边缘安全（EdgeSec）

产品介绍

文档版本 08

发布日期 2024-10-30

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 什么是边缘安全?

边缘安全（Edge Security，EdgeSec）是建立在边缘节点上的安全防护服务。

边缘安全加速（Edge Security Acceleration，ESA）是边缘安全服务的子产品，提供“缓存加速+应用安全”的一体化服务，支持网络加速以及Web攻击防护、DDoS防护、CC防护等多项安全功能，全面提升加速网络的安全防护能力，保障用户优质的访问体验和业务安全。

工作原理

用户请求到达边缘安全加速网络，节点识别并拦截各类攻击请求：对DDoS攻击流量进行清洗，EdgeSec引擎对Web、BOT、CC类型攻击进行行为分析并更新拦截策略，阻断恶意请求到达客户源站，保障业务访问流畅稳定的同时，实现网络动静态加速。

2 基本概念

CDN

CDN（Content Delivery Network，内容分发网络）是构建在现有互联网基础之上的一层智能虚拟网络，通过在网络各处部署节点服务器，实现将源站内容分发至所有CDN节点，使用户可以就近获得所需的内容。

DDoS 攻击

分布式拒绝服务攻击（Distributed Denial of Service Attack，简称DDoS），常见攻击类型：SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood、DNS Flood、SSDP反射攻击等。

CC 攻击

CC (Challenge Collapsar，挑战黑洞)攻击是DDoS攻击的一种类型，使用代理服务器向受害服务器发送大量貌似合法的请求。

OWASP 威胁

OWASP（Open Web Application Security Project，开放式 Web 应用程序安全项目），常见威胁类型： SQL注入、XSS跨站脚本、文件包含、目录遍历、敏感文件访问、命令/代码注入、网页木马上传、后门隔离保护、非法HTTP协议请求等威胁。

BOT 攻击

Bot即机器人，是一种被编程完成特定任务的软件应用程序，用于自动执行重复性任务。常见攻击类型：恶意爬虫、漏洞扫描、DDoS攻击、凭证破解、薅羊毛、点击欺诈等。

API 防护

API（Application Programming Interface，应用程序编程接口）防护，自动发现API资产并分类管理，监控API资产是否有可疑的操作和异常调用行为，快速响应并拦截异常行为。

边缘安全加速节点

边缘安全加速节点，指距离最终用户接入具有较少的中间环节，同时具备安全防护能力的网络节点，对最终接入用户有较好的响应能力和连接速度。

并发数

并发数指系统能够同时处理请求的数目。对于网站而言，并发数即网站并发用户数，指同时提交请求的用户数目。

3 边缘安全加速

3.1 功能特性

DDoS 攻击防护

边缘安全的DDoS攻击防护，基于先进的特征识别算法对流量进行统一精确检测，识别攻击后，可以快速清洗，抵御SYN Flood、UDP Flood、ICMP Flood等各种大流量攻击，保障正常服务平稳运行。

边缘安全节点网络基于分布式架构搭建，智能调度全局负载均衡，当某个CDN边缘站点的业务受攻击流量到达清洗阈值时，就近调度流量至更大带宽的高防机房，应对超大流量DDoS攻击，保障突发攻击时的业务访问流畅稳定。

CC 攻击防护

CC攻击防护规则支持通过限制访问者对防护网站上特定路径（URL）的访问频率，精准识别CC攻击以及有效缓解CC攻击，阻挡暴力破解、探测和统计弱密码撞库等高频攻击。支持人机验证、阻断和仅记录防护动作。

- 策略配置灵活

  可以根据IP字段名设置灵活的限速策略。
- 阻断页面可定制

  阻断页面可自定义内容和类型，满足业务多样化需要。

Web 基础防护

覆盖OWASP（Open Web Application Security Project，简称OWASP）TOP 10中常见安全威胁，通过预置丰富的信誉库，对漏洞攻击、网页木马等威胁进行检测和拦截。

- 全面的攻击防护

  支持SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录（路径）遍历、敏感文件访问、命令/代码注入、XML/Xpath注入等攻击检测和拦截。
- Webshell检测

防护通过上传接口植入网页木马。

- 识别精准
  - 内置语义分析+正则双引擎，黑白名单配置，误报率更低。
  - 支持防逃逸，自动还原常见编码，识别变形攻击能力更强。
    默认支持的编码还原类型：url_encode、Unicode、xml、OCT（八进制）、HEX（十六进制）、html转义、base64、大小写混淆、javascript/shell/php等拼接混淆。
- 深度检测
  深度反逃逸识别（支持同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等的防护）。
- header全检测
  支持对请求里header中所有字段进行攻击检测。
- Shiro解密检测
  支持对Cookie中的rememberMe内容做AES，Base64解密后再检测。

网站反爬虫

动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别多种爬虫行为。

- 特征反爬虫
  自定义扫描器与爬虫规则，用于阻断网页爬取行为，添加定制的恶意爬虫、扫描器特征，使爬虫防护更精准。
- JS脚本反爬虫
  通过自定义规则识别并阻断JS脚本爬虫行为。

3.2 产品优势

精准调度

全球精准IP库，并具备自我进化能力，全网链路质量大数据实时分析、预测，为用户精准调度最优节点，保障访问质量。

简单易用

接入方式简捷，控制台自助配置丰富且易操作，API接口开放，便于企业应用集成、跨云平台管理。

高性能缓存

独创AICache技术+多级缓存（内存→SSD→HDD），有效提升缓存命中率、减少用户访问等待时间。

全方位安全防护

继承华为云在安全攻防领域20多年的技术和经验累积，全方位防护DDoS攻击，Web攻击，CC攻击、恶意爬虫等各类网络攻击，全面支持SQL注入、XSS跨站脚本、文件包含等各类OWASP威胁防护。

合规认证

华为云具备AAA级CDN企业信用评估、IPv6认证、可信云等认证，为加速提供保障。

精细化用量管理

多维度监控告警能力，包括访问情况统计、使用量统计、套餐剩余量预警、离线日志等功能，方便您精细化了解业务运行情况。

3.3 应用场景

行业客户	加速需求	安全防护需求
媒资	• 网站加速 • 点播加速	• L3/L4 DDoS缓解 • CC缓解 • Web应用防护
电商	• 网站加速 • 动态加速	• L3/L4 DDoS缓解 • CC缓解 • Web应用防护 • Bot管理 • API防护
金融	• 网站加速 • 动态加速	• L3/L4 DDoS缓解 • CC缓解 • Web应用防护 • Bot管理 • API防护
下载网站	下载加速	• L3/L4 DDoS缓解 • CC缓解 • Web应用防护

4 服务版本差异

边缘安全提供的服务版本为：企业版，详细的版本说明请参见**版本说明**，各版本支持的功能特性请参见**各版本支持的功能特性**。

版本说明

边缘安全各个版本的相关说明如**表 版本说明**所示。

表 4-1 版本说明

业务规格	企业版
域名个数	20个
CC攻击防护规则	100条
精准访问防护规则	100条
引用表规则	100条
IP黑白名单规则	1000条
地理位置封禁规则	100条
网页防篡改规则	100条
防敏感信息泄露	100条
全局白名单规则	1000条
隐私屏蔽规则	100条

各版本支持的功能特性

每个版本适用的安全功能特性如表4-2所示。

标识说明：

- √：表示在当前版本中支持。
- ×：表示在当前版本中不支持。

表 4-2 安全功能特性

功能模板	企业版
域名扩展包	√
支持添加泛域名	√
批量灵活配置防护策略	√
为防护策略批量配置适用的防护域名	√
常见的Web应用攻击防护，包括SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等	√
云端自动更新最新0Day漏洞防护规则，及时下发0Day漏洞虚拟补丁	√
Webshell检测	√
深度检测，同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等深度反逃逸检测	√
header全检测，对请求里header中所有字段进行攻击检测	√
CC攻击防护	√
精准访问防护	√
引用表管理	√
IP黑白名单设置，支持批量导入IP地址/IP地址段	√
支持对指定国家、省份的IP自定义访问控制	√

功能模板	企业版
检测并拦截搜索引擎、扫描器、脚本工具、其它爬虫等爬虫行为	√
检测并拦截JS脚本反爬虫检测行为	√
防敏感信息泄露	√
全局白名单规则	√
隐私屏蔽	√

5 使用限制

限制项	说明
域名准入条件	● 中国大陆： – 华为账号已完成实名认证。 – 域名已在工信部备案，且当前备案信息正常可用。 – 加速域名接入时需通过内容审核。 ● 中国大陆境外： – 加速域名接入时需通过内容审核。 ● 全球： – 已在华为云进行实名认证。 – 域名已在工信部备案，且当前备案信息正常可用。 – 加速域名接入时需通过内容审核。
内容审核	不支持接入违反相关法律法规的域名，包括但不限于： ● 涉黄、涉赌、涉毒、涉诈、侵权内容的网站 ● 游戏私服类网站 ● 盗版游戏 / 软件 / 盗版视频网站 ● P2P类金融网站 ● 彩票类网站 ● 违规医院和药品类网站 ● 网站无法正常访问或内容不含有任何实质信息 **说明** ● 如果您的加速域名含有以上违规的内容，您将自行承担相关风险。 ● 如果发现涉黄、涉赌、涉毒、涉诈等违规行为，ESA将执行域名封禁策略（删除相关加速域名且不允许再次接入，与违规域名使用相同源站的加速域名同样执行域名封禁策略），账号加速域名配额降为0。

限制项	说明
域名配额	域名配额由边缘安全加速套餐决定。如果域名配额无法满足使用需要，您可以购买套餐外域名包来增加防护域名数。 ● 域名数量（企业版）：20。
请求方式	常见的HTTP请求方式里面，支持GET、PUT、POST和DELETE这几种请求方式。

6 安全

6.1 责任共担

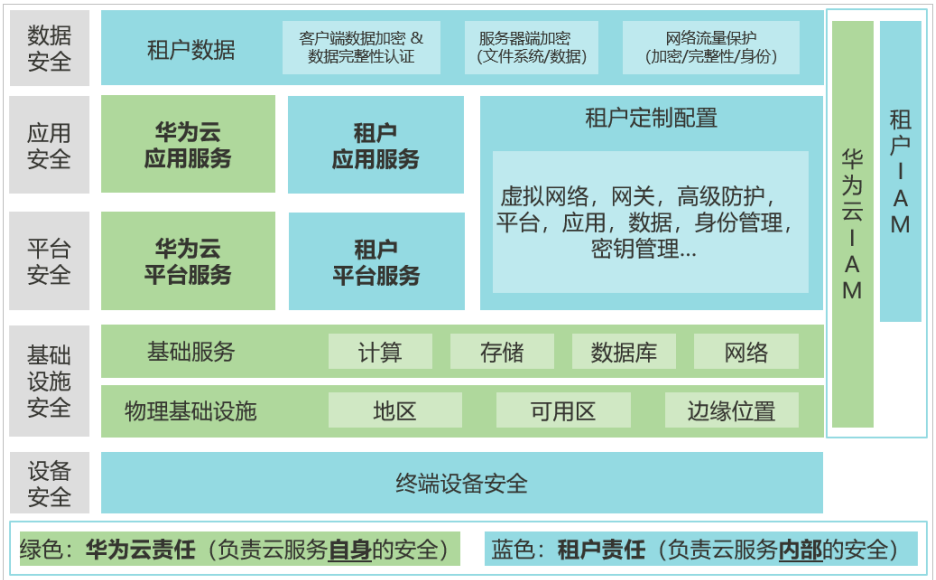
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图6-1**所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 6-1 华为云安全责任共担模型



6.2 身份认证与访问控制

EdgeSec对接了统一身份认证服务（Identity and Access Management，IAM）服务。EdgeSec租户身份认证与访问控制通过IAM权限控制。

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助EdgeSec服务安全地控制访问权限。通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对EdgeSec资源的访问范围。关于对EdgeSec资源的访问权限，详细请参考**权限管理**。

6.3 数据保护技术

EdgeSec通过多种数据保护手段和特性，保证通过EdgeSec的数据安全可靠。

表 6-1 EdgeSec 的数据保护手段和特性

数据保护手段	简要说明
静态数据保护	EdgeSec通过敏感数据加密保证用户流量中敏感数据的安全性。
传输中的数据保护	微服务间数据传输进行加密，防止数据在传输过程中泄露或被篡改。 用户的配置数据传输采用安全协议HTTPS，防止数据被窃取。
数据完整性校验	EdgeSec进程启动时，配置数据从配置中心获取而非直接读取本地文件。
数据隔离机制	租户区与管理面隔离，租户的所有操作权限隔离，不同租户间的策略、日志等数据隔离。

数据保护手段	简要说明
数据销毁机制	考虑到残留数据导致的信息泄露问题，华为云根据客户等级设定了不同的保留期时长，保留期到期仍未续订或充值，存储在云服务中的数据将被删除，云服务资源将被释放。EdgeSec对云服务自动感知并在保留期到期后释放资源。

同时，EdgeSec服务充分尊重用户隐私，遵循法律法规，不会采集和存储任何用户隐私数据。 更多隐私数据使用和保护问题，请参考**隐私政策声明**。

6.4 审计与日志

- 审计

  云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

  用户开通云审计服务并创建和配置追踪器后，CTS可记录EdgeSec的管理事件和数据事件用于审计。

  CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

- 日志

  出于分析或审计等目的，用户开启了云审计服务后，系统开始记录EdgeSec资源的操作。云审计服务管理控制台保存最近7天的操作记录。

6.5 服务韧性

华为云EdgeSec按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减少由硬件故障、自然灾害或其他灾难带来的服务中断，华为云EdgeSec提供灾难恢复计划。

当发生故障时，EdgeSec的五级可靠性架构支持不同层级的可靠性，因此具有更高的可用性、容错性和可扩展性。

华为云EdgeSec已面向全球用户服务，并在多个分区部署，同时EdgeSec的所有管理面、引擎等组件均采用主备或集群方式部署。

6.6 监控安全风险

EdgeSec已对接云监控服务（Cloud Eye，CES），可以通过管理控制台，查看EdgeSec的相关指标，及时了解EdgeSec防护状况，并通过指标设置防护策略。CES服务是华为云为用户提供一个针对各种云上资源的立体化监控平台，用户通过云监控服务可以全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

用户通过设置EdgeSec告警规则，可自定义监控目标与通知策略，告警规则包含名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助用户及时了解EdgeSec防护状况，从而起到预警作用。

如何使用CES对EdgeSec进行监控，请参见：

- **EdgeSec监控指标说明**
- **设置监控告警规则**
- **查看监控指标**

6.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 6-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 6-3 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 6-4 销售许可证&软件著作权证书

7 权限管理

如果您需要对华为云购买的EdgeSec资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为账号中给员工创建IAM用户，并授权控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些员工拥有EdgeSec的使用权限，但是不希望这些员工拥有删除EdgeSec等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用EdgeSec，但是不允许删除EdgeSec的权限，控制员工对EdgeSec资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用EdgeSec的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

EdgeSec 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

EdgeSec部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问EdgeSec时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对EdgeSec服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，

如**表 EdgeSec系统角色**所示，包括了EdgeSec的所有系统角色。

表 7-1 EdgeSec 系统角色

系统角色/策略名称	描述	类别	依赖关系
EdgeSec FullAccess	边缘安全服务所有权限	系统策略	无。
EdgeSec ReadOnlyAccess	边缘安全服务只读权限	系统策略	

相关链接

- **IAM产品介绍**
- **创建用户组并授权使用EdgeSec**

8 与其他云服务的关系

本章节介绍边缘安全与其他云服务的关系。

与内容分发网络的关系

内容分发网络（Content Delivery Network，CDN）是构建在现有互联网基础之上的一层智能虚拟网络，通过在网络各处部署节点服务器，实现将源站内容分发至所有CDN节点，使用户可以就近获得所需的内容。CDN服务缩短了用户查看内容的访问延迟，提高了用户访问网站的响应速度与网站的可用性，解决了网络带宽小、用户访问量大、网点分布不均等问题。

EdgeSec是基于CDN边缘节点提供的安全防护服务。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）为EdgeSec提供云服务资源的操作记录，记录内容包括从访问管理控制台发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

CTS记录了EdgeSec相关的操作事件，方便用户日后的查询、审计和回溯。

与云监控服务的关系

云监控服务可以监控边缘安全的相关指标，用户可以通过指标及时了解边缘安全的状况，并通过这些指标设置防护策略。具体请参见《云监控服务用户指南》。

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为边缘安全提供了权限管理的功能。需要拥有EdgeSec FullAccess权限的用户才能使用EdgeSec服务。如需开通该权限，请联系拥有Security Administrator权限的用户。

与云日志服务的关系

云日志服务（Log Tank Service，简称LTS）用于收集来自主机和云服务的日志数据。边缘安全可以设置将攻击日志、访问日志记录到LTS中，为您提供一个实时、高效、安全的日志处理功能。

与企业管理的关系

企业中有多个项目，多个项目的资源需要分开结算，且分属不同人员进行管理。同时项目可以单独启动或停止，对其他项目没有影响。**企业管理**可以针对企业中的每个项目，分别建立企业项目，管理各自的资源，并且针对不同的企业项目，设置不同的人员进行管理。

边缘安全支持企业管理，您可以将边缘安全的资源按照企业项目进行管理，并设置每个企业项目的用户权限。