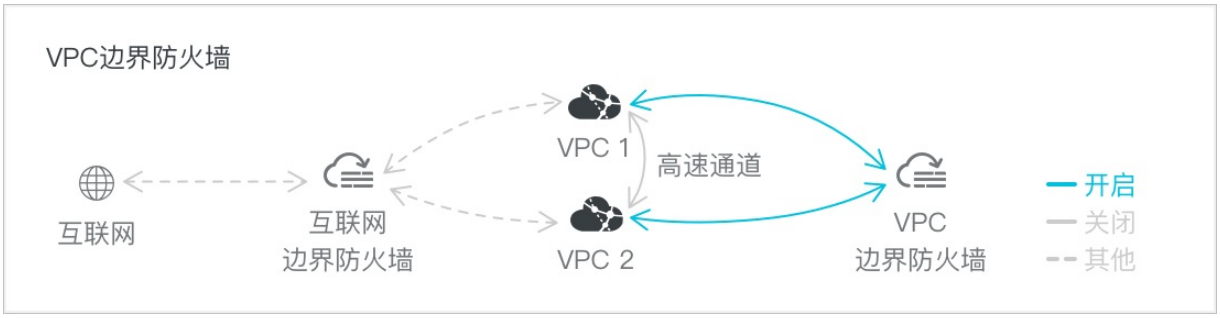
互联网边界防火墙主要用于检测互联网和云上资产间的通信流量，它是一种集中式管理的防火墙。互联网边界防火墙部署在互联网和用户主机之间，原理图示：



互联网边界防火墙内置威胁入侵防御模块，支持失陷主机检测、主动外联行为的阻断、业务访问关系可视等功能。互联网边界防火墙支持一键开启防护，无需复杂的网络接入配置和镜像文件安装，使用集群化部署方式，支持性能平滑扩展。

VPC边界防火墙

VPC边界防火墙主要用于检测两个VPC间的通信流量，是一种分布式防火墙。VPC边界防火墙部署在两个VPC网络之间，原理图示：



VPC边界防火墙仅支持部署在高速通道联通的两个VPC网络之间，或同一个云企业网的两个VPC网络之间。VPC边界防火墙不会默认存在，需要您指定两个VPC网络进行创建。

安全组和主机防火墙

安全组是ECS提供的分布式虚拟主机防火墙，具备状态检测和数据包过滤功能，用于设置ECS实例间的网络访问控制。安全组是由同一个地域（Region）内具有相同安全防护需求并相互信任的实例组成。在创建实例的时候您需要指定安全组，每个实例至少属于一个安全组。

主机防火墙底层使用了安全组的功能，您既可以在**访问控制**页面的**主机边界防火墙**页签下配置策略，也可以在**ECS管理控制台**配置策略，两边配置自动保持同步。

主动外联

主动外联是指阿里云主机主动访问外部IP的连接分析，可以帮助您及时发现可疑主机。

失陷感知

失陷感知是一种监控网络传输，检查是否有可疑活动的系统，在检测到可疑事件时发出告警或者采取主动反应措施。云防火墙集成阿里云近十年检测防御能力，对经过云防火墙的流量进行实时分析、统计，智能发现失陷主机、阻断异常网络活动。

开放应用、开放端口、开放公网IP

开放应用指您暴露在互联网上的应用，如HTTP、SSH等。

开放端口指您暴露在互联网上的端口，如80、22等。

开放公网IP指您暴露在互联网上的资产的公网IP。

目前云防火墙支持识别以下几种资产的公网IP：

- EIP（支持绑定到专有网络类型的ECS实例、专有网络类型的私网SLB实例、弹性网卡和NAT网关上）
- NatPublicIp（ECS系统分配的公网IP）

应用组

应用组是云防火墙东西向业务可视中提供的相同或相似服务的应用集合，如所有部署了MySQL的ECS可以归属到同一个DB应用组。

应用是云防火墙东西向业务可视的最小单位，默认情况下一个应用等于一台ECS上所有开放端口的集合，您可以通过指定端口的克隆应用来创建新的应用。

业务区

业务区是云防火墙东西向业务可视中构成您某个业务的各个应用组的集合，如门户网站业务区包含Web应用组、DB应用组等。

高危应用组和高危业务区

高危应用组指开放了高危端口（如445端口）的应用集合。每一个高危端口会独立产生一个高危应用组。

高危业务区是高危应用组的集合。

高危业务区和高危应用组可以帮助您发现哪些ECS实例开放了不安全的高危端口以及具体哪些ECS访问了高危端口。

目前高危业务区由云防火墙自动创建和识别。

依赖区和被依赖区

依赖区和被依赖区是云防火墙东西向业务可视中提供的抽象概念，是指两个业务区的访问关系。如业务区A访问了业务区B，那么我们称业务区B是业务区A的依赖区，而业务区A是业务区B的被依赖区。

首次流量

首次流量指源IP到目的IP的访问流量在统计周期内第一次出现。您可以根据首次流量出现的时间、源IP和目的IP等信息，进一步排查首次流量出现的原因。通常情况下首次流量由新业务上线或者入侵造成。

地址簿

为了方便您引用IP地址或端口信息，实现IP地址或端口的灵活配置，云防火墙支持将多个IP地址或者多个端口指定成一个地址簿。在配置时，只需要引用该地址簿即可实现对多个IP地址或端口的批量配置。

云防火墙目前支持四类地址簿：

- IP地址簿：您可以配置一组IP地址。
- 端口地址簿：您可以配置一组端口。

- 域名地址薄：您可以配置一组域名。
- 云地址薄：您可以配置一组IP地址或域名。

地址簿还具有以下特点：

- 云防火墙内置一些全局地址簿，全局地址簿不可以编辑也不可以删除。
- 多个地址簿可以包含同一个IP地址或端口。
- 地址簿内IP或端口变动，在访问控制策略中会自动生效。

7.支持的地域

本文为您介绍云防火墙支持的地域信息。

您可以参考以下表格，查询云防火墙功能（互联网边界防火墙、VPC边界防火墙、NAT防火墙、DNS防火墙）在不同地域下的支持情况。

> **说明** 其中✓表示支持，×表示不支持。

地域名称	地域代码	互联网边界防火墙		VPC边界防火墙		NAT防火墙	DNS防火墙
		IPv4	IPv6	高速通道和云企业网（TR基础版）	云企业网（TR企业版）		
华北1（青岛）	cn-qingdao	×	×	×	×	×	×
华北2（北京）	cn-beijing	✓	×	✓	×	×	×
华北3（张家口）	cn-zhangjiakou	✓	×	×	×	×	×
华北5（呼和浩特）	cn-huhehaote	×	×	×	×	×	×
华北6（乌兰察布）	cn-wulanchabu	×	×	×	×	×	×
华东1（杭州）	cn-hangzhou	✓	×	×	×	×	×
华东2（上海）	cn-shanghai	✓	×	✓	×	×	×
华南1（深圳）	cn-shenzhen	✓	×	✓	×	×	×
华南2（河源）	cn-heyuan	✓	×	×	×	×	×
华南3（广州）	cn-guangzhou	×	×	×	×	×	×
西南1（成都）	cn-chengdu	×	×	×	×	×	×

地域名称	地域代码	互联网边界防火墙		VPC边界防火墙		NAT防火墙	DNS防火墙
		IPv4	IPv6	高速通道和云企业网（TR基础版）	云企业网（TR企业版）		
中国（香港）	cn-hongkong	✓	×	✓	提工单开启	×	×
亚太东南1（新加坡）	ap-southeast-1	✓	×	✓	✓	×	×
亚太东南2（悉尼）	ap-southeast-2	×	×	×	×	×	×
亚太东南3（吉隆坡）	ap-southeast-3	✓	×	✓	×	×	×
亚太东南5（雅加达）	ap-southeast-5	✓	×	×	提工单开启	×	×
亚太南部1（孟买）	ap-south-1	✓	×	×	×	×	×
亚太东北1（东京）	ap-northeast-1	✓	×	×	×	×	×
美国西部1（硅谷）	us-west-1	✓	×	×	×	×	×
美国东部1（弗吉尼亚）	us-east-1	×	×	×	×	×	×
欧洲中部1（法兰克福）	eu-central-1	✓	×	×	×	×	×
英国（伦敦）	eu-west-1	✓	×	×	×	×	×
中东东部1（迪拜）	me-east-1	×	×	×	×	×	×

8.技术原理

云防火墙是阿里云云盾团队结合云的部署便捷、弹性扩展等技术优势，为云上客户量身定制的融合访问控制、业务隔离、流量识别等功能的网络安全产品。

云防火墙主要由以下两个控制模块组成：

- **南北向流量控制模块**：主要用于实现互联网到主机间的访问控制，支持4-7层访问控制。
- **东西向流量控制模块**：主要是利用安全组对主机之间的交互流量进行控制，实现4层访问控制。