边缘安全

快速入门

文档版本 01

发布日期 2025-11-11

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 快速接入边缘安全

以CNAME方式接入域名时，边缘安全加速ESA会为您添加的域名分配对应的CNAME值，通过DNS服务商解析将用户请求转发到边缘安全节点上，实现全站加速、安全防护。

前提条件

- 已注册华为云账号，并完成实名认证。
- 已开通CDN服务。

购买边缘安全

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“CDN与智能边缘 > CDN与安全防护”，进入华为云CDN页面。

步骤3 在左侧导航栏选择“域名管理”，单击“添加域名”，为域名配置CDN加速服务。

步骤4 在“添加域名”界面，配置域名参数。参数选择如下：

- 服务范围：中国大陆
- 加速域名：自定义
- 业务类型：网站加速

  说明

  如果有动态请求，“业务类型”请选择“全站加速”。
- 回源方式：协议跟随

步骤5 在源站配置模块单击“添加源站”，填写源站地址，为域名添加源站。

步骤6 单击“确定”，完成源站添加。

步骤7 单击“确定”，弹出“域名添加状态”，确认后再次单击“确定”，完成域名添加。

步骤8 （可选）快速配置，单击“跳过”。也可选择模板后单击“提交配置”。

步骤9 配置CNAME，单击右下角“跳过，稍后再配”。

步骤10 域名添加完成后系统会自动为您的加速域名分配对应的CNAME域名，在“域名管理”页面中的CNAME列可查看。

说明

- 加速域名在CDN服务中获得的CNAME域名不能直接访问，必须在加速域名的域名服务商处**配置CNAME解析**，将加速域名指向CNAME域名，访问加速域名的请求才能转发到CDN节点上，达到加速效果。
- 如果您的业务覆盖中国境内和海外，那么您需要将您的“CDN业务”选择“海外”，，然后在云解析平台上将您在中国大陆的解析服务和海外的解析服务均添加一条指向该cname的解析记录。
- 关于添加域名更多详细的操作，请参见**添加域名**。

步骤11 添加CNAME解析记录后，说明您的流量就可以调度到CDN了，您可以在“安全防护”购买边缘安全加速来使用安全防护业务。

步骤12 单击“购买”，进入“购买边缘安全”页面，设置您使用的产品参数。

步骤13 确认订单详情无误后，单击“去支付”，完成购买操作。

----结束

接入域名

步骤1 在左侧导航栏选择“安全防护 > 域名接入”，进入“安全防护”的“域名接入”页面。

步骤2 在列表左上角，单击“添加域名”，参数说明如**表 添加防护网站参数说明**所示。

图 1-1 添加防护网站

表 1-1 添加防护网站参数说明

参数名称	参数说明
防护域名	选择防护域名，支持选择在CDN服务中“域名管理”页面“业务类型”为“网站加速”、“文件下载加速”、“点播加速”、“全站加速”的域名。 **说明** 此处添加的防护域名是在CDN域名管理中添加的域名。
策略配置	选择已创建的防护策略，默认为“系统自动生成策略”。

步骤3 单击“确定”，完成防护网站的添加。

----结束

配置防护策略

步骤1 在左侧导航栏选择“安全防护 > 防护策略”，进入“安全防护”的“防护策略”页面。

步骤2 在列表左上角，单击“添加防护策略”，设置策略名称。

步骤3 单击“确认”，完成防护策略的添加。

步骤4 单击已添加的防护策略的名称，进入配置策略页面，开启Web基础防护和CC攻击防护按钮，具体参数配置推荐如下：

表 1-2 推荐策略配置

策略名称	配置参数
Web基础防护	● 防护动作：仅记录 ● 常规检测：开启 ● Webshell检测：开启
CC攻击防护	● 限速模式：源IP ● 限速条件：“字段”为“路径”，“逻辑”为“包含”，“内容”为“/”。表示路径内容含“/”都将匹配CC规则。 ● 限速频率：5次，1分钟。表示如果源IP在1分钟内命中限速条件5次，在防护时长内请求会被阻断（返回响应码418），如果选择人机验证，则页面返回验证码，输入验证码后继续访问。 ● 防护动作：阻断 ● 防护时长：60秒

步骤5 返回“防护策略”页面，单击策略名称操作列的“更多 > 添加防护域名”，选择需要绑定的防护域名，单击“确定”。

----结束

2 通过 CC 攻击防护规则拦截大流量高频攻击

CC攻击防护规则支持通过限制访问者对防护网站上资源的访问频率，精准识别CC攻击以及有效缓解CC攻击；当您配置完CC攻击防护规则并开启CC攻击防护后，才能根据您配置的CC攻击防护规则进行防护。

操作流程

操作步骤	说明
准备工作	注册华为账号、开通华为云，并为账户充值、赋予EdgeSec权限。
步骤一：购买边缘安全	购买边缘安全，选择版本、计费方式等信息。
步骤二：将防护网站添加到边缘安全	将防护网站添加到边缘安全防护，实现流量检测并转发。
步骤三：配置CC攻击防护拦截大流量高频攻击	配置并开启CC攻击防护规则，助力网站有效缓解CC攻击。
步骤四：查看防护统计事件	在防护事件中检索CC防护安全事件，快速定位攻击源或对攻击事件进行分析。

准备工作

1. 在购买边缘安全之前，请先注册华为账号并开通华为云。
   如果您已开通华为云并进行实名认证，请忽略此步骤。
2. 请保证账户有足够的资金，以免购买边缘安全失败。具体操作请参见**账户充值**。
3. 请确保已开通CDN服务。
4. 已在“域名管理”中，添加了域名，域名管理请参见**域名管理**。

步骤一：购买边缘安全企业版

边缘提供了专业版和企业版，不同版本之间的差别，请参见**服务版本差异**。

1. **登录EdgeSec服务控制台。**

2. 单击“购买”，进入“购买边缘安全”页面，设置您使用的产品参数。
3. 确认订单详情无误后，单击“去支付”，完成购买操作。

步骤二：将防护网站添加到边缘安全

1. 在左侧导航树中，选择“安全防护 > 域名接入”，进入“安全防护”的“域名接入”页面。
2. 在列表左上角，单击“添加域名”，参数说明如**表 添加防护网站参数说明**所示。

图 2-1 添加防护网站

表 2-1 添加防护网站参数说明

参数名称	参数说明
网站名称	网站的名称。命名规则如下： ● 不可重名。 ● 须以字母开头。 ● 长度不能超过128个字符。 ● 支持英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_:）。
防护域名	选择防护域名，支持选择在CDN服务中“域名管理”页面“业务类型”为“网站加速”、“文件下载加速”、“点播加速”、“全站加速”的域名。 **说明** 此处添加的防护域名是在CDN域名管理中添加的域名。
策略配置	选择已创建的防护策略，默认为“系统自动生成策略”。

3. 单击“确定”，完成防护网站的添加。

步骤三：配置 CC 攻击防护拦截大流量高频攻击

您可以配置以下CC规则，当一个IP在30秒内访问当前域名下路径的次数超过1000次，则封禁该IP在该路径的请求10个小时。该规则可以作为一般中小型站点的预防性配置。

1. 在左侧导航树中，选择“安全防护 > 防护策略”防护策略，进入“防护策略”页面。
2. 单击目标策略名称，进入目标策略的防护配置页面。
3. 选择“CC攻击防护”配置框，开启CC攻击防护策略。

    ：开启状态。

    ：关闭状态。
4. 在“CC攻击防护”规则配置列表左上方，单击“添加规则”，在弹出的对话框中，参考如图2-2所示进行配置。

   示例中仅解释必要参数，其余大多数配置可保留默认值。必要参数说明请参见表2-2。

图 2-2 配置 CC 防护规则

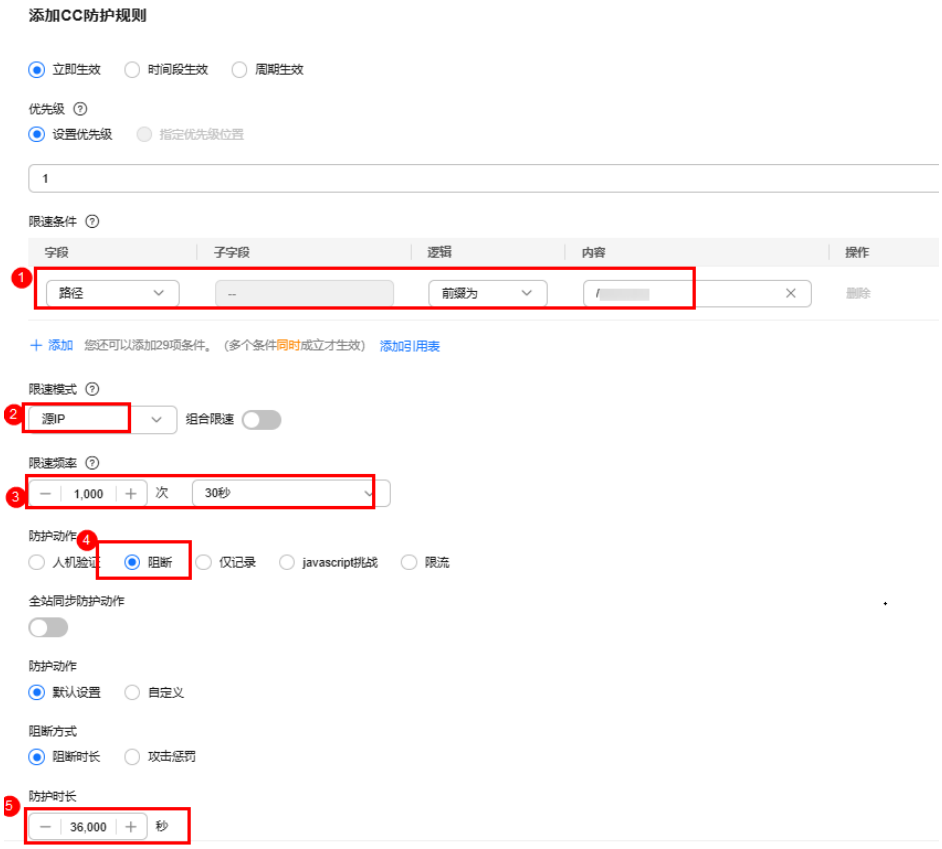

表 2-2 必要参数说明

参数	示例	参数说明
限速模式	源IP	• 源IP：根据IP区分单个Web访问者。 • 源IP C段：根据IP C段区分Web访问者组，按用户访问者组进行计数和限速。 • Cookie：根据Cookie区分单个Web访问者。 • Header：根据需要防护的自定义HTTP首部区分单个Web访问者。
限速条件	• “字段”：路径 • “逻辑”：前缀为 • “内容”：/	单击“添加”增加新的条件，至少配置一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 • 字段：地理位置、路径、IPV4、IPV6、Cookie、Method、Header、Params、返回码(HTTP Code)、ASN、Range。 **说明** 当“字段”为“地理位置”和“ASN”时，暂不支持IPV6类型IP请求匹配。 • 子字段：当“字段”选择“Cookie”、“Header”、“Params”时，请根据实际需求配置子字段。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 • 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 **说明** 1. 当“逻辑”关系选择“包含任意一个”、“不包含任意一个”、“等于任意一个”、“不等于任意一个”、“包含任意前缀”、“不包含任意前缀”、“包含任意后缀”或者“不包含任意后缀”时，需要选择引用表，创建引用表的详细操作请参见**创建引用表**。 2. 配置条件为长度相关的逻辑时，长度的值不宜过大。当用户请求的长度过大时，可能会被后端引擎之前的服务拦截，导致请求无法到达后端引擎，从而使配置的防护规则失效。 • 内容：输入或者选择条件匹配的内容。
限速频率	**1,000次30秒**	单个Web访问者在限速周期内可以正常访问的次数，如果超过该访问次数，边缘安全将根据配置的“防护动作”来处理。

参数	示例	参数说明
防护动作	**阻断**	当访问的请求频率超过“限速频率”后，在防护时长范围内，对新的请求会执行防护动作，可设置以下防护动作： ● 人机验证：表示超过“限速频率”后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。人机验证目前支持英文。 ● 阻断：表示超过“限速频率”将直接阻断。 ● 仅记录：表示超过“限速频率”将只记录不阻断。 ● 限流：表示超过“限速频率”将限制流量速率。 **说明** ● 人机验证依赖JavaScript在浏览器环境中执行，如果是不支持JavaScript的环境，如纯文本终端、某些不具备完整浏览器功能的设备或环境，就无法进行人机验证。因为这些环境无法运行用于验证用户身份和合法性的JavaScript代码，也就无法完成人机验证流程。 ● 人机验证完成后，需要依赖响应页面在浏览器中渲染来恢复页面，对于响应不需要浏览器页面渲染的情况，会出现显示问题（如一直显示人机验证页面）。
阻断时长	**36,000秒**	防护动作的执行时长。建议防护时长配置大于限速周期，取值范围为0~65535。

5. 确认参数配置无误后，单击“确定”。

步骤四：查看防护统计事件

当遭到CC攻击时，您可以在防护事件中检索CC防护安全事件，快速定位攻击源或对攻击事件进行分析。

1. 在左侧导航栏选择“安全防护 > 防护统计”，进入“防护统计”的“Web防护事件”页面。
2. 选择查询时间为“自定义”，查询范围不超过一个月。
3. 在搜索框选择“源IP”为目标IP的防护事件，查询对应的防护事件。
4. （可选）您可以在目标防护事件的“操作”列单击“更多”，对防护事件进行处理。

   说明

   防护事件的三种处理方式如下：
   - 误报处理
   - 添加至地址组
   - 添加至黑白名单

相关信息

关于CC攻击防护更多详细的操作，请参见**配置CC攻击防护规则防御CC攻击**。

