边缘安全（EdgeSec）

常见问题

文档版本 07

发布日期 2024-10-30

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2024。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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

 版权所有 © 华为云计算技术有限公司

1 产品咨询

1.1 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。

1.2 边缘安全是否支持单独使用?

支持。边缘安全可以单独使用，边缘安全是基于内容分发网络（Content Delivery Network，CDN）站点提供的服务，包含了CDN和全站加速，您只需要购买边缘安全服务就可以获得CDN、全站加速、安全防护一体化服务。

因此，边缘安全支持单独使用。

1.3 边缘安全支持哪些地域?

边缘安全支持的国家区域包括：新加坡、泰国、印度尼西亚、马来西亚、菲律宾、巴西及以上国家临近区域。

当您的业务部署区域离以上国家较远时，访问时延将会增加，请充分考虑实际应用场景，再决定是否使用边缘安全。

1.4 边缘安全提供的是几层防护?

边缘安全提供的防护如下：

三层（网络层），四层（传输层）和七层（应用层）防护。

 版权所有 © 华为云计算技术有限公司

1.5 防护对象类相关咨询

边缘安全是否支持基于应用层协议和内容的访问控制?

边缘安全支持应用层协议（HTTP/HTTPS）和内容的访问控制。

边缘安全是否防御 XOR 注入攻击?

边缘安全提供XOR注入攻击防御。

边缘安全是否支持漏洞检测?

边缘安全的网站反爬虫功能可以对第三方漏洞攻击等威胁进行检测和拦截。在配置网站反爬虫防护规则时，如果您开启了扫描器，将对扫描器爬虫，如OpenVAS、Nmap等进行检测。

有关网站反爬虫防护规则的详细操作，请参见**配置网站反爬虫防护规则**。

边缘安全是否可以对用户添加的 Post 的 body 进行检查?

边缘安全的内置检测会检查Post数据，webshell是Post提交的文件。Post类型提交的表单、json等数据，都会被边缘安全的默认策略检查。

您可以通过配置精准访问防护规则，对添加的Post的body进行检查。有关配置精准访问防护规则的详细操作，请参见**配置精准访问防护规则**。

边缘安全是否支持限制域名访问速度?

不支持。

边缘安全支持通过自定义CC防护规则，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。

有关CC防护规则的详细介绍，请参见**配置CC攻击防护规则**。

边缘安全是否支持拦截包含特殊字符的 URL 请求?

不支持，URL请求中有特殊字符时，边缘安全不会拦截。边缘安全中边缘安全可以对来源IP进行检测和限制。

边缘安全可以拦截 Web 页面调用其他接口的请求数据吗?

分为以下两种情况：

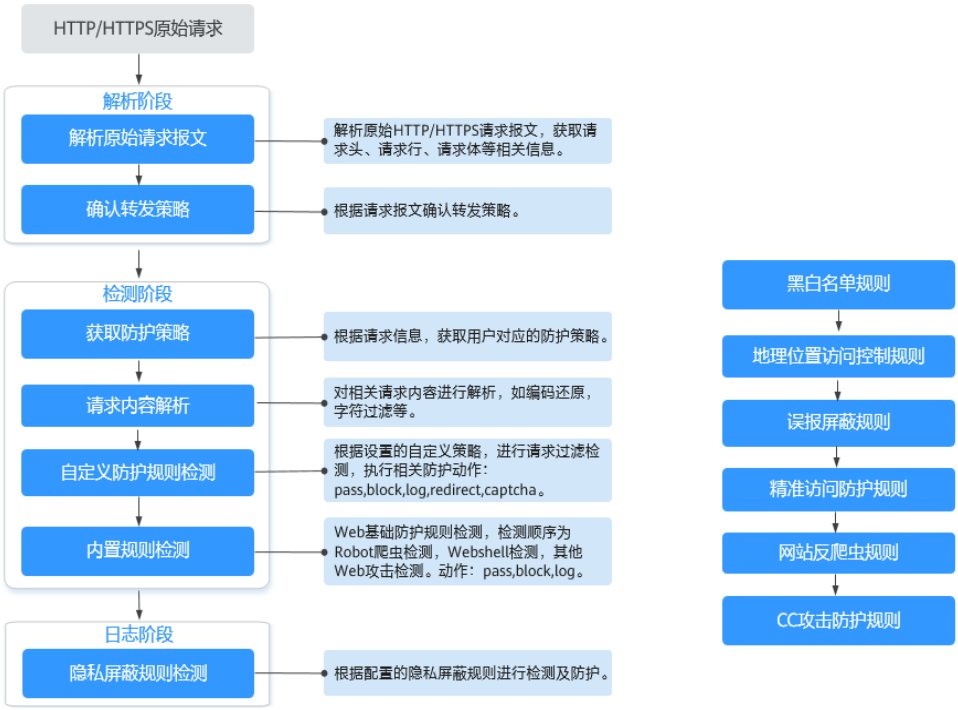
- Web页面调用其他接口的请求数据在边缘安全防护域名内：该请求数据将经过边缘安全，边缘安全会检测并阻断该请求数据。
- Web页面调用其他接口的请求数据不在边缘安全防护域名内：该请求数据不经过边缘安全，边缘安全不会拦截该请求数据。

版权所有 © 华为云计算技术有限公司

边缘安全支持自定义 POST 拦截吗?

边缘安全不支持自定义POST拦截。针对HTTP/HTTPS原始请求，边缘安全引擎内置防护规则的检测流程如图 WAF引擎检测图所示。

图 1-1 引擎检测图



有关边缘安全防护流程的详细介绍，请参见**配置引导**。

边缘安全是否支持跨域禁止访问功能?

边缘安全不支持配置跨域禁止访问功能。有关EdgeSec功能的详细介绍，请参见**功能特性**。

边缘安全可以设置域名限制访问吗?

边缘安全不能直接通过域名限制访问。

边缘安全支持配置黑白名单规则（即设置IP黑/白名单），阻断、仅记录指定IP或IP段的访问请求，请参见**配置IP黑白名单规则**。

边缘安全有 IPS 入侵防御系统模块吗?

边缘安全没有传统防火墙的IPS模块，不支持IPS入侵防御，仅支持对HTTP/HTTPS协议的入侵检测。

边缘安全是硬防火墙还是软防火墙?

边缘安全是软防火墙。当您购买边缘安全后，只需要将域名接入边缘安全，就可以使用边缘安全的防护功能。

版权所有 © 华为云计算技术有限公司

有关域名接入边缘安全的详细操作，请参见**添加防护网站**。

边缘安全可以防护 Apache Struts2 远程代码执行漏洞（CVE-2021-31805）吗?

边缘安全中边缘安全的Web基础防护规则可以防护Apache Struts2远程代码执行漏洞（CVE-2021-31805）。

具体的操作请参见**配置Web基础防护规则**。

1.6 协议类相关咨询

边缘安全是否支持 QUIC 协议?

不支持。

边缘安全是否支持 SSL 双向认证?

不支持。

边缘安全是否支持 HTTP/3 协议?

不支持，目前边缘安全中边缘安全最高支持HTTP/2协议。

边缘安全是否支持防护 CS 架构的网站?

如果该网站的CS架构是七层HTTP/HTTPS协议，则边缘安全可以防护，否则不支持防护。

边缘安全可以防护使用 HSTS 策略/NTLM 代理认证访问的网站吗?

可以。边缘安全中边缘安全支持防护HTTP/HTTPS协议业务。

- 网站选择使用HSTS（HTTP Strict Transport Security，HTTP严格传输安全协议）策略后，会强制要求客户端（如浏览器）使用HTTPS协议与网站进行通信，以减少会话劫持风险。配置HSTS策略的网站使用的是HTTPS协议，边缘安全可以防护。
- NTLM（New Technology LAN Manager，Windows NT LAN管理器）代理是Windows平台下HTTP代理的一种认证方式，其认证方式与Windows远程登录的认证方式是一样的，客户端（如浏览器）和代理之前需要三次握手才开始传递信息。

  对于客户端（如浏览器）和代理之前使用NTLM认证的业务，边缘安全可以防护。

 版权所有 © 华为云计算技术有限公司

2 功能咨询

2.1 边缘安全对 SQL 注入、XSS 跨站脚本和 PHP 注入攻击的检测原理?

SQL（Structured Query Language）注入攻击是一种常见的Web攻击方法，攻击者通过把SQL命令注入到数据库的查询字符串中，最终达到欺骗服务器执行恶意SQL命令的目的。例如，可以从数据库获取敏感信息，或者利用数据库的特性执行添加用户、导出文件等一系列恶意操作，甚至有可能获取数据库乃至系统用户最高权限。

XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，但实际上也可以包括Java、 VBScript、ActiveX、 Flash 或者甚至是普通的HTML。攻击成功后，攻击者可能得到包括但不限于更高的权限（如执行一些操作）、私密网页内容、会话和Cookie等各种内容。

边缘安全针对 SQL 注入攻击的检测原理

边缘安全针对SQL注入攻击的检测原理是检测SQL关键字、特殊符号、运算符、操作符、注释符的相关组合特征，并进行匹配。

- SQL关键字（如 union，Select，from，as，asc，desc，order by，sort，and ，or，load，delete，update，execute，count，top，between，declare，distinct，distinctrow，sleep，waitfor，delay，having，sysdate，when，dba_user，case，delay 等）
- 特殊符号（’ ”,; ()）
- 运算符（±*/%|）
- 操作符（=，>,<,>=,<=,!=,+=,-=）
- 注释符（–，/**/）

边缘安全针对 XSS 攻击的检测原理

边缘安全对XSS跨站脚本攻击的检测原理主要是针对HTML脚本标签、事件处理器、脚本协议、样式等进行检测，防止恶意用户通过客户端请求注入恶意XSS语句。

- XSS关键字（javascript 、script、object、style、iframe、body、input、form、onerror、alert等）；

 版权所有 © 华为云计算技术有限公司

- 特殊字符（<、>、’、”）；
- 外部链接（href=“http：//xxx/”，src="http：//xxx/attack.js"）。

说明

如果业务需要上传富文本，可以用multipart方式上传，不用body方式上传，放在表单里，即使base64编码也会解码。分析业务场景，建议限制引号、尖括号输入。

边缘安全针对 PHP 攻击的检测原理

如果请求中包含类似于system(xx) 关键字，该关键字具有PHP注入攻击风险，因此，边缘安全会拦截该类请求。

2.2 如何获取边缘安全中访问者真实 IP?

网站接入边缘安全后，边缘安全作为一个反向代理存在于客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到边缘安全的IP地址。

通常情况下，网站访问并不是简单地从用户的浏览器直达服务器，中间可能部署有CDN、EdgeSec、高防。例如，采用这样的架构：“用户 > CDN/EdgeSec/高防 > 源站服务器” 。那么，在经过多层代理之后，服务器如何获取发起请求的真实客户端IP呢?

一个透明的代理服务器在把用户的HTTP请求转到下一环节的服务器时，会在HTTP的头部中加入一条“X-Forwarded-For”记录，用来记录用户的真实IP，其形式为“X-Forwarded-For：访问者的真实IP，代理服务器1-IP， 代理服务器2-IP，代理服务器3-IP，……”。

因此，访问者的真实IP可以通过获取“X-Forwarded-For”对应的第一个IP来得到。

2.3 边缘安全如何拦截请求内容?

边缘安全通过检测请求的首部和body体，对不符合防护规则的请求内容进行拦截，例如body的表单、xml、json等数据。

有关边缘安全防护流程的详细介绍，请参见**配置引导**。

2.4 在安全组中配置边缘安全白名单，需要开放所有端口吗?

可以开放所有端口。

但是为了降低网络安全风险，建议只开放80和443端口。

2.5 为什么 Cookie 中有 HWEdgeSecSESID 或 HWEdgeSecSESTIME 字段?

HWEdgeSecSESID：会话ID；HWEdgeSecSESTIME：会议时间戳；这两个字段用于标记请求，如CC防护规则中用户计数。

防护域名/IP接入边缘安全后，边缘安全会在客户请求Cookie中插入HWEdgeSecSESID（会话ID），HWEdgeSecSESTIME（会话时间戳）等字段，这些字段服务于边缘安全统计和安全特性。

版权所有 © 华为云计算技术有限公司

2.6 边缘安全支持对受到攻击发送告警通知吗?

边缘安全支持对受到攻击发送告警通知。

当Web攻击单个域名在5分钟内承受攻击达到10万次，DDOS攻击在5分钟内最大攻击带宽达到100Mbps时，会发送告警通知。

您可以单击控制台右上角的“消息中心”按钮，在消息中心页面左侧选择“站内消息 > 全部消息”，在“运维消息”页签下可以查看详细的告警信息。

版权所有 © 华为云计算技术有限公司

3 区域与可用区

3.1 什么是区域和可用区?

什么是区域、可用区?

通常使用用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图3-1阐明了区域和可用区之间的关系。

图 3-1 区域和可用区

目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

 版权所有 © 华为云计算技术有限公司

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

版权所有 © 华为云计算技术有限公司