安全加速 SCDN

用户指南

腾讯云

文档目录

用户指南
域名接入

最近更新时间：2023-11-03 11:32:13

开通安全加速套餐后，可以登录 SCDN 控制台，添加安全加速域名。域名添加后会将相关域名安全配置下发至全网 SCDN 安全加速节点，不会影响现网业务可用性。

添加域名

进入防护配置页面，单击**添加域名**。

> **注意**
> 暂不支持音视频点播类型的域名配置。

添加域名页面由两部分组成：

- 基础防护配置
- 高级防护配置

基础防护配置

选择需要接入 SCDN 的域名，默认开启四层流量攻击防护、七层流量攻击防护（可关闭）。

- 防护域名
- 选择1个或多个需要接入安全加速的域名（暂不支持泛域名）。
- 域名需要已接入 CDN，且 CDN 服务处于“已启动”状态。
- 最多一次添加10个域名，且完成添加后总计域名数量，不能超过当前安全加速套餐域名数量上限。

- 当所购套餐支持弹性防护时，弹性防护默认开启。当所购套餐不支持弹性防护时，弹性防护默认关闭。详情请见 计费说明 。

> **说明**
> 四层流量攻击防护对应旧版 DDoS 攻击防护，七层流量攻击防护对应旧版 CC 攻击防护。

高级防护配置

用户可根据业务情况，开通高级防护配置。

- Web 攻击防护 ：您可以选择开启 Web 攻击防护。
  - 防护等级：分为宽松、中等、严格、高危，防护严格程度逐渐加大，适用于不同的业务防护场景。
  - 防护模式：选择拦截，当节点检测到 Web 攻击请求时，会拦截该请求，并按拦截页面设置，响应默认拦截页面和 403 状态码，或将请求重定向至用户自定义拦截页面。选择观察，后台监控并记录访问行为，不做其他防护操作。
  - 自定义页面地址：当设置拦截页面为“自定义页面”时，节点将重定向所拦截的 Web 攻击请求至指定的自定义拦截页面。
  - 重定向状态码：可指定上述重定向响应的状态码301或302。
- BOT 爬虫防护：初次开启 BOT 爬虫流量智能检测，默认为观察模式，不会影响现网业务。

提交配置

域名配置完成后，单击**提交**，即可添加域名。在弹出框中，单击**返回防护配置**，即可返回安全加速域名列表页，查看域名配置，或对域名安全配置进行进一步调整。单击**继续添加**继续添加安全加速域名。添加的域名，系统将在后台为您部署相关配置，生效时间大约为5分钟。

域名操作

最近更新时间：2023-11-03 11:32:13

您可以在 SCDN 控制台，对已经接入 SCDN 的域名进行删除和安全加速配置管理等操作。

删除域名

您可以**删除**安全加速域名，关闭域名的安全加速服务。删除域名后，安全加速配置将不会保留，具体操作如下。

> **说明**
> - 安全加速服务关闭后，域名 CDN 加速服务将继续生效，不会受到影响。
> - 在 SCDN 控制台页面，找到需要停止安全加速服务的域名，需要先点击**关闭防护**，再**删除**域名。
> - 列表支持对多个域名批量操作。

管理配置

您可以查看和变更域名安全加速配置，具体操作如下。

- 在 SCDN 控制台页面，找到需要查看或变更安全加速服务配置的域名，单击**管理**。
- 配置管理相关详情请参见 配置管理 。

配置管理
配置指引

最近更新时间：2021-10-15 17:17:20

您可以在 SCDN 控制台中查看域名的安全加速配置。您可以根据业务需要对域名的防护配置策略进行修改。修改提交后，系统将在后台为您部署相关配置，生效时间大约为5分钟。

域名配置页面

登录 SCDN 控制台，找到需要查看或变更安全加速服务配置的域名，单击**管理**。

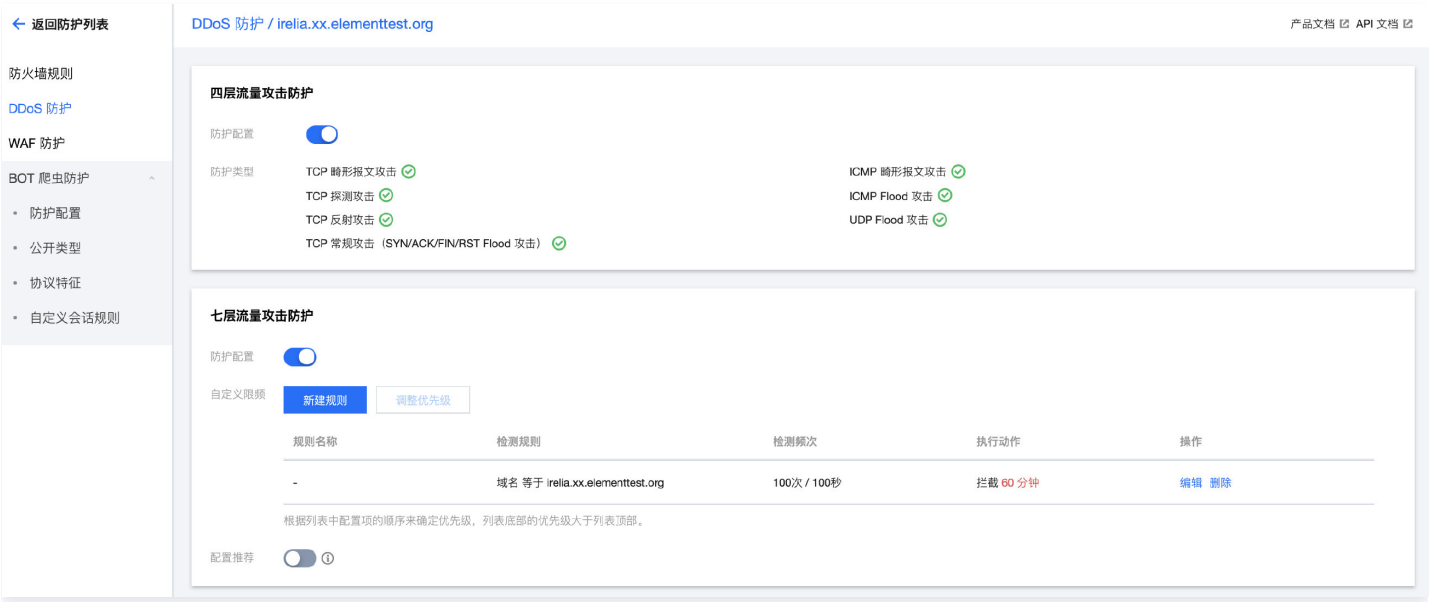
域名管理页面展示该域名所有安全防护配置，包括域名防火墙规则、 DDoS 防护、Waf 防护、BOT 爬虫防护配置策略等。您可以在左侧防护类型中选择并查看详细的防护配置信息。

防火墙规则

用户自定义的防火墙规则，操作指引详见 防火墙规则 。

DDoS 防护

四层流量攻击防护与自定义七层流量攻击防护，操作指引详见 DDoS 防护 。

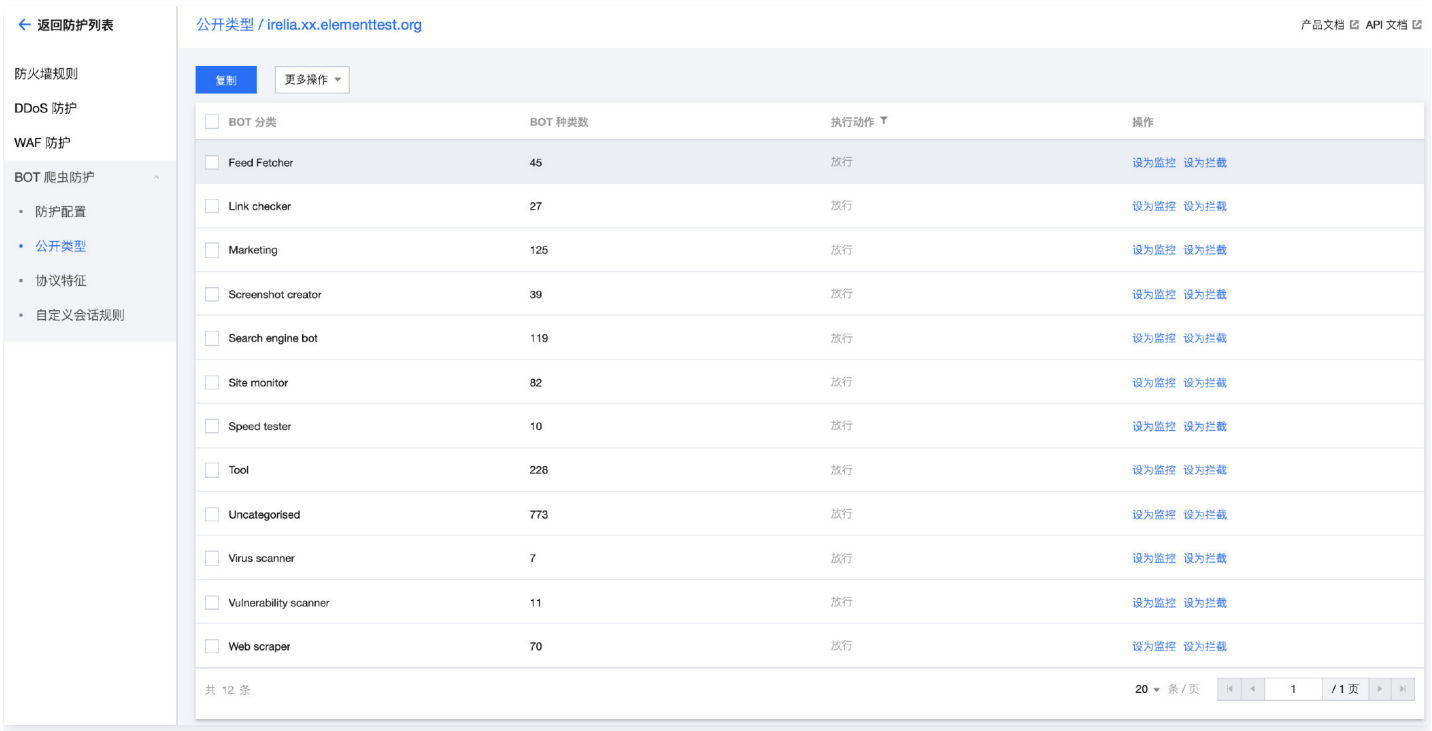


WAF 防护

WAF防护规则库与自定义 WAF 路径白名单，操作指引详见 WAF 防护 。

BOT 爬虫防护

BOT 爬虫防护策略库与自定义 BOT 会话规则配置，操作指引详见 BOT 爬虫防护 。



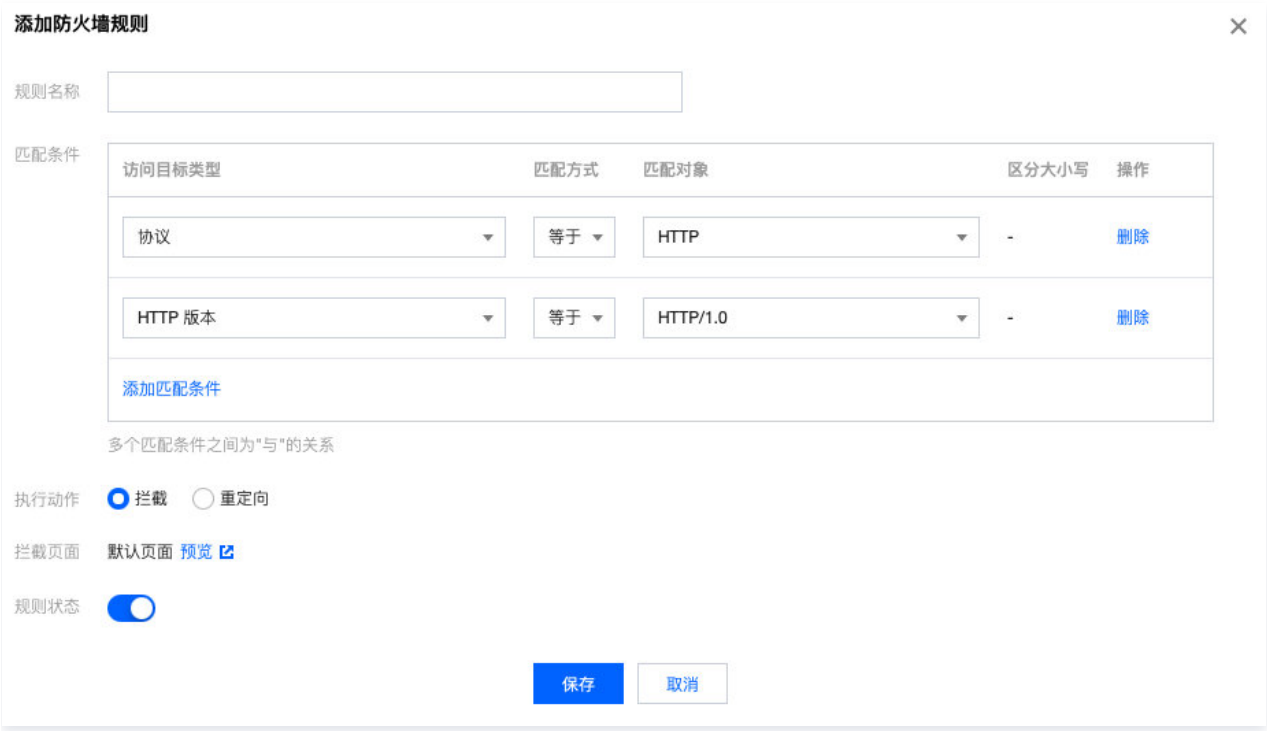
修改配置
防火墙规则

最近更新时间：2023-11-03 11:32:13

您可以在域名管理页面，对域名的防护策略进行修改。

应用场景

安全加速支持精确至 IP、URI、Referer、User-Agent 等字段的复杂访问规则配置，您可以根据业务场景，配置自定义的防火墙防护策略，对请求进行多条件组合过滤。



防护配置

- 添加、修改防护规则
  - 支持创建规则上限为200条， 每一条规则中可定义20个匹配条件 。规则之间为“或” 关系、匹配条件之间为 “与” 关系，满足任意规则中的任意一条条件，即会触发防护规则，执行配置的防护动作。
  - 访问目标类型支持：协议、HTTP 版本、请求方法、ASN、请求源 IP、国家、大区、XFF、URI、首页、文件全路径、文件拓展名、请求参数、Referer、Cookie、User- Agent、自定义请求头。
  - 匹配方式支持：包含、不包含、等于、不等于、长度小于、长度等于、长度大于。
  - 匹配对象仅允许填写**一个**匹配项，暂时不支持正则匹配，不填写默认为空。
- 停用、删除规则
  - 您可以单击**停用**，使某一条规则暂停生效；单击**启用**再次启用规则。
  - 您可以单击**删除**，删除某一条规则。被删除的规则将不可恢复。
- 调整优先级
  - 您可以单击**调整优先级**调整规则列表各条规则的顺序。在当前匹配逻辑下，规则顺序不影响最终拦截结果。

DDoS 防护

最近更新时间：2023-11-03 11:32:13

您可以在域名管理页面，对域名的防护策略进行修改。

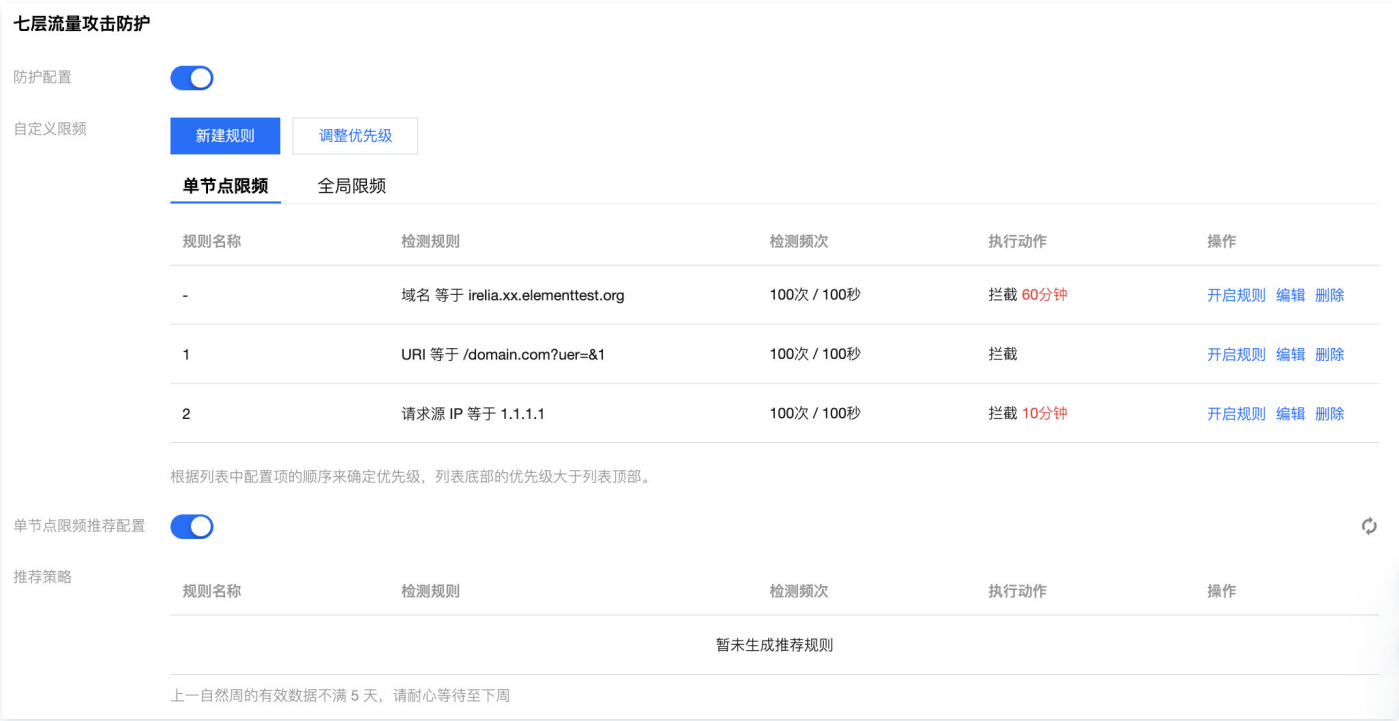
应用场景

安全加速基于腾讯云先进特征识别算法对请求流量进行精确清洗，抵御 SYN Flood、TCP Flood、ICMP Flood 等各类四层流量攻击，同时依赖自研智能行为判定、拦截专利技术，根据平台推荐拦截策略，结合用户多维度自定义规则对恶意七层流量攻击进行分析、拦截。

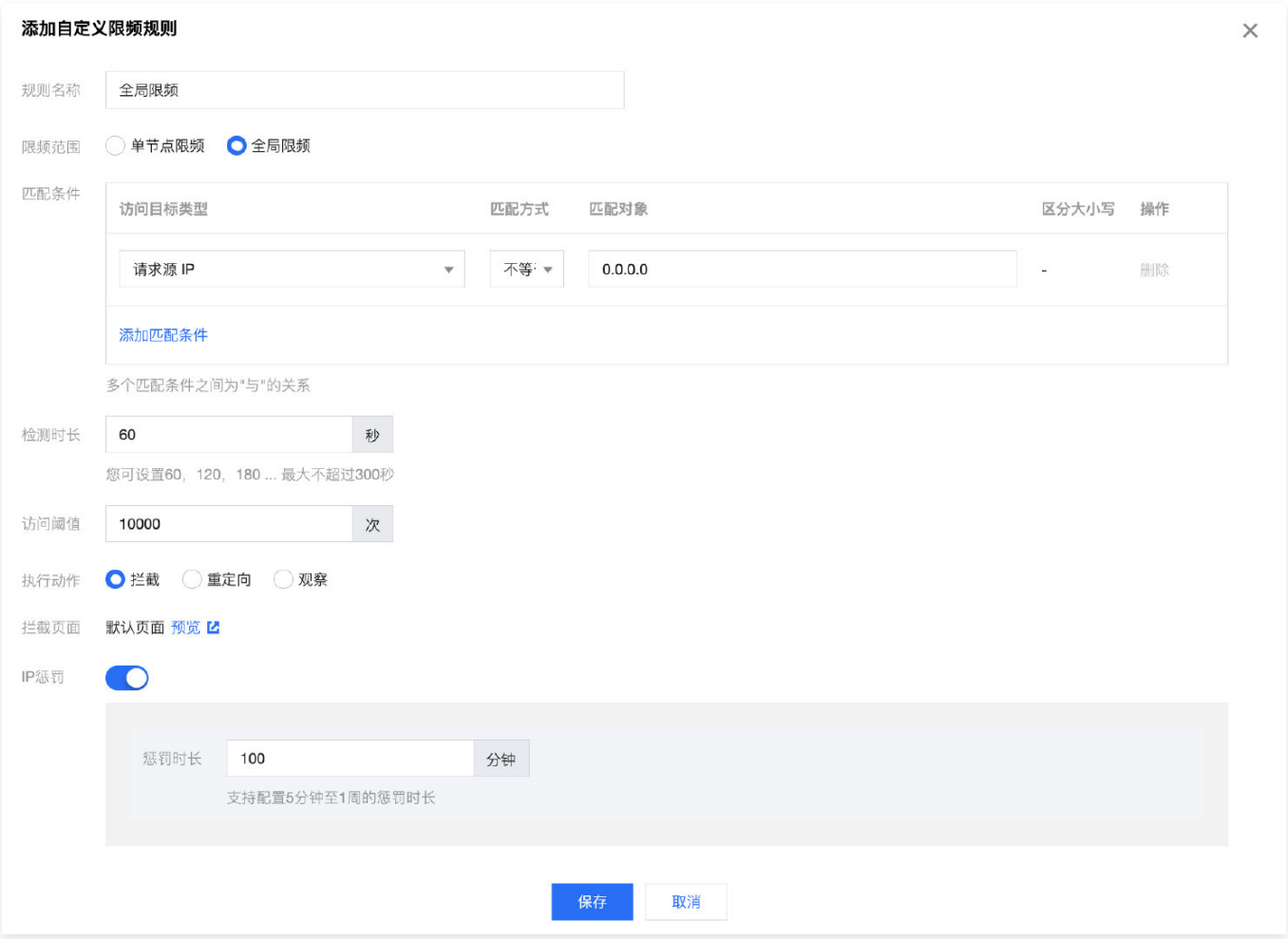
防护配置

- 域名的四层流量攻击防护默认开启。

- 域名的七层流量攻击防护通过　定义限频配置进　观察/拦截/重定向，达到控制恶意　频请求的　的。该功能默认关闭，需要您开启并设置自定义限频规则后，才能拦截七层流量攻击。



- 配置推荐：开启后，会根据上个自然周的历史数据生成配置策略推荐。
- 单击**新建规则**弹窗设置自定义限频规则。您可根据业务需求配置检测时　、访问阈值，为避免策略配置影响到正常　户访问，可先配置为**观察**模式，发现恶意 IP 、UA　为后，再进　拦截/重定向设置。



- **访问目标类型**：您可根据协议、请求方法、域名、请求源 IP、URI、首页、文件全路径、文件拓展名、请求参数、Referer、Cookie、User-Agent、自定义请求头等特征进行规则配置，对具有一定特征的高频攻击进行拦截。
- **访问频次**：您可根据业务情况设置访问频次。建议输入正常访问次数的3倍 – 10倍，例如，网站人平均访问20次/分钟，可配置为60次/分钟 – 200次/分钟，可依据被攻击严重程度调整。
- **IP 惩罚**：您可根据业务情况，结合拦截动作对明显具有攻击特征的 IP 进行惩罚，不允许其访问。我们将根据您设置的匹配条件和检测时长，对触发访问阈值的 IP 进行惩罚。

> **注意**
> IP 惩罚仅面向单节点、单 IP 进行访问频次统计与惩罚。

WAF 防护

最近更新时间：2023-12-28 10:18:01

您可以在域名管理页面，对域名的防护策略进行修改。

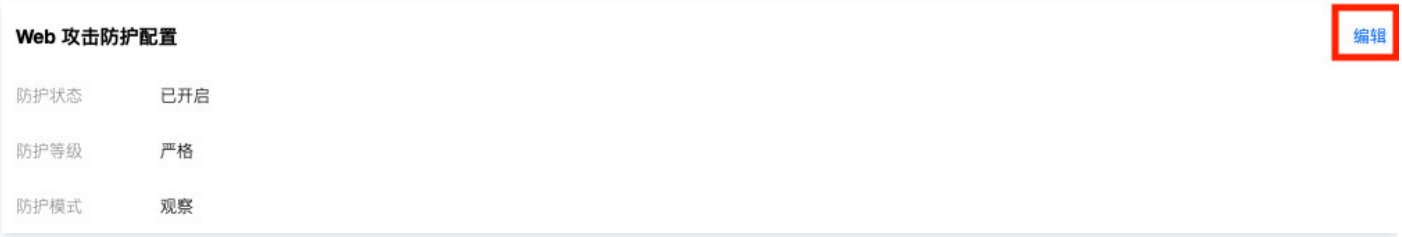
应用场景

安全加速基于腾讯海量 Web 攻击样本库，支持对访问进行特征匹配，有效抵御 SQL 注入、XSS 攻击、本地文件包含等各类 Web 攻击，实时保护用户源站。

防护配置

1. 登录 SCDN 控制台，进入 WAF 防护管理页面，可编辑 Web 攻击防护配置，查看防护规则明细。

2. 单击**编辑**，支持弹窗修改防护等级和防护模式。



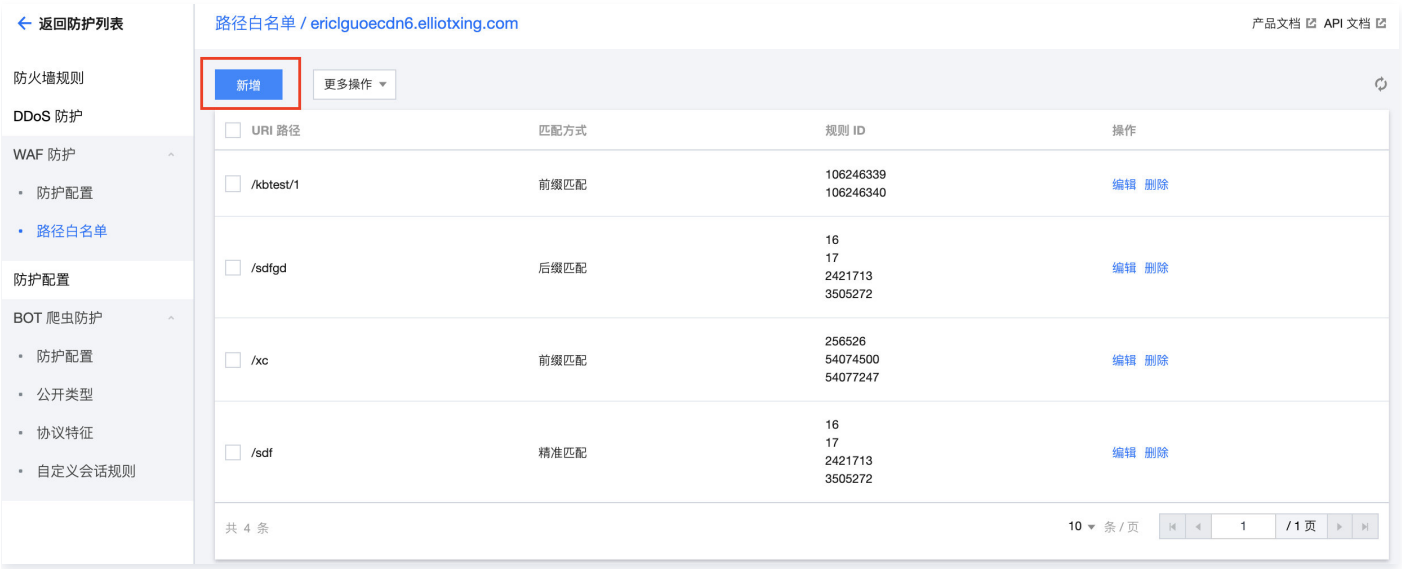
- 您可以选择开启 Web 攻击防护，调整防护等级。
- 防护等级：域名开启 Web 攻击防护配置时，可根据业务要求，配置宽松、中等、严格、高危四种级别的防护策略。其中，中等包括了中等与宽松等级的 Web 防护规则，严格包括了宽松、中等、严格等级的 Web 防护规则。以此类推，防护等级越严苛，防护规则越丰富，越有效识别攻击。
- 防护模式：支持拦截和观察。选择拦截，当节点检测到 Web 攻击请求时，会拦截该请求，并按拦截页面设置，响应默认拦截页面和403状态码，或将请求重定向至用户自定义拦截页面。选择观察，仅记录被判定为 Web 攻击的请求及其被识别的攻击类型，不会影响正常响应。
- 拦截页面：支持配置默认页面和自定义拦截页面。后者，节点将重定向所拦截的 Web 攻击请求至指定的自定义拦截页面。
- 重定向状态码：可指定上述重定向响应的状态码301或302。

3. 规则类型：Web 攻击防护规则按照防护的攻击类型分为以下 类，共计430条规则细则，除了根据规则等级进 宽松、中等、严格、高危策略调整外，也可针对规则细则进 开启/关闭。

攻击分类	攻击描述
命令/代码注入攻击	注 攻击的 种，包含 shell 命令注 ，PHP 代码注 ，Java 代码注 等。若被攻击者成功利 ，可导致 站执 攻击者注 的代码。
开源组件漏洞	常见 Web 开源组件漏洞产生的攻击行为。
SQL 注入攻击	在网站实现上，对于输入参数过滤不严，导致 SQL 数据库的内容被非法获取。
任意 件读取/下载	检测某些配置 件、数据库 件及参数数据，是否被随意下载。
文件上传攻击	当上传文件伪装成正常后缀的恶意脚本时，攻击者可借助本地文件包含漏洞执行该文件。
其他漏洞攻击	由于Web 服务器本身安全和其他软件配置安全或漏洞引起的攻击。
常 CMS 漏洞攻击	内容管理系统CMS，如wordpress,phpcms,discuz等存在漏洞，导致站点 临 侵威胁。
XSS 跨站脚本攻击	当应用程序的新网页中包含不受信任的、未经恰当验证或转义的数据，或者使用可以创建 HTML 或 JavaScript 的浏览器 API 更新现有的网页时，会出现 XSS 缺陷。XSS 让攻击者能够在受害者的浏览器中执行脚本，并劫持用户会话、破坏网站或将用户重定向到恶意站点。
扫描器攻击漏洞	检测 站是否被恶意扫描。
Webshell 检测攻击	攻击者上传webshell 后 ，得到 个命令执 环境，已达到控制 站服务器的 的。
XXE 攻击	由于 XML 处理器在 XML 件中存在外部实体引 。攻击者可利 外部实体窃取使 URI 件处理器的内部 件和共享 件、监听内部扫描端 、执 远程代码和实施拒绝服务攻击。
LDAP 注 攻击	攻击者通过ldap（轻量级 录访问协议）注 攻击，可以获取敏感数据。
常 OA 漏洞攻击	针对常 OA、邮箱的等国产闭源软件的漏洞防护。
服务端模板注入漏洞	服务端错误的将用户输入作为模板进行解析，导致了模板中恶意语句被执行，进而造成代码执行等。
服务端请求伪造	防护攻击者借助服务器访问请求接口的缺陷发起恶意请求的攻击。
未授权访问漏洞	一些管理后台，调试页面，没有对请求的用户进行权限校验，攻击者利用系统的一些功能，可能造成敏感信息的泄漏，代码执行等。

路径白名单

安全加速支持基于指定 WAF 规则，添加针对特定域名的路径白名单。白名单生效后，该路径不会触发指定的 WAF 规则防护。



- 单击**新增**添加需要添加白名单的路径 URI。
- **匹配方式：支持 URI 全路径精准匹配，URI 前缀匹配、URI 后缀匹配。**

BOT 爬虫防护

最近更新时间：2023-11-03 11:32:13

您可以在域名管理页面，对域名的防护策略进行修改。

应用场景

融合腾讯云 Web 防火墙 AI+规则的 Bot 爬虫防护功能，面向全量加速请求进行行为分析，对友好及恶意的 Bot 爬虫进行甄别，支持自定义策略管理。

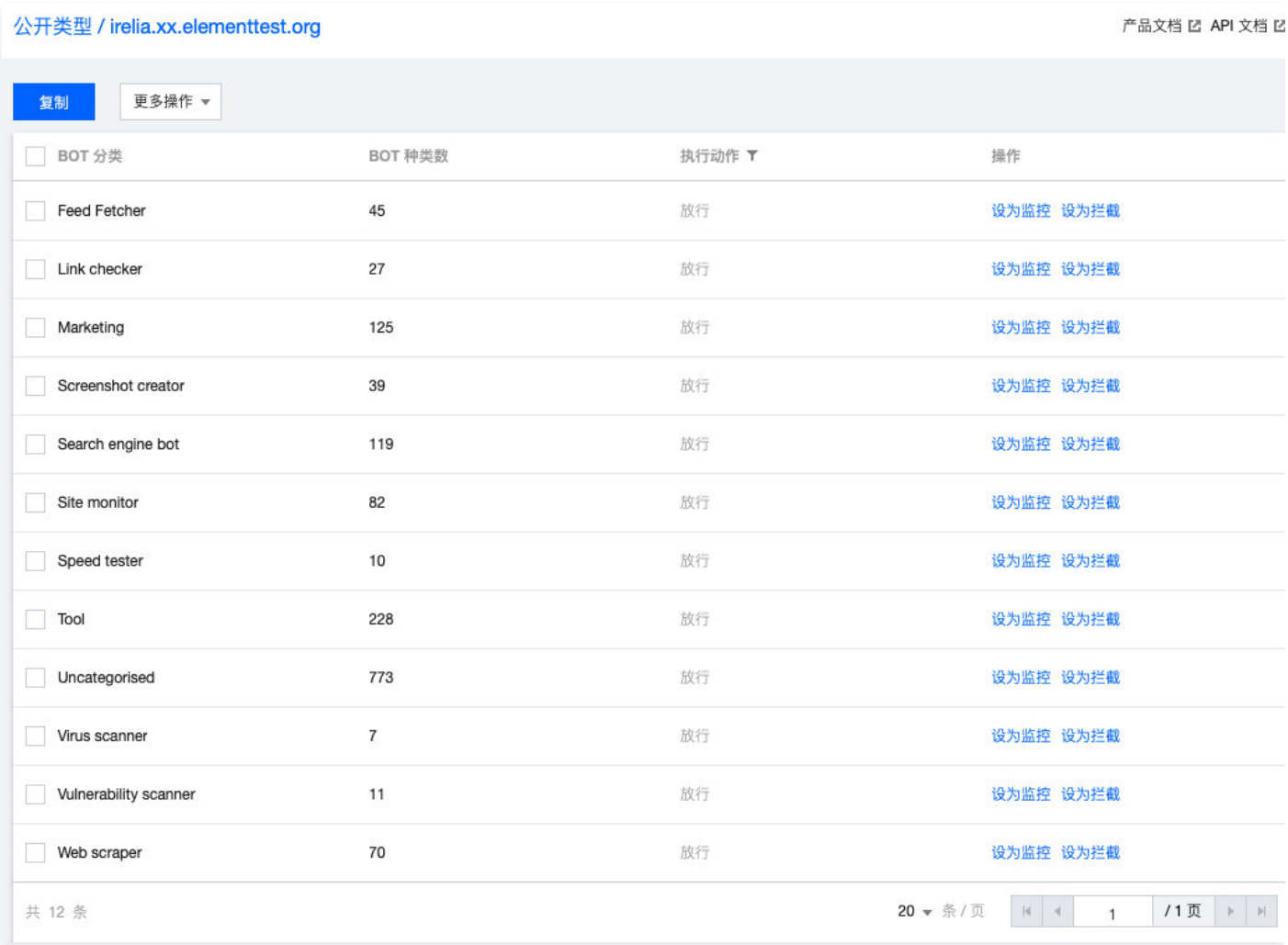
防护配置

购买 BOT 防护功能的用户，可登录 SCDN 控制台，进入 BOT 防护管理**防护配置**页面，开启/关闭 BOT 防护。

公开类型策略配置

SCDN 前提供12个已知公开的 BOT 类，超过1000+的 BOT 类，包括搜索引擎、测速 具、内容聚合、扫描和 爬 等类别。 户可以根据 身需求对公开 BOT 类别设置防护动作（放 、监控、拦截），防护引擎将对命中公开类型的 BOT 请求进 相应处理。进入 **BOT 爬虫防护** > **公开类型**页面，默认展示 BOT **公开类型**列表，页面操作说明如下：

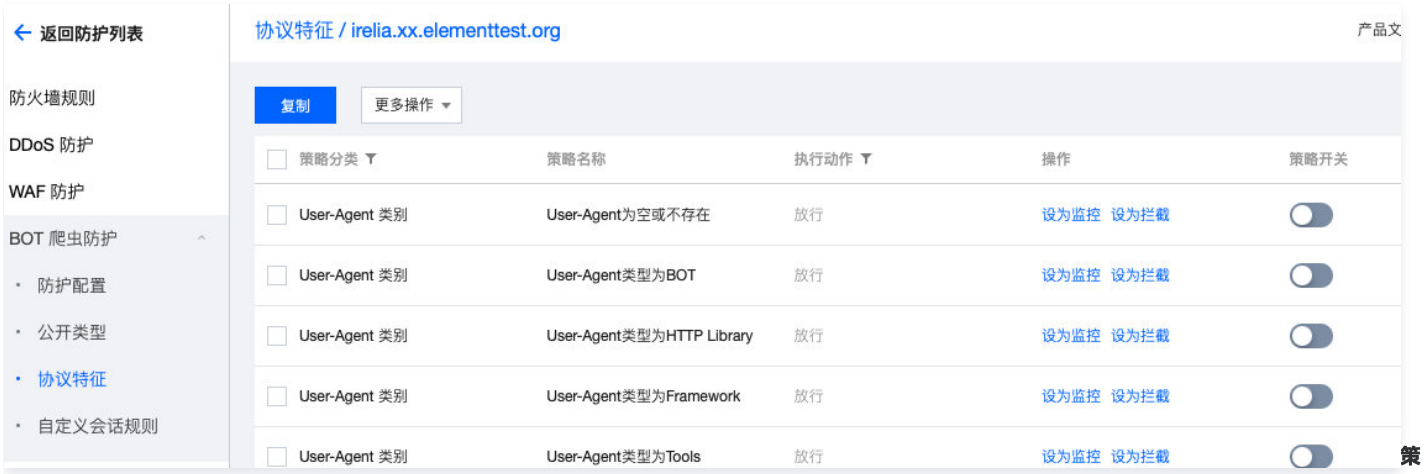
- 单击**设为监控**：若访问域名出现该 BOT 行为将触发 BOT 监控。
- 单击**设为拦截**：若访问域名出现该 BOT 行为将触发 BOT 拦截。



- **单击复制：**可以将当前域名的公开类型 BOT 设置信息复制到其他开启了 BOT 防护的域名，最多可选20个域名。

协议特征策略配置

安全加速支持17种协议特征 BOT 防护规则配置。



略分类：分为 User-Agent 类别、HTTP 头部、HTTP 协议特征。
执行动作：协议特征策略开启时默认动作为“放行”，可通过右侧操作栏进行设置为“拦截”或者“监控”。
策略开关：默认为关闭。您可根据业务需求开启单项协议特征策略。

自定义会话规则配置

安全加速支持用户可自定义配置BOT会话特征规则，进入**自定义会话规则**页面。

策略名称：策略名称和描述信息。
匹配条件：策略匹配条件内容，1条策略最多可以添加10个匹配条件，匹配条件之间是“与”的关系。
执行动作：策略动作信息，展示添加策略时设置的动作信息，可通过右侧操作栏进行修改。
操作：对策略进行编辑或删除操作。单击**编辑**可进行规则内容修改。
策略开关：展示添加策略时设置的开关状态信息。
批量操作：支持批量编辑自定义会话特征（如，统一修改执行动作、复制到其他已开启 BOT 防护的域名等）。

单击**新增配置**：添加自定义会话特征。

定义会话特征匹配条件说明如下：

分类	过滤条件	条件说明
会话特征	会话平均速度	为会话请求总次数 / 会话持续时间，单位为：次/分钟。
	会话窗口速度	每2分钟（窗口）内的会话访问速度，单位为：次/分钟。
	会话总次数	一个 BOT 会话发生的总访问次数。

	会话持续时间	BOT 会话的持续时间。
	会话存在 Robots.txt	会话请求中访问 Robots.txt 文件。
	会话发生在凌晨	会话请求发生在凌晨2:00 – 5:00之间。
请求特征	请求最多的 URL	会话请求中，请求最多的 URL。
	URL 重复比	会话请求中 URL 重复比例，取值范围0 – 1，根据实际业务情况，进行参数配置，过高或过低为疑似异常（根据实际情况进行判断）。
	URL 种类	会话请求中 URL 去重后条目数。
	请求最多的参数	会话请求出现最多的参数，包括 GET 请求参数（Query 内容）或 POST 请求参数（Body 内容）。
	参数重复比	会话请求中 GET 请求参数（Query 内容）或 POST 请求参数（Body 内容）重复比例，取值范围0 – 1，根据实际业务情况，进行参数配置，过高或过低疑似异常（根据实际情况进行判断）。
COOKIE	COOKIE 存在性	会话请求中，判断 HTTP 头部字段是否存在 COOKIE。
	请求最多的 COOKIE	会话请求中， 出现最多的 COOKIE。
	COOKIE 重复比	会话请求中 COOKIE 的重复比例，取值范围0 – 1。
	COOKIE 存在比	会话请求中 COOKIE 存在比例，取值范围0 – 1。
	COOKIE 滥用	多种不同的 UA 使用相同的 COOKIE。
	COOKIE 种类	会话请求中 COOKIE 去重后的数目。
Referer	Referer 存在性	会话请求中，判断 HTTP 头部字段是否存在 Referer。
	请求最多的 Referer	会话请求中，HTTP Referer 字段出现最多的值。
	Referer 重复比	会话请求中 Referer 的重复比例，取值范围0 – 1，对浏览器访问有效，过高疑似异常（根据实际情况进行判断）。
	Referer 存在比	会话请求中 Referer 存在比例，取值范围0 – 1，对浏览器访问有效，过低疑似异常（根据实际情况进行判断）。
	Referer 滥用	多种不同的 UA 使用相同的 Referer。
	Referer 种类	会话请求中 Referer 去重后的数目。
UA	UA存在性	会话请求中，判断 HTTP 头部字段是否存在 User-Agent。
	请求最多的 UA	会话请求中，HTTP User-Agent 字段出现最多的值。
	UA 存在比	会话请求中 UA 的存在比例，取值范围0 – 1，过低疑似异常（根据实际情况进行判断）。
	UA 种类	会话请求中 UA 去重后的数目，过多疑似异常（根据实际情况进行判断），对非代理 IP 有效。
	UA 类型	UA 类型为浏览器。UA 类型为移动端。UA 类型游戏终端或电视终端。UA 类别为公开 BOT 类型。UA 类别为未公开 BOT 类型。UA 类别为自动化工具。UA 类别为未知类型。UA 类别为公开扫描器。UA 类别为开发框架。UA 类别为语言 HTTP 库。
	UA 随机性指数	会话请求中 UA 的随机分布情况，取值范围0 –1，指数越高越异常。 参考值阈值：超过0.6疑似异常，指数超过0.92基本确定为异常。
其他 HTTP 头部	Accept 存在性	会话请求中判断 HTTP 头部字段是否存在 Accept 字段。
	Accept-Language 存在性	会话请求中判断 HTTP 头部字段是否存在 Accept-Language 字段。
	Accept-Encoding 存在性	会话请求中判断 HTTP 头部字段是否存在 Accept-Encoding 字段。
	Connectiton 存在性	会话请求中判断 HTTP 头部字段是否存在 Connectiton 字段。
	请求方法占比	会话请求中判断请求使用方法。

	返回状态码比例	会话请中 WAF 返回给客户状态码比例。

攻击监控

Web 攻击监控

最近更新时间：2023-11-03 11:32:13

功能简介

安全加速 SCDN 提供实时监控与数据统计功能。进入控制台 攻击监控，您可以查看域名的 Web 攻击监控数据。

页面说明

筛选查询条件

- 在页面左上角设置查询时间范围。单击域名筛选框，进行域名选择或搜索。
- 选择防护地域和攻击类型，单击**查询**可查看所选时间段内攻击数据。

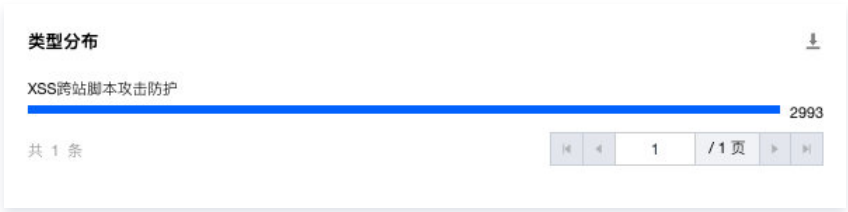
查看监控数据

Web 攻击监控数据分为四个模块：Web 攻击次数、域名排行、类型分布、攻击次数排行。

1. Web 攻击次数：根据上方筛选条件，展示 Web 攻击次数监控数据。支持选择不同的统计时间粒度（每分钟/每5分钟/每小时）查看 Web 攻击次数，支持数据下载。

2. 域名排行：根据上方筛选条件，从大到小展示被 Web 攻击的域名、攻击次数以及攻击占比。其中，攻击占比=该域名被 Web 攻的次数/整个账号被 Web 攻击的总次数。

3. 类型分布：监控页面按攻击类型进行 Web 攻击数据展示。



4. 攻击次数排行：支持 “URL” 或者“攻击源 IP” 筛选，展示攻击次数排行。

- 若选中 “URL”，则展示域名、URL、总攻击次数、最后攻击时间。
- 若选中“攻击源 IP”，则展示攻击 IP、IP 所属地区、总攻击次数、最后攻击时间。

DDoS 攻击监控

最近更新时间：2023-11-03 11:32:13

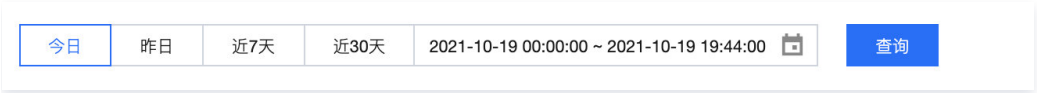
功能简介

安全加速 SCDN 提供实时监控与数据统计功能。进入控制台 攻击监控，您可以查看域名的 DDoS 攻击监控数据。

页面说明

筛选查询条件

在页面左上角设置查询时间范围，展示指定时段内账户内所有域名 DDoS 攻击防护情况。

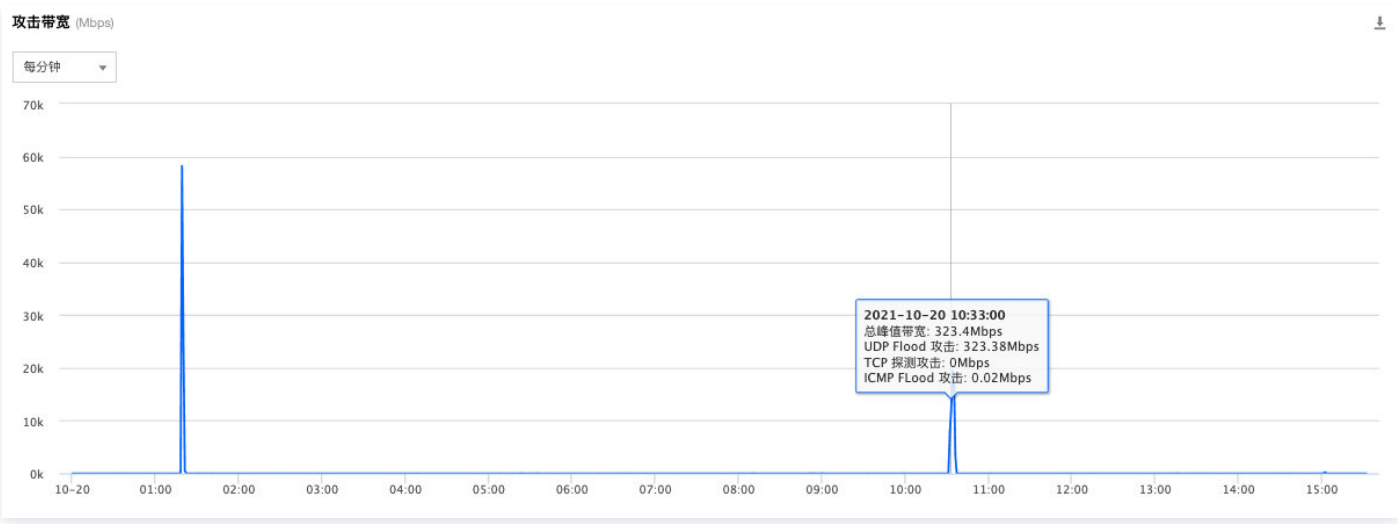


查看监控数据

DDoS 攻击监控数据分为三个模块：攻击带宽、攻击类型分布、TOP 10 DDoS IP排名。

1. 攻击带宽：查看该时间范围内 DDoS 防护遭受的攻击情况，根据1分钟 DDoS 攻击总流量除以时间（60秒）折算而来。支持不同时间粒度（每分钟/每5分钟/每小时）查看历史数据，支持数据下载。

   攻击事件：将鼠标悬停在攻击带宽曲线上任意点，可了解该时间节点发生的攻击事件总峰值带宽以及所有攻击类型带宽消耗。



2. 攻击类型分布：根据攻击带宽大小，从大到小顺序展示各攻击类型。

3. TOP 10 DDoS IP 排名：展示攻击次数排名前十的 DDoS 攻击源 IP 相关信息。

Top 10 DDoS IP 排名

攻击源 IP	IP 归属	攻击次数
61.151.182.206	上海市 中国电信	410440077
121.14.91.25	广东省 中国电信	151133431
59.36.128.146	广东省 中国电信	139918227
47.101.55.143	上海市 阿里巴巴	101605921
58.251.121.90	广东省 中国联通	87506400
61.151.180.54	上海市 中国电信	45971163
116.128.163.145	上海市 中国联通	35917560
61.129.7.179	上海市 中国电信	33319730
183.192.173.200	上海市 中国移动	31230347
112.49.60.183	福建省 中国移动	28513404

CC 攻击监控

最近更新时间：2023-11-03 11:32:13

功能简介

安全加速 SCDN 提供实时监控与数据统计功能。进入控制台 攻击监控，您可以查看域名的 CC 攻击监控数据。

页面说明

查询条件筛选

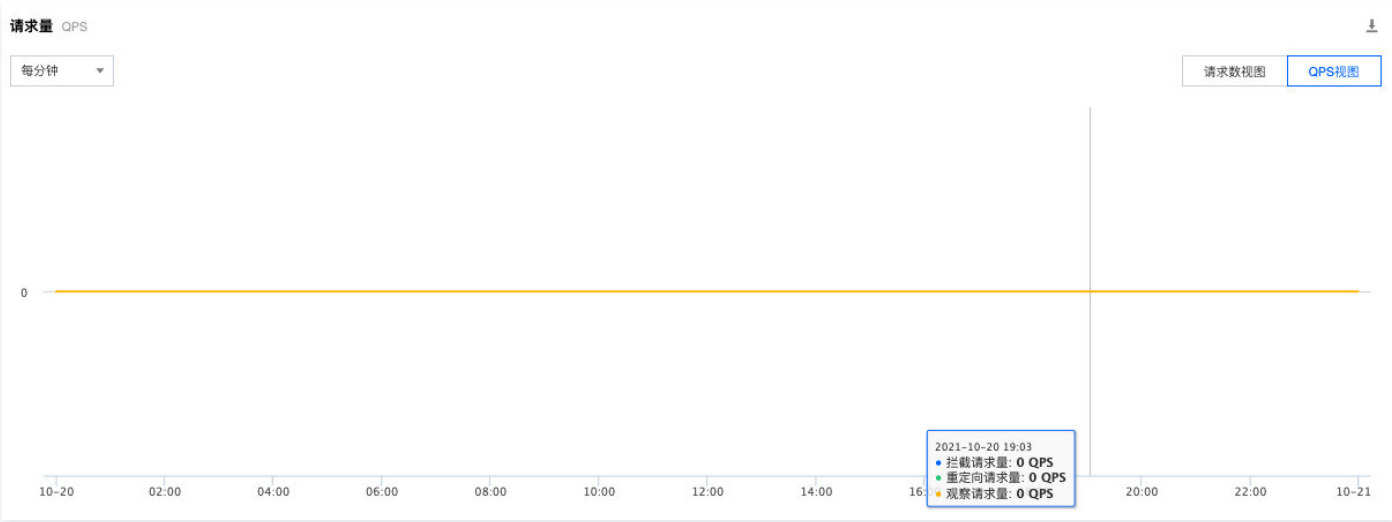
- 在页面左上角设置查询时间范围。单击域名筛选框，进行域名选择或搜索。
- 选择防护地域和执行防护动作，单击**查询**可查看所选时间段内攻击数据。

查看监控数据

CC 攻击监控数据分为四个模块：请求数视图、QPS 视图、攻击源排名、攻击请求 TOP UA。

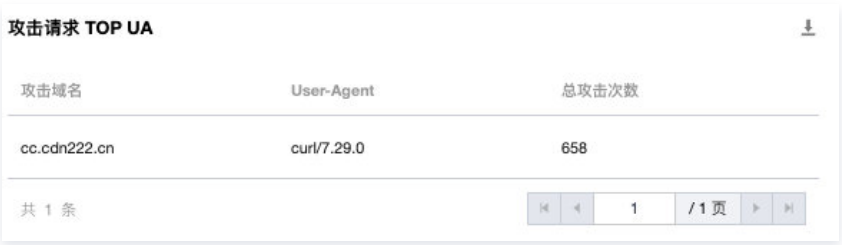
1. 请求数视图：从请求数维度展示 CC 攻击情况，支持数据下载。

2. QPS 视图：即请求量视图，展示服务器在单位时间内处理的 CC 攻击流量，计算公式为：QPS = 并发量/平均响应时间。该视图支持不同时间粒度（每分钟/每5分钟/每小时）QPS 历史数据查询。



3. 攻击源排名：根据攻击源 IP 的总攻击次数（从多到少）展示历史数据排名。该模块展示攻击域名、攻击源 IP、目标 URL、总攻击次数信息。

4. 攻击请求 TOP UA：根据攻击源 User-Agent 的总攻击次数（从多到少）展示 TOP UA 排名。该模块展示攻击域名、User-Agent、总攻击次数信息。



说明

CC 攻击监控展示内容为新版七层流量攻击防护监控数据。

BOT 行为监控

最近更新时间：2023-11-03 11:32:14

功能简介

安全加速 SCDN 提供实时监控与数据统计功能。进入控制台 攻击监控，您可以查看 BOT 分析监控数据。

页面说明

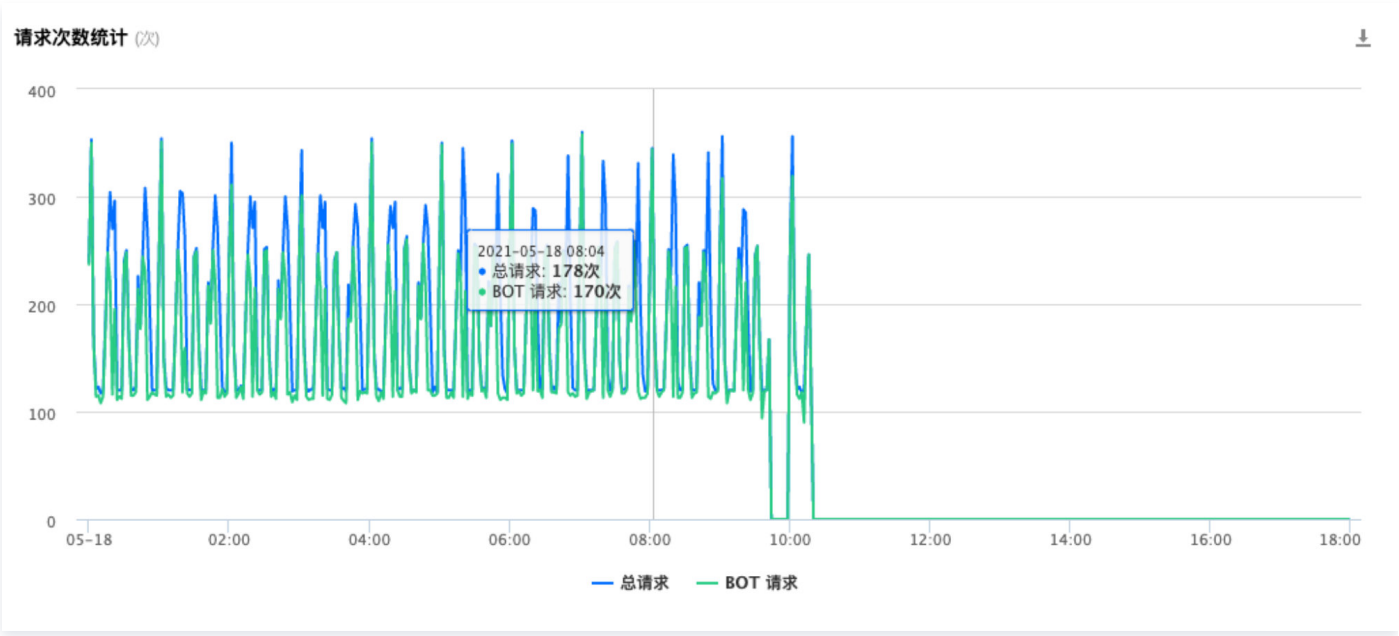
查询条件筛选

- 单击域名筛选框，进行域名选择或搜索。
- 选择防护地域，设置查询时间范围，可查看 BOT 分析数据。

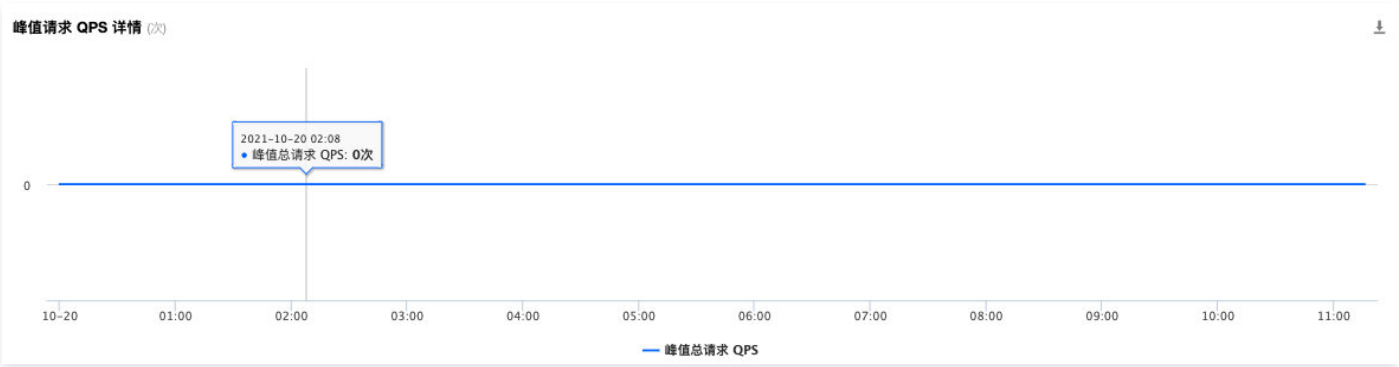
查看监控数据

BOT 分析数据分为四个模块：请求次数统计、峰值请求 QPS 详情、TOP BOT IP 排名、TOP BOT 会话数域名。

1. 请求次数统计：提供总请求和 BOT 请求次数趋势统计，单天数据（例如，近1小时、近6小时、今日、昨日）数据统计粒度为2分钟，多天区间数据（例如近7天）数据统计粒度为1小时，支持数据下载。

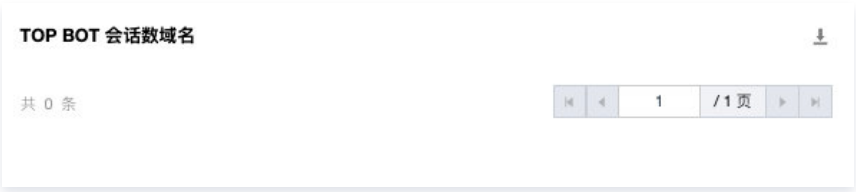


2. 峰值请求 QPS 详情：根据用户选择的时间区段，展示峰值请求数据。



3. TOP BOT IP 排名：提供攻击源 IP 按攻击次数（从多到少）排名、及其对应的 IP 归属。

4. TOP BOT 会话数域名：提供按 BOT 会话数（从多到少）的域名排名。



事件日志

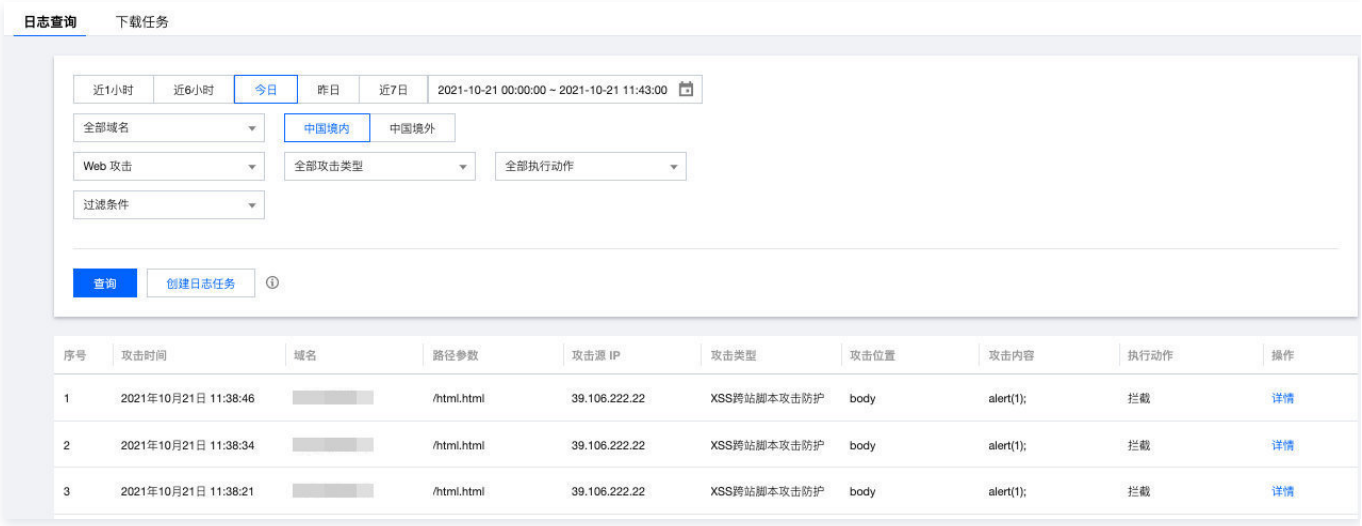
最近更新时间：2024-01-12 16:46:31

功能介绍

安全加速 SCDN 对 Web 攻击/CC 攻击/BOT 会话的 志信息进行记录，您可以根据需要，查看并下载日志详情。

操作指引

1. 查看安全日志
   设置查询时间范围，进行域名选择和攻击类型条件筛选，单击**查询**可查看日志。
   - Web 攻击 志查询： 持根据攻击类型、执 动作进 筛选，也 持针对攻击位置和攻击源 IP 进 过滤。针对过滤出来的条 ，单击右侧**详情**进 详情 ，可查看明细日志。

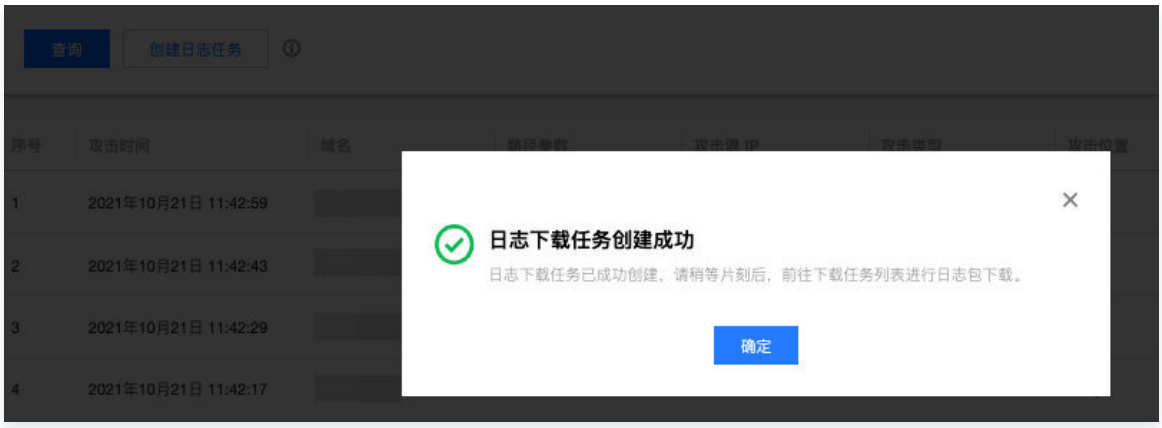


   - CC 攻击 志查询： 持根据执 动作（拦截/观察/重定向）进 筛选，也 持针对攻击源 IP 进 过滤。针对过滤出来的条 ，单击右侧**详情**进 详情 ，可查看 志明细。

   - BOT 会话 志查询： 持根据 BOT 类型（未知/自定义/公开类型）进 筛选，也 持针对攻击源 IP 进 过滤。针对过滤出来的条 ，单击右侧**查看详情**进 详情 ，可查看基础信息和访问详情。

2. 创建及下载日志

- 根据查询的日志列表，单击**创建日志任务**。



- 日志任务创建后，切换到**下载任务**页面，单击**下载**即可获取离线日志。

说明

- BOT 会话仅支持下载查询列表，详情请在**查看详情**页中查看。
- SCDN 支持下载最近1周范围内的攻击日志。
- 单个日志任务最多支持下载1000条日志；每日允许创建100个下载任务。
- 日志任务生成的日志文件保留7天。

日志字段说明

SCDN 事件日志文件包命名方式为 `[host]-scdn-[uuid]`，默认打包为 `.gz` 文件。其中 [host] 为指定域名，[uuid] 为该日志任务的唯一识别码。日志文本使用 JSON 格式，其中攻击记录包含的字段及其含义如下表所示：

字段名（key）	中文名/释义	字段值（value）示例

datetime	请求日期、时间（北京时间 UTC+8），格式为 YYYYMMDDHHMMSS	20200514145500
server_ip	边缘安全节点 IP	119.29.29.29
client_ip	客户端 IP	119.29.29.29
host	请求域名	cloud.tencent.com
path_query	请求路径、查询字符串	/cache.txt?id=1%20or%205=5
status_code	响应状态码。当 WAF 状态码为 566 时，Web 攻击防护执行动作为拦截；当状态码为其他时，执行动作为观察。当 CC 状态码为 514 时，CC 攻击防护执行动作为拦截；为302/301时，CC 攻击防护执行动作为重定向；当状态码为其他时，执行动作为观察。	566
time_taken	响应时间（毫秒），指节点从收到请求后到响应所有回包所花费的时间	12
referer	请求 referer 头部信息	https://cloud.tencent.com/
user_agent	请求 User-Agent 头部信息	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
req_header_size	请求头部大小（字节）	360
req_body_size	请求正文大小（字节）	0
rsp_header_size	响应头部大小（字节）	259
rsp_bytes	响应字节数，节点实际响应客户端内容大小（字节），包括头部、正文	259
uuid	请求唯一标识符	2844838522671723187
action	CC日志特有。防护动作	intercept
waf_attack_payload	WAF 日志特有。Web 攻击请求的攻击内容	/cache.txt?id=1 or 5=5
waf_attack_type	WAF 日志特有。Web 攻击请求的攻击类型	xss
waf_attack_location	WAF 日志特有。Web 攻击请求发生的位置，例如请求参数、URI、IP 等	REQUEST_URI_RAW
cookie	WAF 日志特有。请求 Cookie 头部信息	isQcloudUser=false; language=zh
req_header	WAF 日志特有。请求头内容	略
rsp_header	WAF 日志特有。响应头部内容	略
req_body	WAF 日志特有。请求正文内容	略

关于 Web 攻击类型字段说明：

waf_attack_type	Web 攻击类型
webshell	Webshell 检测防护
oa	常见 OA 漏洞防护
xss	XSS 跨站脚本攻击防护
xxe	XXE 攻击防护
webscan	扫描器攻击漏洞防护
cms	常见 CMS 漏洞防护
upload	文件上传攻击防护

cmd_inject	命令/代码注入攻击防护
sql	SQL 注入攻击防护
osc	开源组件漏洞防护
file_read	任意文件读取/下载防护
ldap	ldap 注入攻击防护
other	其它漏洞防护
SSRF	服务器端请求伪造
ssti	服务端模板注入漏洞
backend	未授权访问漏洞