ALIBABA CLOUD

Alibaba Cloud

云防火墙

产品简介

文档版本：20201119

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（Cloud Firewall）是业界首款公共云环境下的SaaS化防火墙，可统一管理互联网到业务的访问控制策略（南北向）和业务与业务之间的微隔离策略（东西向）。内置的威胁入侵检测模块（IPS）支持全网流量可视和业务间访问关系可视，是您业务上云的第一个网络安全基础设施。

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、部分SLB公网IP（详见以下说明）、HAVIP、EIP、ECS EIP、ENI EIP、NAT EIP。

  > **说明** 阿里云提供公网和私网两种类型的负载均衡（SLB）服务。由于历史网络架构的原因，部分公网SLB不支持云防火墙引流，推荐您采用私网SLB加EIP的方案（详细内容请参见绑定EIP），将流量牵引到云防火墙上进行防护。

- VPC间：已使用云企业网或高速通道连接VPC间通信的流量。

产品介绍视频

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。

相关文档

功能特性

计费方式

概述

云防火墙支持防护的范围

2.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。

3.功能特性

阿里云云防火墙是业界首款云平台SaaS化的防火墙，可统一管理南北向和东西向的流量，提供流量监控、精准访问控制、实时入侵防御等功能，全面保护您的网络安全。

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。

应用场景	功能名称	描述	支持的版本	相关文档
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。	所有付费版本	概览
访问控制	互联网边界防火墙	支持互联网双向访问控制（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。	所有付费版本	互联网边界防火墙（内外双向流量）
	VPC边界防火墙	支持VPC间流量访问控制。	仅企业版、旗舰版	VPC边界防火墙
	主机边界防火墙	支持内网ECS之间的微隔离（东西向）。	所有付费版本	主机边界防火墙（ECS实例间）
网络流量实时监控和分析	主动外联活动	实时监控云资产主动外联的行为。	所有付费版本	主动外联活动
	互联网访问活动	支持云上网络访问流量统计和分析。	所有付费版本	互联网访问活动
	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。	仅企业版、旗舰版	VPC访问活动
	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。	所有付费版本	失陷感知
	IPS拦截记录	云防火墙提供入侵防御功能并同步进行智能阻断，提供被阻断的访问流量分析，帮助您有效识别被云防火墙阻断的网络流量。	所有付费版本	IPS拦截记录
	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。	所有付费版本	全量活动搜索
	漏洞攻击防护	实时检测可被网络侧攻击利用的漏洞，并提供针对此类漏洞的攻击防御能力。	所有付费版本	漏洞攻击防护

应用场景	功能名称	描述	支持的版本	相关文档
入侵防御	入侵防御	• 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。 • 威胁情报联动：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。 • 内置云平台长期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、高危0day和N day漏洞的利用进行精准防护。	所有付费版本	入侵防御开关
日志	日志审计	提供日志审计和行为回溯，详细介绍如下： • 提供事件日志，可实时查看被入侵防御模块检测和拦截到的威胁或入侵事件。 • 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。	所有付费版本	日志审计
	日志分析	实时地自动采集并存储（存储时长可达6个月）出、入方向的流量日志并进行分析；支持基于特定指标定制准实时的监测与告警，确保在关键业务发生异常时能及时响应。	所有付费版本	开通日志分析服务
常用网络流量检测工具	工具箱	提供网络抓包、策略回滚、安全组配置检查等功能，帮助您全面了解经过云防火墙的网络流量。	• 安全组配置检查和等保合规检测功能支持免费版和所有付费版本。 • 网络抓包、策略备份与回滚功能仅支持付费版本。	策略回滚 网络抓包 安全组配置检查
业务可视	安全组可视、应用分组可视	支持业务可视，帮助您全面了解云资产的信息和访问关系。	所有付费版本	安全组可视 应用分组可视
	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。	所有付费版本	自定义分组

4.产品优势

阿里云云防火墙是业界首款云平台SaaS化的防火墙，可统一管理南北向和东西向的流量，全面保护您的网络安全。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，首次在公共云提供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Available Zone （AZ，可用区）部署，任意一台服务器或者任意一个AZ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。

满足等保合规要求

满足等保要求中的边界防护和访问控制等要求。

5.应用场景

云防火墙是用户上云后的首个安全组件，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6个月以上的访问日志，助力网站符合等保合规要求。

6.产品版本与使用限制

本文档介绍了云防火墙不同版本功能差异和支持的地域。

产品版本功能与计费项

各版本支持的功能与计费项	基础版	高级版	企业版	旗舰版	说明
基础价格	免费	420 USD/月	1,450 USD/月	3,900 USD/月	无
公网方向可防护的流量峰值	不支持	默认10 Mbps/月（可扩展）。	默认50 Mbps/月（可扩展）。	默认200 Mbps/月（可扩展）。	**额外费用**：扩展带宽7 USD/Mbps/月。
支持防护的公网IP数	不支持	默认支持20个（可扩展）。	默认支持50个（可扩展）。	默认支持400个（可扩展）。	**额外费用**：扩展公网IP 7 USD/个/月。
支持的访问控制策略最大条数	不支持	• 互联网边界防火墙策略：4,000条 • VPC边界防火墙策略：4,000条	• 互联网边界防火墙策略：10,000条 • VPC边界防火墙策略：10,000条	• 互联网边界防火墙策略：20,000条 • VPC边界防火墙策略：20,000条 （可提交工单申请扩展）	策略条数按照访问控制策略管控的流量条数来计算，即单个策略中源地址、目的地址或端口地址含多个IP地址段或端口的时候，该策略的条数计算为**源地址段个数*目的地址段个数*端口个数**；单个策略如果只涉及单个源地址段、单个目的地址段和单个端口，则计算为**1条**策略。
IPS威胁检测、虚拟补丁	不支持	支持	支持	支持	无
IPS白名单	不支持	不支持	支持	支持	无
安全组流量可视	不支持	不支持	支持	支持	无
同步安全组的策略配置	支持	不支持	支持	支持	无
VPC间防护隔离	不支持	不支持	支持	支持	无

各版本支持的功能与计费项	基础版	高级版	企业版	旗舰版	说明
支持防护的VPC数量	不支持	无	默认支持2个VPC，可提交工单申请扩展。	默认支持5个VPC，可提交工单申请扩展。	对于企业版和旗舰版用户，扩展VPC的**额外费用**300 USD/个/月。
可防护的VPC间最大流量	不支持	无	100 Mbps	1 Gbps	无
多账号下VPC间统一防护（云企业网打通）	不支持	不支持	不支持	支持	无
日志审计（默认存储7天）	不支持	提供五元组日志 **说明** 五元组是指源IP地址、源端口、目的IP地址、目的端口和传输层协议。	提供五元组日志	提供五元组日志	开通云防火墙日志分析功能，可以存储6个月的日志，并支持日志的导出备份。
专家服务	不支持	支持	支持	支持	无
集群部署	不支持	共享资源	共享资源	独享资源，如需其他规格可提交工单定制。	无
售卖规格	免费（无需开通即可使用）	最少购买6个月。	支持按月购买。	支持按月购买。	无

云防火墙支持的地域

您可以登录云防火墙控制台在**互联网边界防火墙**页面查看云防火墙支持的地域。

云防火墙支持的地域界面

说明 购买云防火墙前，请确认您的云资产在云防火墙支持的地域内。云资产包括：ECS公网IP、SLB EIP、HAVIP、EIP、ECS EIP、ENI EIP、SLB公网IP、NAT EIP。如果您的上述云资产不在云防火墙支持的地域内，即使购买了云防火墙后也无法使用云防火墙的服务。这种情况下，您需要提交工单申请退款。

云账号所在地区	支持的地域
国际站账号	**中国地域：** • 华北2（北京） • 华北3（张家口） • 华东1（杭州） • 华东2（上海） • 华南1（深圳） • 中国香港
	中国以外地域： • 新加坡 • 马来西亚（吉隆坡） • 印度尼西亚（雅加达） • 德国（法兰克福） • 日本（东京）

VPC边界防火墙限制说明

VPC边界防火墙帮助您检测和管控高速通道或云企业网中两个VPC间的通信流量。由于您业务的网络环境不同，开启VPC边界防火墙存在一定的限制条件。详细内容请参见VPC边界防火墙限制说明。

7.售前常见问题

云防火墙是否支持对公网SLB的访问？

阿里云提供公网和私网两种类型的负载均衡（SLB）服务。由于历史网络架构的原因，部分公网SLB不支持云防火墙引流，推荐您采用私网SLB加EIP的方案（详细内容请参见绑定EIP），将流量牵引到云防火墙上进行防护。

> **说明** 对于已使用了公网SLB的用户，云防火墙无法防护来自公网SLB的流量。不建议您自行对网络进行变更处理。如有任何需要，请联系SLB技术支持。

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。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、部分SLB公网IP（详见以下说明）、HAVIP、EIP、ECS EIP、ENI EIP、NAT EIP。

  > **说明** 阿里云提供公网和私网两种类型的负载均衡（SLB）服务。由于历史网络架构的原因，部分公网SLB不支持云防火墙引流，推荐您采用私网SLB加EIP的方案（详细内容请参见绑定EIP），将流量牵引到云防火墙上进行防护。

- VPC间：已使用云企业网或高速通道连接VPC间通信的流量。

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。使用钉钉扫描下方的二维码，您将可以得到阿里云云防火墙安全专家的指导建议。

8.常见术语

本文档主要介绍了云防火墙相关的常见术语。

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，缺省集群化部署，支持性能的平滑扩展。

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积累，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，如门户网站业务区将包含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

为了方便的引用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。