云防火墙

快速入门

文档版本 02

发布日期 2023-11-07

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

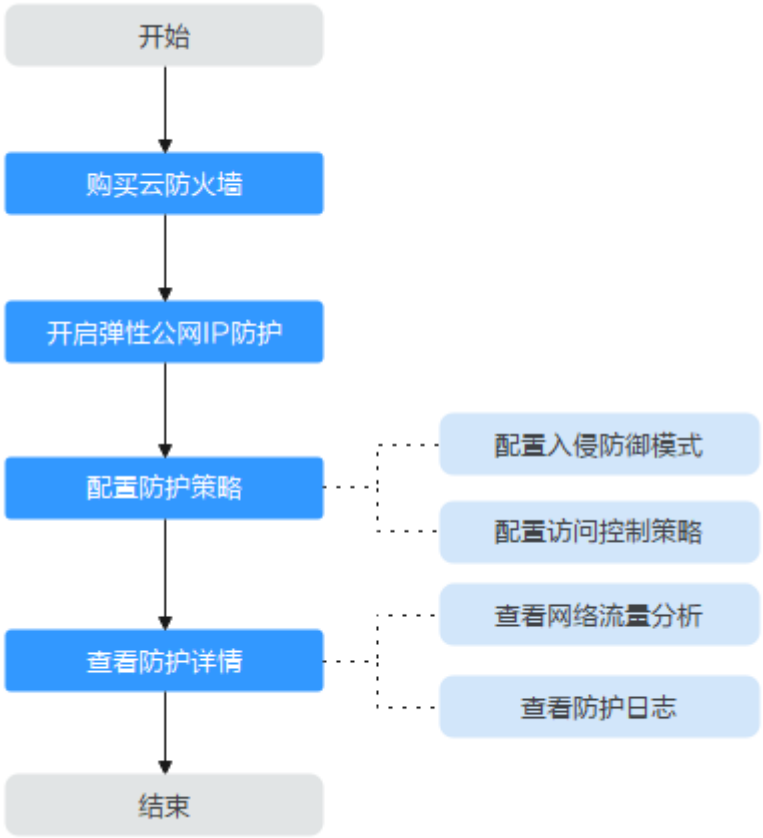
目 录

1 入门指引

云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。

本文档介绍如何使用云防火墙防护互联网边界，使用流程如**图 使用流程**所示。

图 1-1 使用流程



2 步骤一：购买云防火墙

云防火墙支持包周期方式购买，本节介绍如何购买云防火墙。

版本信息说明

云防火墙提供了“基础版”、“标准版”、“专业版”供您使用，包括访问控制、入侵防御、流量分析以及日志审计等功能。

表 2-1 版本差异说明

功能		基础版	标准版	专业版
防护规格	防护互联网边界公网IP数	20个（不可扩容）	20个（可扩容）	50个（可扩容）
	防护互联网边界的流量峰值	10Mbps（不可扩容）	10Mbps（可扩容）	50Mbps（可扩容）
	防护的VPC数量	×	×	2个（可扩容）
	防护的VPC间最大流量峰值	×	×	200Mbps（随VPC数量扩容）
访问流量控制	公网资产ACL访问控制（基于IP、域名、域名组、地理位置等）	√（仅支持通过Host或SNI字段匹配策略）	√	√
	南北向流量防护，统一隔离防护云上资产在互联网的暴露风险（含EIP、ECS公网IP等）	√	√	√
	南北向流量审计，日志查询	√（仅支持访问控制日志和流量日志）	√	√

功能		基础版	标准版	专业版
	东西向流量防护，VPC间的资产保护、全流量分析	×	×	√
	东西向流量监控，实时获取VPC间流量数据	×	×	√
防护策略	入侵防御IPS	×	√	√
	自定义IPS特征库	×	×	√
	虚拟补丁	×	√	√
	敏感目录、反弹Shell	×	√	√
	病毒防御AV	×	×	√

购买包年/包月防火墙

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 单击“购买云防火墙”，进入“购买云防火墙”页面，相关参数如表2-2所示。

表 2-2 购买包年/包月云防火墙的参数说明

参数名称	参数说明
区域	购买云防火墙的区域。 **须知** 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**云防火墙支持哪些区域？** 。
版本规格	选择版本： • 标准版 • 专业版 **说明** 各版本之间的具体差异请参见**服务版本差异**。
引擎类型	直路引擎：直路部署。具备精细化应用管控，可为用户提供灵活的安全访问控制，包括策略阻止、会话限制等。同时，还具备入侵防御、病毒过滤、攻击防护等功能，满足客户安全访问、攻击防护以及应用识别和控制等需求。

参数名称	参数说明
扩展防护公网IP数	（可选）选择需扩展的防护公网IP数，可选择范围：0~2000个 **说明** 此处为套餐外购买数量，例如标准版防护公网IP数默认20个（套餐内费用包含），如果您的公网IP是65个，那么只需要填写45个。
扩展防护流量峰值	（可选）选择需扩展的防护流量峰值（出流量或入流量的最大峰值），可选择范围：0~5000Mbps/月（需为5的整数倍） **说明** • 此处为套餐外购买流量值，例如标准版防护互联网边界流量峰值默认10Mbps/月（套餐内费用包含），如果您的防护流量是200Mbps/月，那么只需要填写190Mbps/月。 • 防护流量按照出流量或入流量的最大峰值取值。
企业项目	在下拉列表中选择您所在的企业项目。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。
防火墙名称	设置当前防火墙的名称。 命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）、空格和特殊字符（-_）。 • 长度支持1-48个字符。
高级设置	标签：如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，请参见**资源标签简介**。 如您的组织已经设定云防火墙的相关标签策略，则需按照标签策略规则为防火墙实例添加标签。标签如果不符合标签策略的规则，则可能会导致防火墙创建失败，请联系组织管理员了解标签策略详情。
购买时长	自主选择购买时长。 选择时长后，可勾选“自动续费”若您勾选并同意自动续费，则在服务到期前，系统会自动按照购买周期生成续费订单并进行续费，无需手动续费。自动续费规则请参见**自动续费规则说明**。

步骤5 确认购买信息无误后，单击“立即购买”。

步骤6 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

生效条件

付款成功后，您可以在管理控制台左上方查看当前购买的CFW版本以及配额信息。

3 步骤二：开启弹性公网 IP 防护

当您首次使用云防火墙时，需要先进行资产同步并对EIP资产开启防护，才能将您的业务流量经过云防火墙。

开启防护后，云防火墙的默认防护动作为“放行”，将根据您后续设置的防护策略实施拦截。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在左侧导航栏中，选择“资产管理 > 弹性公网IP管理”，进入“弹性公网IP管理”页面，弹性公网IP信息将自动更新至列表中。

步骤6 开启弹性公网IP。

- 开启单个弹性公网IP。在所在行的“操作”列中，单击“开启防护”。
- 开启多个弹性公网IP。勾选需要开启防护的弹性公网IP，单击表格上方的“开启防护”。

须知

- 一个EIP只能在一个防火墙上开启防护。
- 仅支持当前账号所属企业项目下的弹性公网IP。

步骤7 在弹出的界面确认信息无误后，单击“绑定并开启防护”，可查看操作行的“防护状态”列显示“防护中”。

说明

EIP开启防护后，访问控制策略默认动作为“放行”。

----结束

4 步骤三：配置防护策略

4.1 配置入侵防御模式

CFW提供基础防御功能，结合多年攻防实战积累的经验规则，针对访问流量进行检测与防护，覆盖多种常见的网络攻击，有效保护您的资产。

配置入侵防御模式操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的  ，选择区域。

步骤3 在左侧导航树中，单击左上方的  ，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在左侧导航栏中，选择“攻击防御 > 入侵防御” 。

表 4-1 入侵防御功能介绍

功能名称	功能说明
防护模式	• **观察模式**：仅对攻击事件进行检测并记录到“攻击事件日志”中，不做拦截。 • **拦截模式**：在发生明确攻击类型的事件和检测到异常IP访问时，将实施自动拦截操作。 – 拦截模式-宽松：防护粒度较粗。拦截可信度高且威胁程度高的攻击事件。 – 拦截模式-中等：防护粒度中等。满足大多数场景下的防护需求。 – 拦截模式-严格：防护粒度精细，全量拦截攻击请求。 **说明** • 建议您优先开启“观察模式”，等待业务运行一段时间后，再逐步更换至“拦截模式”，查看攻击事件日志，请参见**攻击事件日志**。 • 若存在误拦截情况，可对基础防御规则库的单条防御规则进行动作修改。具体操作请参见**管理基础防御规则**。
基础防御	为您的资产提供基础的防护能力，默认开启。防御功能包括： • 检查威胁及漏洞扫描； • 检测流量中是否含有网络钓鱼、特洛伊木马、蠕虫、黑客工具、间谍软件、密码攻击、漏洞攻击、SQL注入攻击、XSS跨站脚本攻击、Web攻击； • 是否存在协议异常、缓冲区溢出、访问控制、可疑DNS活动及其他可疑行为。 **说明** 查看基础防御规则请参见**查看IPS规则库**
虚拟补丁	在网络层级为IPS提供热补丁，实时拦截高危漏洞的远程攻击行为，同时避免修复漏洞时造成业务中断。 虚拟补丁规则库中展示新增的IPS规则，查看规则库请单击“查看虚拟补丁内容”，规则库中参数说明请参见**查看IPS规则库**。 自动更新：开启“自动更新”后，虚拟补丁中的规则将生效，实时防护并支持手动修改防护动作。
自定义IPS特征	当基础防御规则库不满足需求时，CFW支持自定义IPS特征。 仅专业版防火墙支持自定义IPS特征，操作步骤请参见**自定义IPS特征**。

功能名称		功能说明
高级	敏感目录扫描防御	防御对用户主机敏感目录的扫描攻击。 “动作”： • 观察模式：发现敏感目录扫描攻击后，CFW仅记录攻击日志，查看攻击日志请参见**攻击事件日志**。 • 拦截Session：发现敏感目录扫描攻击后，拦截当次会话。 • 拦截IP：发现敏感目录扫描攻击后，CFW会阻断该攻击IP一段时间。 “持续时长”：“动作”选择“拦截IP”时，可设置阻断时间，范围为60~3600s。 “阈值”：对于单个敏感目录扫描频率达到设定的阈值后，CFW会采取相应“动作”。
	反弹Shell检测防御	防御网络上通过反弹shell方式进行的网络攻击。 “动作”： • 观察模式：发现反弹shell攻击后，仅记录攻击日志，查看攻击日志请参见**攻击事件日志**。 • 拦截Session：发现反弹shell攻击后，拦截当次会话。 • 拦截IP：发现反弹shell攻击后，CFW会阻断该攻击IP一段时间。 “持续时长”：“动作”选择“拦截IP”时，可设置阻断时间，范围为60~3600s。 “模式”： • 低误报：防护粒度较粗，单次会话中攻击次数达到4次时触发观察或拦截，确保攻击处理没有误报。 • 高检测：防护粒度精细，单次会话中攻击次数达到2次时触发观察或拦截，确保攻击能够及时被发现并处理。

----结束

4.2 配置访问控制策略

访问控制策略默认状态为放行，通过配置合适的策略调整防护能力，实现更有效的精细化管控，防止内部威胁扩散，增加安全战略纵深，配置访问控制策略请参见**互联网边界防护规则**，如需阻断所有访问仅放行某条流量请参见**配置示例-单独放行入方向中指定IP的访问流量**，如需阻断某个地区的访问流量请参见**配置示例-拦截某一地区的访问流量**。

配置示例-单独放行入方向中指定 IP 的访问流量

配置两条防护规则，一条拦截所有流量，如**图 拦截所有流量**所示，优先级置于最低，一条单独放行指定IP的流量访问，如**图 放行指定IP**所示，优先级设置最高，其余参数可根据您的部署进行填写。

图 4-1 拦截所有流量

图 4-2 放行指定 IP

配置示例-拦截某一地区的访问流量

假如您需要拦截所有来源“北京”地区的访问流量，可以参照以下参数设置防护规则。

图 4-3 拦截北京地区的访问流量

5 （可选）步骤四：查看防护详情

5.1 查看网络流量分析

通过流量分析实时查看云主机出入流量、攻击趋势的详细信息，排查异常流量。

查看入云流量

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在左侧导航栏中，选择“流量分析 > 入云流量”，进入“入云流量”页面。

步骤6 查看经过防火墙的流量统计信息，您可以在下拉框中选择查询时间。

- 流量看板：互联网访问内部服务器时最大流量的相关信息。
- 入云流量：入方向请求流量和响应流量数据。
- 可视化统计：查看指定时间段内入方向流量中指定参数的 TOP 5 排行，参数说明请参见**表 入云流量可视化统计参数说明**。单击单条数据查看流量详情，每个详情支持查看50条数据。

表 5-1 入云流量可视化统计参数说明

参数名称	参数说明
TOP访问源IP	入方向流量的源IP地址。
TOP访问来源地区	入方向流量的源IP所属的地理位置，
TOP访问目的IP	入方向流量的目的IP地址。

参数名称	参数说明
TOP开放端口	入方向流量的目的端口。
应用分布	入方向流量的应用信息。

- IP分析：查看指定时间段内 TOP 50 的流量信息。
  - 公开IP分析：目的IP的流量信息。
  - 访问源IP分析：源IP的流量信息。

----结束

查看出云流量

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在左侧导航栏中，选择“流量分析 > 出云流量”，进入“出云流量”页面。

步骤6 查看经过防火墙的流量统计信息，您可以在下拉框中选择查询时间。

- 流量看板：内部服务器访问互联网时最大流量的相关信息。
- 出云流量：出方向请求流量和响应流量数据。
- 可视化统计：查看指定时间段内出方向流量中指定参数的 TOP 5 排行，参数说明请参见**表 出云流量可视化统计参数说明**。单击单条数据查看流量详情，每个详情支持查看50条数据。

表 5-2 出云流量可视化统计参数说明

参数名称	参数说明
TOP访问目的IP	出方向流量的目的IP地址。
TOP访问目的地区	出方向流量的目的IP所属的地理位置。
TOP访问源IP	出方向流量的源IP地址。
TOP开放端口	出方向流量的目的端口。
应用分布	出方向流量的应用信息。

- IP分析：查看指定时间段内 TOP 50 的流量信息。
  - 外联IP：目的IP的流量信息。
  - 公网外联资产：源IP为公网IP的流量信息。

- 私网外联资产：源IP为私网IP的流量信息。

----结束

5.2 查看防护日志

通过攻击事件日志查看云墙检测到的攻击流量详情，请参见**攻击事件日志**。

通过访问控制日志查看根据访问控制策略放行或阻断的所有流量，及时调整访问控制策略，请参见**访问控制日志**。

攻击事件日志

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在左侧导航树中，选择“日志审计 > 日志查询”。进入“攻击事件日志”页面，可查看近一周的攻击事件详情。

图 5-1 攻击事件日志

表 5-3 攻击事件日志参数说明

参数	说明
发生时间	攻击事件发生的时间。
攻击类型	攻击事件所属类型，主要包括：IMAP、DNS、FTP、HTTP、POP3、TCP、UDP等。
危险等级	危险等级包括：严重、高、中、低。
规则ID	对应规则的ID号。
规则名称	规则库中相对应的命中规则名称。
源IP	攻击事件的来源IP。
源国家/地区	攻击事件源IP所属的地理位置。
源端口	攻击事件的源端口。

参数	说明
目的IP	攻击事件中受到攻击的IP地址。
目的国家/地区	攻击事件目的IP所属的地理位置。
目的端口	攻击事件的目的端口。
协议	攻击事件的协议类型。
应用	攻击事件的应用类型。
方向	包括两个方向：出方向、入方向。
响应动作	包括放行、阻断、阻断IP、丢弃。
操作	操作：查看攻击事件的“基本信息”和“攻击payload”。

----结束

访问控制日志

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在左侧导航树中，选择“日志审计 > 日志查询”。选择“访问控制日志”页签，可查看近一周的访问控制流量详情。

图 5-2 访问控制日志

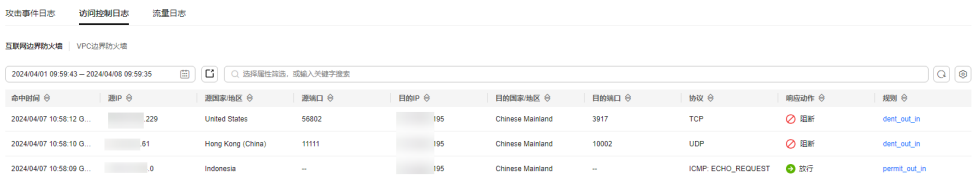


表 5-4 访问控制日志参数说明

参数	说明
命中时间	访问发生的时间。
源IP	访问的源IP地址。
源国家/地区	访问源IP所属的地理位置。

参数	说明
源端口	访问控制的源端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
目的IP	访问的目的IP。
目的网址	访问的域名地址。
目的国家/地区	访问目的IP所属的地理位置。
目的端口	访问控制的目的端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
协议	访问控制的协议类型。
响应动作	包括观察者模式（“观察”）和拦截模式（“阻断”或“放行”）。
规则	访问控制的规则类型，包括黑名单、白名单。

----结束

6 入门实践

当您配置入侵防御和访问控制策略后，可以根据业务场景使用CFW提供的一系列常用实践。

表 6-1 常用实践

实践	描述
配置IP地址组和服务组访问策略	介绍如何批量配置IP地址组和服务组（端口、协议），适用于业务部署在企业或有多个IP地址或端口协议需要配置的场景。
VPC间边界防火墙配置	介绍VPC边界防火墙的配置流程，适用于对VPC间流量防护有需求的场景。
等保二级解决方案	该解决方案能帮您快速在华为云上搭建等保二级合规安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保二级合规要求。
等保合规安全解决方案	该解决方案介绍，华为云依托自身安全能力与安全合规生态，为客户提供一站式的安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保合规要求。