

边缘安全加速平台

用户使用指南

天翼云科技有限公司

1.1 产品简介	1
1.2 术语解释	4
1.3 产品优势	8
1.4 功能特性	10
1.5 应用场景	13
2 计费说明	
2.1 计费项	16
2.2 计费模式	16
3.操作指导	20
3.1 购买安全与加速服务	
3.2 服务概览	25
3.3 安全与加速	26
3.4 购买零信任服务	69
3.5 零信任服务	73
3.6 运营管理	89
3.7 计费详情	95
4 最佳实践	

目录

4.1 安全与加速接入配置最佳实践	96
5 常见问题	
5.1 计费类	
5.2 开通类	
5.3 操作类	
5.4 使用限制	

1.1 产品简介

1.1.1 产品定义

边缘安全加速平台-依托全国各地的分布式边缘资源并基于边缘云底座;利用云原生技术实现网络底层对性能、安全、算力原子能力编排融入统一网络;多终端、多协议(5G/L3/L4/L7等) all-in-one 的网络统一接入;自助化服务、运营管理与分析、可视化报表与分析等集中化的统一管理平台;满足不同场景需求的性能及安全智能边缘网络。



安全与加速服务

基于天翼云边缘云节点提供加速和安全的解决方案,为政企、电商与零售、金融服务、内容资讯与游戏等 行业保驾护航,为用户提供加速与安全防护一体的服务。

加速方面:天翼云全国各地的分布式边缘节点更贴近用户,有效降低了数据访问时间延迟,避免数据传输 抖动,保障大量数据传输的稳定性和有效性。同时,产品提供了动静态数据加速,智能路由优化等加速特性,高效支撑对时延敏感的相关业务。

安全方面:抵御 DDoS 攻击、CC 攻击、Web 类攻击,爬虫攻击等网络攻击。节点识别并拦截 L3/L4/L7 层各类攻击请求,对 DDoS 攻击流量进行清洗,智能 AI 引擎、BOT 策略引擎对 Web、BOT、CC 类型攻 击进行行为分析并更新拦截策略,阻断恶意请求到达用户源站,保障业务访问流畅稳定。

零信任服务

利用天翼云全国各地的边缘云资源,基于边缘云底座原子能力为用户提供零信任服务。能够灵活部署到分 布式边缘云端且支持按需动态扩展,并具备安全插件结合能力抵御恶意攻击,实现简单、安全的远程访问 管理,同时针对不同的用户访问场景,不同的企业应用,提供一体化的配置管理功能,覆盖企业应用访问 全周期的安全防护能力,如访问请求拦截、流量转发、信息采集、流量管控、流量加密、建立双向认证的 访问通道等能力;无论访问企业应用的是员工,合作伙伴,还是用户,基于多因子认证以及多源评估策略 引擎,实现对用户访问始终认证,可信授权,帮助企业轻松地从根本上解决安全问题并提供卓越的访问体 验。

边缘接入服务

边缘接入服务包括应用安全加速网和边缘接入网(后续上线)。

应用安全加速网,结合安全抗 D,依托天翼云 CDN 平台的优质节点及线路,通过智能调度、传输优化等 核心自研技术,有效解决因公网链路抖动、拥塞等导致的源站响应慢问题,显著提升各类基于 TCP/UDP 协议的办公应用、业务系统、金融及游戏行业的各种动态指令及接口的访问速度与稳定性。

开发者平台

开发者平台提供 Serverless 边缘函数以及边缘存储。开发者无需关注服务部署区域、无需搭建和维护基础 设施,只需要一键部署代码,就可在天翼云的边缘节点上即时生效,就近响应终端用户或设备的请求。

1.1.2 版本功能差异对比

安全与加速服务

分类	高级版	企业版	旗舰版	备注
价格 (元/月)	3800	9800	83660	
流量 (/月)	1TB	2TB	5TB	流量/带宽二选一
业务带宽 (Mbps/月)	100	150	300	流量/带宽二选一
DDos 防护(/ 月)	防护带宽: 40Gbps 防护次数: 2 次	防护带宽: 无限防 防护次数: 2 次	防护带宽: 无 限防 防护次数: 不 限次数	
请求数 (万次/ 月)	200	400	1000	开启动态能力后, 开始计费动态请 求数
域名个数 (/月)	1	2	3	一级域名个数
静态加速 (/日)	文件刷新上 限:10000 条 url/日 目录刷新上 限:100 条/ 日 预取上限:	文件刷新上 限:10000 条 url/日 目录刷新上 限:100 条/ 日 预取上限:	文件刷新上 限: 10000 条 url/日 目录刷新上 限:100 条/日 预取上限: 1000 条 url/	

	1000条 url/ 日	1000 条 url/日	E	
动态加速	\checkmark	\checkmark	\checkmark	
WebSockets	默认超时时 间:1-50s	默认超时时 间: 1-120s	默认超时时 间:1-300s	
quic 协议	\checkmark	\checkmark	\checkmark	
IPv6 访问	\checkmark	\checkmark	\checkmark	
非标准端口防 护(除 80、 8080、443、 8443)	\checkmark	V	V	
web 防护-规 则防护引擎	\checkmark	\checkmark	\checkmark	
web 防护-Al 防护引擎	×	×	\checkmark	
web 防护-自 定义规则	\checkmark	\checkmark	\checkmark	
基础 bot 管理 (限时免费)	\checkmark	\checkmark	\checkmark	
CC 防护	\checkmark	\checkmark	\checkmark	
访问控制(/月)	20条/域名	50条/域名	100条/域名	
频率控制(/月)	20条/域名	50条/域名	100条/域名	
基础业务防护	\checkmark	\checkmark	\checkmark	网页防篡改、敏感 词防护
高级业务防护	V	V	V	撞库防护、广告防 护、批量注册、暴 力破解、web 挖 矿、跨站点 WebSocket 劫 持、CSRF 防护、 Cookie 防护
攻击挑战	\checkmark	\checkmark	\checkmark	
最大上传大小	300M	300M	500M	
服务	7*24 小时远	7*24 小时	1、7*24 小时	

	程	远程+微信 群支持	远程+微信群 支持	
			2、远程专家 咨询服务 3、重保服务	
SLA	99.5%	99.5%	99.5%	

零信任服务

分类	免费版	基础版	企业版	备注
价格 (元/月)	0	340	550	
终端数 (个/月)	10	10	10	免费版不支持增 加终端数
防护流量规格: (GB/ 月)	100	500 或者 5Mbps	800 或者 10Mbps	免费版不支持扩 展流量或者带宽
内网访问	\checkmark	\checkmark	\checkmark	
桌面终端	\checkmark	\checkmark	\checkmark	
IAM 权限控制	\checkmark	\checkmark	\checkmark	
日志审计	×	\checkmark	\checkmark	
双因子认证	×	\checkmark	\checkmark	
监控告警	×	\checkmark	\checkmark	
行为管理	×	×	\checkmark	
精细粒度访问控制	×	×	\checkmark	
双因子认证	×	×	\checkmark	
信任评分	x	×		
终端检测	×	×	\checkmark	

1.2 术语解释

1.2.1 CNAME 记录

CNAME (Canonical Name),即别名,用于把一个域名解析到另一个域名,当 DNS 系统在查询 CNAME 左面的名称的时候,都会转向 CNAME 右面的名称再进行查询,一直追踪到最后的 PTR 或 A 名称,成功查询后才会做出回应,否则失败。例如,您有一台服务器,使用 docs.example.com 访 问,您又希望通过 documents.example.com 也能访问该服务器,那么就需要在您的 DNS 解析服务 商添加一条 CNAME 记录,将 documents.example.com 指向 docs.example.com,添加该条 CNAME 记录后,所有访问 documents.example.com 的请求都会被转到 docs.example.com,获 得相同的内容。

1.2.2 DNS

DNS 即 Domain Name System,是域名解析服务的意思。它在互联网的作用是:把域名转换成为网络可以识别的 ip 地址。人们习惯记忆域名,但机器间互相只认 IP 地址,域名与 IP 地址之间是——对应的,它们之间的转换工作称为域名解析,域名解析需要由专门的域名解析服务器来完成,整个过程是自动进行的。比如:上网时输入的 www.baidu.com 会自动转换成为 220.181.112.143。

常见的 DNS 解析服务商有: 阿里云解析, 万网解析, DNSPod, 新网解析, Route53 (AWS), Dyn, Cloudflare 等。

1.2.3 边缘安全节点

边缘安全节点是相对于网络的复杂结构而提出的一个概念,指距离最终用户接入具有较少的中间环节 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。其作用是将访问量较大的网页内容和对 象保存在服务器前端的专用 Cache 设备上,以此来提高网站访问的速度和质量。

1.2.4 回源 HOST

回源 host 决定回源请求访问到源站上的具体某个站点。

例1:源站是域名源站为 www.a.com,回源 host 为 www.b.com,那么实际回源是请求到 www.a.com 解析到的 IP,对应的主机上的站点 www.b.com。

例 2: 源站是 IP 源站为 1.1.1.1,回源 host 为 www.b.com,那么实际回源的是 1.1.1.1 对应的主机 上的站点 www.b.com。

1.2.5 协议回源

协议回源指回源时使用的协议和客户端访问资源时的协议保持一致,即如果客户端使用 HTTPS 方式 请求资源,当 CDN 节点上未缓存该资源时,节点会使用相同的 HTTPS 方式回源获取资源;同理如 果客户端使用 HTTP 协议的请求,CDN 节点回源时也使用 HTTP 协议。

1.2.6 过滤参数

过滤参数是指当 URL 请求中带"?"并携带参数请求到 CDN 节点的时候, CDN 节点在收到该请求 后可根据配置决定是否将该带参数的 URL 请求回源站。当开启过滤参数时, 该请求到 CDN 节点后会 截取到没有参数的 URL 向源站请求。并且 CDN 节点仅保留一份副本。如果关闭该功能, 则每个不同 的 URL 都缓存不同的副本在 CDN 的节点上。

示例:

客户端发起请求"http://www.test.com/a.jpg?x=1"到 CDN 节点 开启"过滤参数"功能: CDN 节点收到客户端请求后, 向源站发起请求为: "http://www.test.com/a.jpg"(忽略参数 x=1), 待源站响应"http://www.test.com/a.jpg"请求指向的内容、且 CDN 节点获取到该内容后, CDN 节点保留一份所获取内容的副本, 然后向终端返回该内容。此后, 在该内容副本的有效期内, 客户端 所 有 类 似 " http://www.test.com/a.jpg? 参 数 " 的 请 求 , CDN 节 点 均 返 回 存 储 的 "http://www.test.com/a.jpg"副本。

关闭"过滤参数"功能:

对于所有类似"http://www.test.com/a.jpg?参数"的请求,每个不同的URL都缓存不同的副本在 CDN的节点上。例如:"http://www.test.com/a.jpg?x=1"和"http://www.test.com/a.jpg?x=2" 会缓存两份副本,根据源站返回的内容,这两份副本可能相同,也可能不同。

1.2.7 Web 安全

相关 Web 应用层面的安全问题与事件,包括各种 Web 组件、协议、应用等。

1.2.8 正则防护

经验规则集,自动为网站防御 SQL 注入、XSS 跨站、Webshell 上传、命令注入、后门隔离、非法文件请求、路径穿越、常见应用漏洞攻击等通用的 Web 攻击。

1.2.9 网站白名单

通过设置网站白名单,可以让满足条件的请求不经过任何边缘安全加速平台—安全与加速服务防护模块的检测,直接访问源站服务器。

1.2.10 IP 黑名单

支持一键阻断来自指定 IP 地址、IP 地址段以及指定地理区域的 IP 地址的访问请求。

1.2.11 Oday 漏洞

0Day 是指在系统商在知晓并发布相关补丁前就被掌握或者公开的漏洞信息。

1.2.12 CC 安全防护

根据访问者的 URL,频率、行为等访问特征,智能识别 CC 攻击,迅速识别 CC 攻击并进行拦截,在 大规模 CC 攻击时可以避免源站资源耗尽,保证企业网站的正常访问。

1.2.13 防敏感信息泄露

帮助网站过滤服务器返回内容(异常页面或关键字)中的敏感信息(例如身份证号、银行卡号、电话 号码和敏感词汇),脱敏展示敏感信息或返回默认异常响应页面。

1.2.14 网络爬虫

又称为网页蜘蛛,网络机器人,是一种按照一定的规则,自动地抓取万维网信息的程序或者脚本。

1.2.15 挖矿

借助大量计算能力来计算产生虚拟货币。

1.2.16 零信任

一组围绕资源访问控制的安全策略、技术与过程的统称。从对访问主体的不信任开始,通过持续的身份鉴别和监测评估、最小权限原则等,动态调整访问策略和权限,实施精细化的访问控制和安全防护。

1.2.17 策略引擎

负责最终决定是否授予指定访问主体对资源(访问客体)的访问权限。策略引擎使用企业安全策略以 及来自外部源的输入作为"信任算法"的输入,以决定授予或拒绝对该资源的访问。

1.2.18 TCP 协议

TCP 协议指传输控制协议(Transmission Control Protocol),是一种面向连接的、可靠 的、基于 字节流的传输层通信协议,由 IETF 的 RFC 793 定义。TCP 工作在网络 OSI 的七 层模型中的第四层 (传输层),连接到不同但互连的计算机通信网络的主计算机中的成对 进程之间依靠 TCP 提供可靠 的通信服务。

1.2.19 UDP 协议

Internet 协议集支持一个无连接的传输协议,该协议称为用户数据包协议(UDP, User Datagram Protocol)。UDP为应用程序提供了一种无需建立连接就可以发送封装的 IP 数据包的方法。RFC 768 描述了 UDP。 6 Internet 的传输层有两个主要协议,互为补充。无连接的是 UDP,它除了给应用程序发送 数据包功能并允许它们在所需的层次上架构自己的协议之外,几乎没有做什么特别的事情。面向连接的是 TCP,该协议几乎做了所有的事情。

1.2.20 无服务器 Serverless

无服务器是一种云原生开发模型,可使开发人员专注构建和运行应用,而无需管理服务器。无服务器 方案中仍然有服务器,但它们已从应用开发中抽离了出来。云提供商负责置备、维护和扩展服务器基 础架构等例行工作。开发人员可以简单地将代码打包到容器中进行部署。部署之后,无服务器应用即 可响应需求,并根据需要自动扩容。公共云提供商的无服务器产品通常通过一种事件驱动执行模型来 按需计量。因此,当无服务器功能闲置时,不会产生费用。

1.2.21 函数即服务 FaaS

函数即服务 (FaaS: Function as a service) 是一种事件驱动计算执行模型;开发人员编写代码逻辑, 部署到完全由平台管理的函数运行时中,然后按需执行。与 BaaS 不同,FaaS 可让开发人员拥有更 大的掌控权力,他们可以创建自定义应用,而不依赖于包含预编写服务的库。代码则部署到边缘安全 加速平台管理的容器运行时中。具体而言,这些函数运行时具有以下特点:

- (1) 无状态 让数据集成变得更加简单。
- (2) 运行周期短 可以只运行非常短的时间。
- (3) 事件触发 可在需要时自动运行。

这样,您只用为所需的计算能力付费,而不必管"闲置"的应用和服务器。 使用 FaaS 时,开发人员可以通过触发器调用无服务器应用。

1.2.22 触发器

用户绑定触发器和对应函数,来实现多种调用效果。目前支持定时触发器以及 HTTP 触发器

1.2.23 HTTP 路由

用户绑定 HTTP 触发器和对应函数后,访问安全与加速服务中托管域名的特定路由,即可在边缘节点 调用起对应函数计算逻辑。

1.2.24 KV 存储

OmniKV 边缘存储提供了 Key-Value 型边缘存储服务,使开发人员能够构建低时延、频 繁读取、不频繁写入的数据驱动的边缘无服务器应用程序。借助 OmniKV,无服务器应 用程序可以将数据存放在靠近用户的位置,避免从云端或本地解决方案中检索信息的需 要,从而实现快速响应。用户快速可以构建高度动态的 API 和网站服务,部署轻量型的 API 网关、BaaS 服务。

1.2.25 运行时

用于在边缘节点运行用户自定义函数的安全隔离环境。函数运行时所支持的编程语言,目前支持 JavaScript 和 Lua

1.2.26 开发者工具

开发人员使用命令行工具,在本地完成函数编写,构建,灰度上线。

1.3 产品优势

1.3.1 极致的加速体验

优质的资源覆盖: CN2 和 163 互备支撑,所有节点和 IDC 出口并行,避免峰值带宽拥堵

动静分离,智能高效:智能分离动静态内容,静态内容就近缓存分发,动态内容 AI 选路传 输回 源。

传输优化:基于先进的内核技术及自研的私有协议,大幅提升传输效率。

多业务加速: 支持 http/https 协议加速、上传加速、websocket 加速、IPv6 升级等。

1.3.2 一体化平台构筑 3-7 层立体防护

DDoS 防护:检测和清洗 DDoS 攻击流量,提供 Tbps 级防护能力 结合云原生、智能调度能力,实现资源动态扩容,满足用户三网防护需求,保障业务可用性

WEB 安全防护:基于 AI+ 规则的 Web 攻击识别,有效防御 SQL 注入、XSS 跨站脚本攻击等 OWASP TOP 10 的关键 WEB 风险

bot 管理:基于已知 Bot 情报、精准访问控制、客户端特性识别、人机交互验证、机器学习等智能识别与检测技术,对业务流量进行实时检测和分析,智能识别并区分真实用户流量与各类 Bot 流量

API 安全防护:基于安全可靠的接入认证方式,保证 API 访问安全。

持续认证动态评估:

持续认证过程引入 RBAC(基于角色的访问控制)与 ABAC(基于属性的访问控制)鉴权体系, 能根据角色及用户属性、环境属性、资源属性等综合授予用户访问权限

全周期安全保护:

基于可信授权、最小授权、持续认证、业务隐身、终端安全、应用安全、链路安全等核心能力, 对访问过程进行持续的安全保护,实现在任意网络环境中安全访问企业资源

1.3.3 多分支地办公统一管控

为具备多分支、居家移动办公场景的企业提供开箱即用的安全服务,通过连接器反向访问企业内 部应用,达到业务和端口隐身的目的,同时叠加全方位的安全能力,保护企业业务和数据安全, 实现企业办公安全统一管控。

1.3.4 完善的售后服务

集中监控和分散维护相结合,NOC工程师 7×24 小时集中监控,网络工程师 7×24 小时在线支 持,所有节点都有现场服务工程师进行服务保障。

1.3.5 极简的运维部署

零部署、零运维,使用 CNAME 接入,云端安全专家配置策略

支持一键开启 IPv6 功能,无缝处理 IPv4 和 IPv6 流量,并且解决天窗问题和支持全站二级,三

级外链替换。

聚焦业务逻辑,无需关心非功能开发,免运维,实现业务的快速试错和验证

1.3.6 灵活的售卖机制

可根据需要选择不同的服务、套餐和扩展服务计费产品,费用透明,可控,灵活。

1.3.7 冷热启动低时延

使用超轻量级的函数安全沙箱,冷热启动只需要 5-10ms

1.4 功能特性

1.4.1 安全与加速

智能加速

通过动静分离、多级缓存、智能路由、协议优化、链路优化等多项技术实现静态内容的就近 交付及动态内容的快速回源,从而解决因网络拥堵、链路抖动、流量突增等因素导致的响应 慢问题,显著提升源站性能。适用于纯动态加速、动静态一体化的站点加速、上传加速、 websocket 加速、IPv6 升级等场景。

DDoS 防护

采用的是分布式架构,将防护能力赋能于更下沉的边缘节点,使用云原生为内核,结合智能 调度,可以实现边缘就近清洗,动态扩容,可以满足业务突发、大规模流量攻击。

Web 防护

依托天翼云的云安全节点形成云安全网络,结合云端大数据分析平台,为用户提供应对 Web 攻击、入侵、漏洞利用、挂马、篡改、后门、爬虫、域名劫持等防护,特有的 AI 引擎融合 威胁情报,打造更聪明的威胁识别大脑,精准有效拦截 Web 威胁。

BOT 行为管理

提供 BOT 管理防护方案,协助客户积极管控肆虐的 BOT 流量,对抗 BOT 流量背后的黑灰产 产业链,保护客户的正常流量,缓解大量针对网站的爬取和异常注册登录行为。 高级访问控制 可针对 IP,IP 段,URI,CI,METHOD,请求地区,请求参数,请求头部,请求协议进行组合, 设置白名单和黑名单,对请求进行拦截和放行,保证客户网站不受未知访问。 高级频率控制 通过配置 IP,URL,ARGS,HEADER,COOKIE,UA,CI 等粒度,进行访问次数限制,防止客户资源被

CC 防护

过度消耗。

针对异常请求配置 CC 阈值防护,当达到指定限制访问次数后,进行人机识别,防止非正常 用户访问网站,造成网站资源耗尽。

IPV6 防护

支持一键开启 IPv6 功能,无缝处理 IPv4 和 IPv6 流量,并且解决天窗问题和支持全站二级, 三级外链替换。

1.4.2 零信任服务

统一身份管理,便捷接入

统一认证和身份管理、集中进行业务管控、为企业带来全面的审计能力。

支持客户通过平台对其组织架构信息进行管理,支持对用户信息进行添加、删除、修改、禁 用等操作,通过用户数据统一管理,授权可信用户范围。

支持不同身份源接入和管理,支持自定义身份源接入,批量导入组织架构账号信息,快速开 启企业内员工用户便捷接入零信任服务。

支持企业微信身份源接入,建立零信任服务平台与企业微信的连接。

支持标准的 SCIM 身份协议进行企业用户组织架构接入,确保可信用户实时生效。

零信任安全访问

零信任策略:基于身份与设备的精细粒度授权管理,支持配置客户端用户可访问资源,支持 按组织架构和用户粒度进行授权,结合多源策略评估引擎,持续认证,动态授权,为企业带 来高可控安全服务。降低社会面攻击风险,为数据提供最高级别的保护,同时为授权用户带 来安全快速的系统访问体验。

资源管理: 支持对接入零信任服务的网络资源进行管理, 包括对 IP 类资源和域名类资源的 增加、删除、修改操作, 通过对应操作, 可调整零信任服务对客户端提供的可访问资源内容, 为企业访问内网业务提供支撑。简单快捷的资源管理, 便于企业实时对业务进行监控, 动态 调整对外服务内容。

智能选路、加密传输

使用加密隧道与零信任网络建立连接,通过加密隧道进行数据传输,有效防范中间人攻击和 数据泄露风险。基于天翼云覆盖全国的边缘节点、可编排的安全原子能力、智能 DNS 选路, 为用户提供安全、可信、快速的网络服务。通过天翼云全网资源,为用户提供就近接入点, 为企业带来近似专线网络的安全加密通信,结合天翼云智能网络加速,择优选取回源链路, 降低网络传输时延,保障企业服务。

1.4.3 边缘接入服务

传输优化

链路优化:长连接保持、链路复用,节省三次握手时间,提升访问效果。

内容优化:通过智能压缩技术,优化传输内容,提升传输效率。

协议优化:使用自研的可靠 UDP 传输协议代替传统 TCP 和 UDP 协议,提升传输效率。

可靠传输

多点覆盖:边缘节点采用多点覆盖,避免单节点故障造成访问故 障,提高可靠性。 零时延切换:当边缘节点与下一跳节点建连时,若发现下一跳节点 故障时,零时延切换到 其他回源链路去。

TCP/UDP 加速

支持基于 TCP/UDP 协议的所有应用, 甚至私有协议的应用加速。

HTTPS 无证书加速

HTTPS 协议,无需部署证书,即可实现加速,保证数据安全不被篡改。

1.4.4 开发者平台

易上手的开发者工具

为开发者提供CLI和Web IDE。CLI提供函数全生命周期管理功能,可以和开发者已有的 CI/CD 流程进行集成。Web IDE 提供了一站式、全流程的函数管理与在线开发平台,帮助开发者专注于业务代码,提高开发效率。

丰富的编程语言生态

支持 JavaScript ECMAScript 6,支持 TypeScript。支持 Node.js 的生态,可直接使用 Node.js 部分代码库,扩展性强。目前支持 WebAssembly,后续扩展支持 go/python 和全球 KV 存储。符合 W3C 标准的 API

提供符合 W3C 标准的 Service Worker API、Streams API、WebCrypto API, 支持常用主流加 解密算法,可以方便地实现边缘自定义访问控制、边缘内容改写和边缘内容生成等功能。

1.5 应用场景

1.5.1 政企网站

客户特点: 政企行业的门户网站作为政府、企业的互联网信息服务的重要渠道, 有着很重要的作

用,要求网站需要保证稳定的运行。

客户需求:

- 1) 大型会议、特殊时期重保。
- 2) 防止被黑、被挂马、篡改等安全事件发生。
- 3) 用户、公民敏感信息不能被窃取。

产品优势:

1.丰富的资源覆盖。

2.国内拥有丰富的节点覆盖承载能力,覆盖多运营商、主要省份和城市无盲点。

3.加速节点可根据需求随时增加,致力于客户的发展壮大。

1.5.2 金融网站

客户特点:业务系统对业务可用性要求非常高,同时需要保障用户个人数据和资金安全,一旦发 生安全问题,也可能会引发投资人恐慌,对公司造成很大的影响。

客户需求:

13

1) 官网、信用卡中心等业务稳定加速运行。

2) 纪念币等发行时突发流量应对。

3) 攻防演练、护网行动保障。

4) 恶意 DDoS 攻击防护,无俱黑客勒索。

5) 防撞库、暴力破解等。

产品优势:

1.可靠的安全防护。

2.分布式集群防护, 单点故障自动转移, 确保网站的高可用性。

3.利用大平台优势,基于全网、全行业流量的攻击数据,结合机器学习算法,构建一套智能防护 体系。

4.精准防护,域名粒度的防护策略,结合客户自身业务定制化防护策略。

1.5.3 电子商务网站

客户特点: 业务对用户体验实时性要求较高, 并且存在用户个人账号信息被盗、敏感信息泄露等

问题,若存在可用性或者安全问题会造成交易问题,流失客户。

客户需求:

1) 业务可用性稳定性保障。

2) 营销活动减少业务欺诈。

3) 用户信息、订单等数据不被窃取。

产品优势:

1.特色的安全防护。

2.敏感信息回显脱敏,保护用的身份证号、手机号和卡号等敏感信息。

3.撞库攻击防护,防止网站撞库攻击,保护网站用户数据安全。

4.恶意挖矿防护, 识别 js 挖矿脚本, 避免访问网站的用户被利用成"挖矿机"。

5.客户端防广告,移除客户端被插入的广告,保护内容安全。

1.5.4 全球办公加速防护

业务特点

疫情快速推动远程/协同办公模式的普及,既存在静态文件的分享,也多人协作编辑、实时沟通 等各类动态数据的传输,其中文件下载过久,沟通延时等问题大大降低了协同办公的效率。而传 统 vpn、专线等的接入方式,只要接入就能访问所有系统,可能造成客户业务核心数据泄漏、病 毒感染等安全事件的发生。

客户痛点

1.远程办公应用登录超时、业务系统响应慢、音视频会议卡顿、延迟以及 vpn 超时、掉线

2.准入安全风险、远程终端造成病毒扩散、终端越权访问、违规操作风险

产品价值

1.智能调度、实时探测最佳路径,私有传输协议,解决网络抖动问题,提升办公效率。

2.全球节点覆盖,就近接入,保障网络的快速和稳定性,提升用户体验

3.任意区域任意网络接入,安全边缘节点,通过加密隧道保证数据安全及隐私

4.多因素认证身份,持续性安全评估,支持指定哪些用户使用什么样的终端设备访问哪些办公应 用,保证可信访问

5.一体化办公安全访问管控,精准识别并阻断钓鱼,C2 外链等攻击行为

2 计费说明

2.1 计费项

计费项	计费说明
套餐	按需购买不同规格套餐获得相应标准的安全与加速服务,具体请见 <u>边缘安全加速平台计费模式</u> 。
扩展服 务	如有带宽扩展、域名扩展需求,可购买相应扩展服务,具体 计费请参考 <u>边缘安全加速平台计费模式</u> 。

2.2 计费模式

2.2.1 安全与加速服务

计费模式:包周期、按需

【计费项说明】

计费方式	描述	说明
套餐计费	按照购买的套餐使用量 进行计费。	套餐为预付费
扩展服务	根据购买的功能进行计 费	扩展服务的有效期与套餐服务有效 期一致,套餐服务失效,扩展产品 自动关停

套餐含安全保底流量或者业务带宽峰值、接入域名数等,按月付费。如果保底业务带宽峰

值不能满足需求,可以购扩展带宽,当带宽超出购买套餐+扩展带宽时,会进行域名限速。

计费项:国内

计费周期:按月结算

1、套餐计费

套餐标准资费

套餐规格	标准资费(月)	套餐主要内容
高级版	3800	流量:1TB/带宽:100Mbps (流量带宽二选一);DDoS 防护:40Gbps/月 (防护 2 次); 域名数:1 个域名
企业版	9800	流量:2TB/带宽:150Mbps (流量带宽二选一);DDoS 防护:无限防(防护2次); 域名数:2 个域名
旗舰版	83660	流量:5TB/带宽:300Mbps (流量带宽二选一);DDoS 防护:无限防(不限次数); 域名数:3个域名

2、扩展服务计费

扩展计费标准资费

扩展服务	标准资费 (月)	功能描述
流量	资源包:100G:17 元 按需:0.18 元/GB	实际流量超过了产品套餐支持的流 量,可通过购买资源包或者按需扩 展
带宽扩展 包	18元/Mbps/月	实际业务带宽超过了产品套餐支持 的带宽,可通过购买带宽扩展
动态请求 数	资源包:100 万次:13 元 按需:0.15 元/万次	开启动态能力收取
域名扩展	1000 元/域名(一个一级	支持一个主域名

包	域名)	
DDos 防护 次数	0Gbps<攻击量≤ 20Gbps, 1000 元/次 20Gbps<攻击量≤ 80Gbps, 4660 元/次 80Gbps<攻击量≤ 150Gbps, 12060 元/次 150Gbps<攻击量, 20160 元/次	实际攻击次数超过了产品套餐支持 的 DDos 防护次数,可通过购买 DDos 防护次数购买
IPv6 外链 改造	600 元/月	IPv6 外链改造,解决天窗问题
内容审核	1.3 元/千张/日	对加速内容进行快速智能检测
高级 bot 管理	3500 元/月	提供针对自动化攻击/Bot 流量的智 能防护方案
API 安全	13500 元/月	提供 API 资产高可见性和 持续安全 检测
态势感知 大屏	1500 元/月	提供网站整体业务及安全状况的可 视化大屏分析
专家服务	10000 元/月	7*24 安全值守服务;接入域名评估 与加固指导;定制防护方案

2.2.2 零信任服务

计费模式:混合计费

【计费项说明】

计费方式	描述	说明
套餐计费	按照购买的套餐使用量进行计 费。	套餐为预付费
扩展服务	根据购买的功能进行计费	扩展服务的有效期与套餐服务有效期一致, 套 餐服务失效, 扩展产品自动关停

套餐含保底流量或者业务带宽,保底终端数等,按月付费。如果保底用量不能满足需求,可以购 扩展服务,当用量超出购买套餐+扩展服务时,会进行服务限制。

计费项: 国内

计费周期:按月结算

1、套餐计费

套餐标准资费

套餐规格	标准资费 (月)	套餐主要内容	备注
免费版	0	终端数:10 防护流量规格:100GB/月 产品功能:内网访问、桌面终端、 IAM 权限控制	不支持增加终端数和扩展流 量或者带宽
基础版	340	终端数:10 防护流量规格:500GB/月或者 5Mbps 产品功能:内网访问、桌面终端、 IAM 权限控制、日志审计、双因 子认证、监控告警	
企业版	550	终端数:10 防护流量规格:800GB/月或者 10Mbps 产品功能:内网访问、桌面终端、 IAM 权限控制、日志审计、双因 子认证、监控告警、行为管理、 精细粒度访问控制、双因子认 证、信任评分、终端检测	

2、扩展服务计费

扩展计费标准资费

扩展服务	标准资费 (月)	功能描述
流量	资源包:100G:17 元 按需:0.18 元/GB	实际业务流量超过了产品套餐支持的流量, 可通过购买资源包或者按需扩展
带宽扩展包	18 元/Mbps/月	实际业务带宽超过了产品套餐支持的带宽, 可通过购买
终端扩展	基础版:34 元/终端/月 企业版:55 元/终端/月	基础版每个终端防护流量为 50GB/月或 1Mbps 高级版每个终端防护流量为 80GB/月或 2Mbps

3.操作指导

3.1 购买安全与加速服务

3.1.1 开通边缘安全加速平台

开通天翼云边缘安全加速平台—安全与加速服务服务,需首先注册天翼云账户。

开通步骤如下:

步骤 1、注册并登录天翼云 <u>http://www.ctyun.cn</u>

2-1 天翼云官网登录页面



热门产品分类

步骤 2、未实名认证的用户请按提示完成实名认证才能开通服务

2-2 实名认证提醒

温馨提示 ×
尊敬的客户,您好: 《中华人民共和国网络安全法》第二十四条规定:网络运营者为用户办理网络接入、域 名注册服务,办理固定电话、移动电话等入网手续,或者为用户提供信息发布、即时通讯等 服务,在与用户签订协议或者确认提供服务时,应当要求用户提供真实身份信息。用户不提 供真实身份信息的,网络运营者不得为其提供相关服务。 为保证您天翼云服务的正常使用,请您尽快完成实名认证,感谢您对天翼云的理解支 持,谢谢。
取消 确认

实名请超链接:

2-3 完成实名认证



步骤 3、实名认证后进入边缘安全加速平台—安全与加速服务产品详情页快速了解产品,之后单

击【立即开通】;

2-4 产品详情页

边缘安全加速平台	
边缘安全加速平台-依托全国局地的分布式边缘资源并基于边缘云观主;利用云原生技术实现局档 起、安全、其方原于能力期间融入统一网络;多终线、多仲仪(SGL3U4U7等)加中-one的网 入;目睑化服务、运营管理与分析、可很化报表与分析考集中化的统一管理平台;展远不同场展	現成が性 発統-地 葉字的
<u>∽2007778</u> 税助交幣 >	
A STAR	2982 2081 实际台湾和国新名头(MODOSIX:街、通明电量的);重调电超力 2983 为用户理例应对 Web 攻击路护 2985 按用户理例应对 Web 攻击路护 2985 透明 Heb 收击路护

步骤 4、在购买页面选择适合的套餐和扩展服务,勾选并阅读服务协议,确认无误后点击"立即

开通",边缘安全加速平台—安全与加速服务服务即开通;

2-5 产品开通页

	Ĩ	国家 Q 当前工作区:网站安全… V 个人中ら 😡
	▲ 套發开通	产品纳制 产品文地 产品环境
₿	安全与加速 零	信任服务 边缘地入服务 开发表平台
æ	基本信息	
6	计费模式	流量计费 月带效峰值计费
	使用范围	围府
	套餐范围	免费版 高级版 企业版 旗組版
R		道用场景: 中小股业务网站加速与标准防护
2	充裕详情	
۲	站点加速	
۲	一级域名数量	1个
8	洗量	178
69	静态加速	转变
~	动态加速	转变
w		开信动态加速机,动态速来观技能计量:0.15元方次,月底出版。也可以 <mark>购买动态速来做-金融也</mark>
100	IPV6(J)[0]:	又符 #01/f03##f02f4a
8	QUIC	anoantrin vii 如

步骤 5、边缘安全加速平台—安全与加速服务服务开通后,便可以根据操作手册去控制台开始接

入您要防护的域名。

3.1.2 续订

支持续订操作,登录官网订单管理-产品-产品视图-产品续订,提交您的续订需求,续订规则详见如下链接:

https://www.ctyun.cn/document/10000038/10303747

G	大翼云 拉制	中心							Q 11	塐		费用 :	C单 备案	支持	合作	∭ *	1	7 0	<mark>.72</mark>			
88	费用中心		续订管	曜 /	手动续订													3	资源被锁定@			
() () ()	总页 订单管理				产品名称		资源ID			资源池	资源状态	5 倒计时	十 续订周	期时	8)			操作后线	卖订周期			
0	我的订单 待支付订单	订单 付订单					Ŷ	边缘安全加 任	速平台-零信	549e03fc2a0	04c2a970b74	8d06e516df		在用	366 天		6	创建:2023-0: 到期:2024-0:	3-15 09:19: 3-15 09:19:	17 12	3个月	
⊗ Għ ⊗	续订管理 进订管理			边缘9 -	史全加速平台-	零信任																
	资金管理	٠	•																			
	撤单管理账单管理	÷	续订	周期	1个月	2个月	〇 3个月	4个月	5个月	6个月	7个月	8个月	9个月	10个月	11个月	1	1年	2年	3年			
	产品视图	•												续	订金額:			¥ 1,0	20.00			
	发票管理															đ	能定提交		取消			
	合同管理																提示: 最	终费用以计	费出账为准			
	成本管理	٠																				
	卡券管理	٠																				
	按需试用																					

3.1.3 变更

您如果有变更套餐的需求,您可以登录天翼云官网,在订单管理-产品中找到您的订单,点

击"订购"提交您的变更需求。目前套餐变更只支持升级套餐,不支持降级套餐的操作。

套 餐修改	74016 74275 7427
零信任服务	
基本信息	
计费模式	2. 这些计会 月前回时后过会
使用范围	804
套板范围	9.000 HA200 C-900
	道用经囊: 适用于大型集团企业多分支办公安全访问及定制化就扩展务
套餐洋情	
终端数: 1	40
	上這些會範疇做交到10个作職。與出版分析網路內或會
防护范围现格:8	0008/3
内网访问:	238
桌面终端: 3	236
IAMEQIR控制: 3	· · · · · · · · · · · · · · · · · · ·
日志审计: 5	結
双因子认证: 3	Sin-
助投告警: 3	Signal Sector Sect
行为管理: 3	559
精细粒度访问控制: う	
信任评分: 3	
1986238	219
8.01	※3162.08 (時間) 前後回復

3.1.4 退订

产品支持退订服务,登录官网-订单管理-产品-产品视图-退订管理,找到您要退订的订单,

进行退订;客户套餐退订后,扩展服务也会一起退订

产品退订页面

G	大翼云	控制中心	2				Q 搜索		9	ŧĦ	工単	备案	支持	合作	测*	11	Ä	0	. <mark>73</mark> ;;;;
	费用中心			4、退订可言 退订规则请 您还可以进	E会导致其他存在的关 查看:追订规则说明 行 0 次七天无理由退	E联业务产生影响。 款													
	总宽 订单管理																		
62	#407M			ŕ	品名称	资源ID		资源池	资源状态	时间	8)			产品会	额		可退订	金额	
© [>]	我的订单	单		~ 送	边缘安全加速平台	ba0661e633f9460ab5087	0a3283602f1		在用	© 食 © 至	刻建:2023- 利期:2024-	03-14 15: 06-14 15:	41:05 41:01	744,66	3.78 元		741,411.	79 元	
ර බ	续订管理 退订管理			边缘安全)	加速平台				边缘安全与加速	-DDOS®	防护								
~	资金管理		•	边缘安全	与加速-Bot管理														
	撤单管理			•															
	账单管理		*																
	产品视图		•	* 请选择退订	原因:										ĩ	*品金	颐:¥7	44,663.	78 元
	发票管理			● 购买云服:	务时选错参数(配	置、时长、台数等)								退订	金額:	¥74	1.41	1.79	元
	合同管理			○ 云服务功能	能不完善,不满足	业务需求									275-07 <u>8</u> 8-9				
	成本管理		Ŧ	 其他云服: 区域选择: 	务商的性价比更高 错误								1	8口确计本	步调订 全	- 207 - En ±	日光弗田	1 赤香)	¥ 400
	卡券管理		Ŧ	○ 云服务故(障无法修复								1	2日期以4	A RE LI Z	1984H 1	нхын		£18
	按需试用			○ 其他												退订		取消	

3.2 服务概览

简介

边缘安全加速平台服务整体概览页,供您快速查看整体情况,含加速及安全服务数据,服务拓扑,

服务订阅,服务推荐。

操作步骤

步骤一:进入边缘安全加速平台控制台

步骤二:在左侧导航栏,单击服务概览



1、基础数据模块中,展示接入终端、接入域名、业务流量、请求数、攻击事件数

接入终端:如果订购了零信任服务,则会展示零信任用户数

接入域名:显示域名管理中域名个数(包括主域名+子域名)

业务流量:显示所有接入域名的今天的总流量

请求数:显示所有接入域名的今天的总请求数

攻击事件数:显示所有 DDos 和 CC 攻击事件数

2、服务订阅模块中,展示用户套餐订购以及实际扩展服务开通个数

3、服务推荐模块中,展示用户订购和未订购的服务,

未开通服务:单击【免费试用】按钮,跳转到对应服务的服务订购页面。

已开通服务:单击【套餐升级】按钮,跳转到对应服务的套餐升级页面。

3.3 安全与加速

3.3.1 域名管理

功能简介

可在【域名管理】中查看域名列表,域名列表已添加域名的的基本信息,包括域名、CNAME、 套餐类型、状态、创建时间、操作、全局防护模式。

详情:查看和编辑该域名的域名配置;

停用:停止该域名的解析,停止加速和安全防护;

启用:开启该域名的解析,开始加速服务;

删除:在域名列表中删除该域名;

1、当域名状态为【已启用】时,可以对域名配置进行【详情】、【停用】操作;

2、当域名状态为【配置中】时,可以对域名配置进行【详情】操作,但是不能编辑配置;

3、当域名状态为【已停用】时,可以对域名配置进行【详情】、【启用】和【删除】操作;

	▲ > 安全与加速 > 城名管理							
AccessOne	域名管理 展示已自用和已停用的域名。新造域名、自用域名、停用域名、	后要配置.						Janet s
○ 服务概范								
只要全与加速 ~		CNAME	教史家田	加速防衛	好去		01589±(iii)	
概范	and second	C. C. C. C.	PRA	And Association	000	10000 000 0	1000mm121-0	
域名管理	1		企业版		配置中)的30年 ~	2023-03-14 14:23:10	评情 1899
证书管理	2		企业版		配置中	(#3)年 ·	2023-03-13 14:58:03	itin BPs
安全报表	3		企业版		配置中	90359 v	2023-03-13 10:12:47	1710 B29
站庶統计 🗸	4		企业版		配置中	101539 v	2023-03-10 15:40:51	1710 200
刷新预取	5	m	企业版	中国内地	已启用	1933年 ~	2023-03-10 14:58:58	1416 1578 BD4
◎ 零倍任服务 ~	6		企业版	中国内地	已启用	·请选择 ~	2023-03-10 14:13:09	1748 1948 1846
 E、开发者+6 回 运营管理 	7		企业版	中国内地	已启用	通法応 >	2023-03-06 23:28:32	洋橋 停用 1883
③ 计费详情	8	in	企业版	中国内地	已启用	清选择 >>	2023-03-07 20:33:40	248 578 894
	9		企业版		配置中	983598 ~	2023-03-03 18:46:08	(21) 200

3.3.1.1 新增域名

简介

使用 安全与加速服务前,需要先将网站接入到 安全与加速服务。未完成接入前,您的 加速 和安全防护功能将无法生效。本文档将指导您如何在控制台中接入域名。

操作步骤

步骤一: 进入边缘安全加速平台控制台

- 1、打开天翼云官网 http://www.ctyun.cn, 注册并登录;
- 2、选择控制中心;



3、下拉选择 CDN 产品,点击对应的边缘安全加速平台服务进入客户控制台;

步骤二:添加域名

1、选择安全与加速—域名管理,点击【添加域名】;

2、填写网站信息,

根据页面的引导填写域名的基本信息和源站设置;

力總成合加速率会	ᢙ > 安全与加速 > 域名管理 > 添加站点		
AccessOre	添加站点		
💮 服务概范			
○ 安全与加速	编写网站信息	选择网站安全配置	18 ALCERCE
概范			
域名管理	基本信息		
证书管理	* 加速域名: 加速的域名进先完成在中国大陆的ICP醫業,同时先成公安與醫業。支持泛或名活	加、城名不支持大号字母。	
安全报表	ipv6开关: 停甩 🔵 🖩 問		
站点统计 ^	海北沿海		
用量直询	· #4	* ~	
热门分析	+ 4000,0000		
用户分析	支持PR就被击。最多可该ID60个		
周新预取	*回译协议: HTTP HTTPS 原题		
🖳 零信任服务 🖂	目前设HTTP协议回避支持自定义属口。HTTPS协议回避使用443高口、跟随选举	的心思選擇得指描述未用這的的心思選到認識這的認識443篇[]	
🖳 开发者平台 🗸	* 2934006日: * http 80		
① 计费详慎			纲写安全配置

配置项说明:

加速域名:填写需要加速和安全防护的域名;域名会进行域名归属权校验,

域谷	3归属权校验			×
域客	名【example.com】需要罚 户工单。	完成归属权验证,您可以通过D	NNS解析验证或文件验证,若操作失败请 <mark>前往客開</mark>	武工单系统 提
DN	S解析验证 文件验	述		
1、	请在您的域名DNS服务	商添加以下TXT记录【验)	正操作指南】	
	记录类型	主机记录	记录值	
	ТХТ	dnsverify	202212061412098d2a 15a19fc84b3e827ac9d ade5d1bcf716633bab 5c44f3bae	
2、	等待TXT解析生成。			
3、	单击下方按钮进行验证	Ę		
	验证 验证结果: <mark>待验证</mark>			

IPv6 开关:开启 IPv6,开启后完成 IPV6 改造,如果要解决 ipv6 天窗问题(提升二、三级链接 ipv6 支持度),需要在【站点配置】中配置外链改造;

源站: 支持 IP 或域名, 最多可添加 60 个;

回源协议:目前仅 HTTP 协议回源支持自定义端口,HTTPS 协议回源使用 443 端口,跟随请求协议回源将根据请求指定的协议回源到您源站的 80 或 443 端口

源站端口: HTTP 默认端口为 80 端口, HTTPS 默认端口为 443 端口, 也可以自定义端口; 回源 HOST: 回源 host 决定了回源请求访问到源站的哪个站点, 自定义配置时, 请确保您的 源站有配置相应的 HOST。如果源站是 IP 类型,回源 host 默认加速域名;如果源站是域名 类型,回源 host 默认是源站域名;

3, 填写网站安全配置

完成网站配置后,单击右下角【填写安全配置】,根据配置指引,完成安全防护配置。

▲ 边缘安全加速率会	☆ > 安全を知識 > 場合養養 → 場切れ来										
AccessOne	添加站点										
☆ 服务概法		<u> </u>									
○、安全与加速 へ	填写网站信息	选择网站安全配置	添加完成								
概范											
城名管理	web防护 描件检查OWASP top 10在内的规则引擎,能够有效的解如SQL注入、XSS攻击、webshel上传、命令注入等攻击										
证书管理	问题1: 请设置站完全局防护模式,仅当防护模式为拦截时,安全规则拦截动作才可生效,即若选择苦答,安全规	则为拦截动作采用告督处理									
安全报表		○ 注載 ○ 音管 (施存) ● 先初									
站点统计	问题2:根据不同的业务场景设置了不同的规则模拟,可以根据业务情况选择规则模拟。										
用量查询	這带于實業問題。且先許少量兼發的止怒场景,這團問規則僅於护等級放力严格。 容易測設的規則处理功作力否要,其他規則处理;	」)作为拦截(网站的护模式为拦截时刻重接进行拦截), 存在一定决模可能性。									
热门分析	问题3:请设置规则模板防护模式。规则引擎需要适配您的业务,为了避免误拦截影响您的处示服务,建议您先3	用告發欄式,注意,只有全局防护欄式和规则防护									
用户分析	○ 拦截 ● 告答 (推荐) ○ 关闭										
刷新预取	问题4:如果您站点的正常请求不会来非中国大陆,可选择是否封禁非中国大陆请求。										
🖳 零信任服务 🗸											
一 开发者平台 ~	问题5:为了体现安全防护效果,建议您开启一次站点风险扫描,扫描后,您能快速看到站点当前存在的安全风险	i									
□ 运营管理 ~											
① 计费详确			上—zb %5.tm%.nk								

4、填写完安全配置后,单击右下角【添加完成】,出现添加完成页面,单击【完成】,回到【域名管理】页面;

• h/4/h 4/h/2/2/4	◎) 会会知道: > 總合範囲: > 總估約項
CA AccessOne	添加站点
☆ 服务概范	₿₿₿
○ 安全与加速 ^	40784/88 334784/8228 354784
概范	
城名管理	站点验证已通过!站点新增大约需要5-10分钟,新增成功后,需要您将防护站点的DNS解析指向我们提供的CNAME,这样访问站点的请求才能转发到天翼云边缘云节点,达到加速与防护效果。
证书管理	站点添加完,如何开始配置?
安全报表	• 开始边接后,可能往 地名加度 进行边积极到的功能配置
站点统计	开始回過版。可解後 安全加步 开册veb50 PL DDos, boltship等安全起意
用量查询	 可能性< (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
热门分析	• 夏多幾代便用,可會考 产盘文档
用户分析	
周新预取	<u>#6</u>
風 零信任服务 ~	

完成新增域名操作后,可通过【域名列表】查看该域名配置是否完成,通过域名的状态字段 判断;

当域名状态为"配置中"时,表示域名配置没有完成,正在配置流转中。

当域名状态为"已启用"时,表示域名配置已经完成,您可以通过域名列表中提供的 CNAME 进行域名解析,接入安全与加速服务。

域名列表页

1							没东	Q 当前1	[作区:test工作区マ 个人中心
心缘安全加速平台	6	安全与加速 > 城名管理							
AccessOne	域名 展示已启	管理 用和已停用的域名,新增域名、扇用域名、停用域名需要配	200.						182
○ 服务概述	新和	Ⅰ状态 ~							查询 重要
○ 安全与加速 ^	编号	域名	CNAME	赛名类型	加速范围	状态	全局防护模式 ①	创建时间	操作
概览	1		а.	企业版	-	配置中	请选择 ~	2023-03-18 10.22:40	洋橋 開始
证书管理	2			企业版		配置中	请选择 ~	2023-03-14 14:23:10	洋情 副称
安全报表	3			企业版		配置中	清选择 ~	2023-03-13 14:58:03	洋橋 副除
站顺统计	4	-		企业版	-	配置中	資选择 ~	2023-03-13 10:12:47	洋橋 部時
用量查询	5	idu com		企业版		配置中	清选择ーーン	2023-03-10 15:40:51	1991gg 18800
热门分析	6		70	企业版	中国内地	已启用	清选择	2023-03-10 14:58:58	洋橋停用 185%
用户分析	7		n.	企业版	中国内地	已启用	请选择 ~	2023-03-10 14:13:09	洋橋 停用 副時
刷新预取	8	*		企业版	中国内地	已启用	講选择 ~	2023-03-08 23:28:32	洋橋 停用 副除
				0.0.0K	a Date	3 co m	Nex14-477	0000.00.07.00.00.40	
E6 开发着千台 ~	9	iterini iterini		IE 3EAR	THEP345	LiAH	antena .	2023-03-07 20.33.40	17710 17710 12500

域名配置完成,生成域名 CNAME,域名状态变更为【已启用】

步骤三: 配置 came

要启用—安全与加速服务,需要您将防护域名的 DNS 解析指向我们提供的 CNAME,这样访问防护域名的请求才能转发到安全节点上,达到防护效果。

1、在边缘安全加速平台—安全与加速服务控制台【域名管理】的域名列表中复制接入域名 对应的 CNAME;

域名列表-复制 CNAME 页

	◎ > 安全与加速 > 综合管理											
AccessOne	域名管理 第元已成明成已中期地域2、新型域2、中期域22、要数域2、新型域22、要数域2											
◎ 服务概范	新女孩去							*R ## 0				
○、安全与加速 へ	编号 域名	CNAME	客候类型	加速范围	状态	全局防护模式 ①	创建时间	操作				
概范	5455 3507	1										
域名管理	1	- 1	12 MAR		BCIRCH	attoire.	2023-03-18 10:22:40	ralli line				
证书管理	2 901		企业版		配置中	请选择	2023-03-14 14:23:10	评慎 图98				
安全报表	3		企业版		配置中	96/33FF	·· 2023-03-13 14:58:03	aria mas				
站廊绕计	4 m		企业版		配置中	请选择	2023-03-13 10:12:47	3710 Mile				
用量查询	5		企业版		配置中	10.53年	· 2023-03-10 15:40:51	17(B) 2010				
热门分析	6		? 企业版	中国内地	已启用	财政师	2023-03-10 14:58:58	1718 1778 2010				
用户分析												
刷新预取	7		企业版	中国内地	已启用	91339	2023-03-10 14:13:09	洋橋 停用 整路				
🖳 零信任服务 🗠	8 *.acc.		企业版	中国内地	已启用	雷选择	✓ 2023-03-08 23:28:32	1918 · 1919 - 2019				
🖳 开发青平台 🔍	9 wenxytesizon) 企业版	中国内地	已启用	清洁择	2023-03-07 20:33:40	17 M 49 H 100				
□ 运营管理 ~												

2、前往您的域名解析(DNS)服务商(如阿里云解析(原万网)、腾讯云解析(原 DNSPod)、 新网等),添加该 CNAME 记录。下面以您的域名在新网为例,其他域名解析服务商请联系 对应厂商技术支持处理。

3、登录新网的域名解析控制台,进入对应域名的域名解析页;

4、选择【添加新的别名】;

添加别名页

别名 (CNAME)(最多允许20条)	别名主机	TTL	操作	帮助
一共有0行,当前第1/0页,每页20行 首页 」	上一页下一页尾页到 页确定			
		3600		
漆加新的别名		提交 主:	只提交新加约	录
域名前缀	控制台复制来的(CNAME值		

【记录类型】选择为 CNAME;

【主机记录】即域名的前缀。例如,要添加 testlive.ctyun.cn, 前缀就是 testlive;

【记录值】填写为您复制的 CNAME 值;

解析线路和 TTL 默认值即可。

5、确认填写信息无误后,单击【提交】;

6、验证服务是否生效;

配置 CNAME 后,不同的服务商 CNAME 生效的时间也不同,一般新增的 CNAME 记录会立即生效,修改的 CNAME 记录会需要较长时间生效;

您可以 ping 或 dig 您所添加的加速域名,如果被指向*.ctdns.cn,即表示 CNAME 配置已经 生效,功能也已生效。

检查域名指向页

0:1. C:\	\Windows\system32\cmd.exe	
C:\Us	ers' >ping	
正在 来自 来自 来自	ctdns. cn [49.7.104.25] 具有 32 字节的数据: 49.7.104.25 的回复: 字节-32 时间=9ms TTL=55 49.7.104.25 的回复: 字节=32 时间=11ms TTL=55 49.7.104.25 的回复: 字节=32 时间=7ms TTL=55 49.7.104.25 的回复: 字节=32 时间=5ms TTL=55	
49.7. 登 征返行 量 C:\Use	104.25 的 Ping 统计信息: 数据包: 己发送 = 4. 己接收 = 4. 丢失 = 0 (0% 丢失), 亏程的估计时间(以毫秒为单位): 读短 = 5ms, 最长 = 11ms, 平均 = 8ms ers	

注意:

配置 CNAME 完毕, CNAME 配置生效后,边缘安全加速平台—安全与加速服务服务生效 CNAME 配置生效时间:新增 CNAME 记录会实时生效,而修改 CNAME 记录需要最多 72 小时生效时间;

添加时如遇添加冲突,可考虑换一个防护域名,或参考以下"解析记录互斥规则"调整记录; 解析记录互斥规则:

	NS	CNAME	Α	URL	МХ	тхт	AAAA	SRV	CAA
NS	可重复	х	х	х	х	х	х	х	х
CNAME	х	可重复	х	х	х	х	х	х	х
А	х	х	可重复	X	无限制	无限制	无限制	无限制	无限制
URL	х	х	х	х	无限制	无限制	х	无限制	无限制
MX	X	х	无限制	无限制	可重复	无限制	无限制	无限制	无限制
TXT	х	х	无限制	无限制	无限制	可重复	无限制	无限制	无限制
CAA	х	х	无限制	无限制	无限制	可重复	无限制	无限制	无限制
AAAA	X	х	无限制	х	无限制	无限制	可重复	无限制	无限制
SRV	x	х	无限制	无限制	无限制	无限制	无限制	可重复	无限制

在提示冲突的时候,说明已经有对应的记录,不允许重复添加或者说不能添加对应的记录, 提供如下说明:

在 RR 值相同的情况下,同一条线路下,在几种不同类型的解析中不能共存(X 为不允许) X:在相同的 RR 值情况下,同一条线路下,不同类型的解析记录不允许共存。如:已经设 置了 www.example.com 的 A 记录,则不允许再设置 www.example.com 的 CNAME 记录; 无限制:在相同的 RR 值情况下,同一条线路下,不同类型的解析记录可以共存。如:已经 设置了 www.example.com 的 A 记录,则还可以再设置 www.example.com 的 MX 记录; 可重复:指在同一类型下,同一条线路下,可设置相同的多条 RR 值。如:已经设置了 www.example.com 的 A 记录,还可以再设置 www.example.com 的 A 记录。

3.3.1.2 域名归属权限验证指南

简介

本文介绍在新增域名操作,如果需要域名归属权验证,要如何操作 客户可根据如下方法一、方法二,任意选择一种方式进行操作验证即可。

方法一: DNS 解析验证

示例为 ctcdn.cn 的解析配置

1、客户需在自己的域名解析服务商,添加天翼云控制台返回的 TXT 记录值(如下记录值仅 为示例)。

记录类型	主机记录	记录值
тхт	dnsverify	202207060000002 jar 4 fb 2 hc 79 iwjq5 cdid 87 t7 rci1 sgp33 exuy vez4 kwo no bxt



2、域名解析操作完成后,等待(建议10分钟)DNS 解析生效后即可进行解析验证。

解析命令: dig dnsverify.ctcdn.cn txt

'\$dig dnsverify.ctcdn.cn txt global options: +cmd Got answer: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14801 flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 ; OPT PSEUDOSECTION: EDNS: version: 0, flags:; udp: 4096 ; QUESTION SECTION: dnsverify.ctcdn.cn. IN TXT ; ANSWER SECTION: dnsverify.ctcdn.cn. 600 IN TXT "202207060000002jar4fb2hc79iwjq5cdid87t7rci1sgp3 ;; Query time: 93 msec ;; SERVER: 119.29.29.29#53(119.29.29.29) ;; WHEN: Fri Jul 29 10:42:31 CST 2022 MSG SIZE rcvd: 124

3、如解析出来的 txt 值和天翼云控制台返回的 TXT 记录值一致,则表示配置正确。

确认配置正确后,可前往天翼云控制台,在新增域名界面点击验证,验证通过就可以正常操作新增域名。

方法二: 文件验证

示例为 ctcdn.cn 的解析配置

1、在您的源站根目录下,创建文件名为: dnsverify.txt 的文件,文件内容为天翼云控制台返回的 TXT 记录值(如下记录值仅为示例)
Internet Information Services (I	IS)管理器						
← → ● → Z → 网站 →	ctcdn.cn 🕨						
文件(F) 视图(V) 帮助(H)							
推接	Ctcdn.cn	内容					
	筛选:	• 🍞 开始(G)	全部显示(A) 分	组依据:不进行	分组・		
	名称		类型 TXT 文件				
> 🔮 www.ctcdn.cn	□ c	tcdn.cn)新建 ~	0 6	e) ¢	<u>ن</u>	↓排序、 三 音看、	.] .
	÷	\rightarrow ~ \uparrow	→ × ↑ 🚞 « wangzhan → ctcdn.cn 🕚		~ C	。	搜索
		二 作业			名称	^	
	>	OneDrive			📔 dnsverify	.txt 🔶	

2、文件在源站根目录下创建完成后,即可进行访问验证(示例为访

问 http://ctcdn.cn/dnsverify.txt)

windows 验证:

	C ctco	dn.cn/dnsverify.txt	×	+
\leftarrow	C	▲ 不安全 c	t <mark>cdn.cn</mark> /dns	sverify.txt

202207060000002jar4fb2hc79iwjq5cdid87t7rci1sgp33exuyvez4kwonobxt

linux 验证:

<pre>curl -v http://ctcdn.cn/dnsverify.txt * Trying 1 :80 * Connected to ctcdn.cn (1 .) port 80 (#0) > GET /dnsverify.txt HTTP/1.1</pre>		
> Host: ctcan.cn > User-Agent: cur1/7.83.1		
Accept: */*		
<pre>* Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Content-Type: text/plain < Last-Modified: Thu, 04 Aug 2022 01:54:02 GMT < Accept-Ranges: bytes < ETag: "3afb4b12a5a7d81:0" < Source: Wiegnooft=LIS/10.0</pre>		
<pre>< Server: Microsoft 113/10.0 < Date: Thu, 04 Aug 2022 02:07:23 GMT < Content-Length: 64 </pre>		
202207060000002jar4fb2hc79iwjq5cdid87t7rci1sgp33exuyvez4kwonobxt	Connection #0	to host ct

3、如访问展示的文件内容和天翼云控制台返回的 TXT 记录值一致,则表示配置正确。 确认配置正确后,可前往天翼云控制台,在新增域名界面点击验证,验证通过就可以正常操 作新增域名。

3.3.1.2 域名配置

简介

通过该模块可以对资源文件的回源地址进行管理以及配合源站实际业务场景进行更高级的 配置,包括源站配置、缓存配置、网络优化等。

操作步骤

步骤一:进入边缘安全加速平台控制台

- 1、打开天翼云官网 http://www.ctyun.cn, 注册并登录;
- 2、选择控制中心;

🗰 2015 🥶 11FTA 🥶 11FMAI 🧰 107/ 🔛 / RRIE 📑 ARAURT 📑 USAA 📑 ARIS 📑 2018	
【 (1) このののののののののののののののののののののののののののののののののののの	饮云主机 <mark>1折起,</mark> 续费升级 <mark>7折起</mark> !
◆ 天興石 最新活动 ◇ 产品 ◇ 解決方案 ◇ 应用商城 ◇ 合作伙伴 ◇ 开发者 ◇ 支持与服务 ◇ 了解天麗云 ◇	Q、 中国站 / 文档 控制中心 备案中心 管理中心 登录
边缘安全加速平台 地球空如應平台-依托全国告변的分布式边球资源并基于边缘云最建;利用云原生技术实现网络底景的性 能、安全、解力原子能力增排融入发一网络;多容弧、多协议(5GL3L4L47等)ail-none的网络核一接 大;自助化服务、运营管理与分析,可限化据表与分析等集中化的统一管理平台;满足不同场景需求的 10开版 帮助文档 >	

3、下拉选择 CDN 产品,点击对应的边缘安全加速平台服务进入客户控制台;

步骤二:编辑源站配置

1、选择安全与加速—域名管理,点击【域名列表】—【详情】进入域名配置页面;

2、单击【站点加速】—【源站配置】

安全与加速		或名管理 > 站点加速 > 源站配置		域名切换 >> 专家告询 和助文档								
< 300	▮ 源站配置 yuk11.tem	ie5.com · 配置中		## <u>#</u> ###								
♥ 安全防护 ~	課站配置 回線H	深汕记置 国港HTTP减未失 国港VR放塔										
🗇 站点加速 🔷	源站配置	Robert m										
源站配置	建始: 88 支持PR地名,最多可测4000个											
城存配置		源站	层级	操作								
网络优化		1.1.1.1	±	修改 副除								
G2 访问控制	回源协议											
	* 回源协议:	• HTTP O HTTPS O INM										
		目前仅HTTP协议回避支持目走义统口、HTTPS协议回避使用443统口、国际请求协议回源将	関媒導求指定的协议回避到您测站的80家443號□									
	*源站端口:	*HTTP 80										
	回源HOST:	游输入										
		回還host決定了回該请求這同到認知的那个私点,默认值为加速域名。自定义配置时,请确保	総約3線站有配置相应的HOST,									

配置项说明:

源站配置: 支持 IP 或域名, 最多可添加 60 个;

回源协议:目前仅 HTTP 协议回源支持自定义端口,HTTPS 协议回源使用 443 端口,跟随请

求协议回源将根据请求指定的协议回源到您源站的80或443端口;

源站端口: HTTP 默认端口为 80 端口, HTTPS 默认端口为 443 端口, 也可以自定义端口; 回源 HOST:回源 host 决定了回源请求访问到源站的哪个站点, 默认值为加速域名。自定义 配置时, 请确保您的源站有配置相应的 HOST。

回源 HTTP 请求头: 支持自定义配置回源 HTTP 请求头;

安全与加速	(□) > 安全与加速 > 域名管理 > 站点加速 > 激站面	著	
< 返回	┃ 源站配置 yuk11.temle5.com ●配置中		
♥ 安全防护 ~	添加HTTP算求失	青求头	×
🗐 站点加速 🔷		请输入请求头参数	
源站配置	添加 管理回源HTTP请求头,可	参数仅支持大小写字母、数字、下划线、中划线	
Correct Philade	取值:	请输入取值	
缓存配置	参数	取值不支持空格及中文文字及字符。	
网络优化		智能要除此序成功应该决关,销售A R (图)。 智需要删除对应该决头,取道不适,置为空。	
☞ 访问控制			
		取消	

回源 uri 改写: 支持对回源请求的 URI 进行改写,可配置多条改写规则,支持正则表达式, 从上到下按顺序依次执行可以匹配的所有规则。

安全与加速	②) 安全与加速) 地名登诺 > 地名达诺 > 地名达诺 > 地名达诺 > 地名达诺 > 地名达诺 > 地名达 > 市场 化 地名达 > 市场 化 地名							
《 正面	Ⅰ 源站配置 yuk11.temie5.com • 配置	÷						
III matern		添加回源URI改	写	×				
C SCEROP	認知能區 回應HITP请求失	1 (53) FOND						
(2) 韩振加速 。	In the second se	146X-91-001.	以/开传的URI,不含http://供及端名。变描正则要达式,如"testk。					
理私配置	連續 支持対弧原请求的UR进行	* 目标Path:						
银行配置	特改写Path		以开头的URI,不含http://块及城名。					
网络优化								
G: 访问控制			Rin Mie					

步骤三:编辑缓存配置

1、选择安全与加速—域名管理,点击【域名列表】—【详情】进入域名配置页面;

2、单击【站点加速】—【缓存配置】,缓存配置是指中国电信天翼云 CDN 加速节点(包括 边缘节点和中心节点)在缓存您的资源文件时遵循的一套过期规则,当资源文件处于过期状 态时,此时用户请求会由节点发送至源站,重新获取资源中心内容并缓存至节点,同时返回 给最终用户;当资源内容未过期时,用户请求到 CDN 加速节点后,会由节点直接响应用户 请求。合理的配置资源文件缓存时间,能够有效的提升缓存命中率,降低回源率,节省您的 源站带宽。

配置项说明:

缓存过期时间设置:

您可以根据业务需求配置边缘节点缓存目录和后缀名文件来设置缓存过期时间时间,从而减 少请求回源对源站造成的压力以及保证源站内容更新的时效性。

当配置缓存过期时间时,类型选中目录,那么所填内容为文件缓存的路径,过期时间由您根据业务决定(一般支持1天、3天、5天)。类型选中后缀名时,所填写的内容为您业务所需要缓存文件的后缀名(动态文件不缓存)配置信息如下图所示:

安全与加速	② > 安全与加速 > 地名管理 > 站	·····································	1				地名切除 ~ 电影乐员 网络文档				
(#0	■ 缓存配置 yuk11 ternie5.com • 配置の										
		添加缓存时间	司规则		×						
V SCENTIP	· · · · · · · · · · · · · · · · · · ·										
2 站底加速 ~	缓存配置	• 类型:	○ 后缀名 🧿 目录 ○ 首页 ○ 全部文件 ○	全路径文件							
源站配置	增加 支持配据自定义资源的第 全局软认优先着低源处理	*内容:	Nest, /ah/c (不能以//结粒)								
接行配用	类型	*过期时间:	ayata / Gerz Ha ak 80	天 ~		92.ML	操作				
网络优化	后缀名	* 缓存规则:	○ 不缓存 ○ 优先遗谣源站 🧿 强制变存			10	17.27 BBA				
OF INTERIO	后缀名	*去问号缓存:				10	19.77 - 19.94				
an analysis	后缀名	*权重:	10			10	62.8M				
	ka 🔼										
完全与timite	② > 安全与加速 > 城名管理 > 始	uttole > letype	<u>.</u>				MSUN - NECH NECH				
又王马加西	I 细花积雪 vukti temieš com · 新聞										
< 3810	1	:#tn(@/=p+i			×						
♥ 安全防护 、	编行过期时间 状态码过期时间	///ut/g17u3/	EK3042								
器 粘带加速 ~	順存配置	* 类型:	◎ 后缀名 ○ 目录 ○ 首页 ○ 全部文件 ○ :	全路径文件							
原始配置	基即 支持配置自定义资源的爆 全局取认优先清晰滞站缓	* 内容:	jpg.png.css (U.". "3721)								
還存款成	美型	· 过期时间:	18時人間停留場合 80	天 ~		权調	銀作				
网络优化	后蜀名	* 續存規則:	○ 不壞存 ○ 优先通货游站 🧿 強制该存			10	95.2 BBs				
	后御名	* 去间号缓存:				10	1932 IBI8				
	后儒名	*权重:	10			10	122 808				

状态码过期时间设置: 您可以配置状态码缓存, 并设置状态码缓存过期时间。状态码可在 403 和 404 之间选择, 缓存时间可选择按天、小时、分钟、秒设置。

R/6 862

安全与加速	② > 安全与加速 > 城名管理 > 共									
< 1500	■ 缓存配置 yuk11 tervie5 com + 配置	J配置 yuktisenie5.com +克田中								
		添加状态码缓	×							
♥ 安全防护 →	维存过期时间 状态和过期时间									
() 始來加速 ~	状态码设置	"过期时间:	80	天						
即站配置	an officerstations)	*状态码:	支持多个状态码输入,用语号"、"分割							
國存在世	状态码									
网络优化										
@ 访问控制										

HTTP 响应头设置:

可设置 HTTP 响应头,目前提供10个 HTTP 响应头参数可供定义取值。分别为: Content-Type、 Cache-Control、Content-Disposition、Content-Language、Expires、 Access-Control-Allow-Origin、Access-Control-Allow-Headers、 Access-Control-Allow-Methods、Access-Control-Max-Age、 Access-Control-Expose-Headers。

安全与加速									
< 返回	■ 缓存配置 yuk11.temie5.com • 配置								
♥ 安全防护 ~	缓存过期时间 状态码过期时间								
盐点加速 ~	Http响应头	* 參数:	请输入响应头参数						
源站配置	适加 管理回源HTTP能应头,可		参数仅支持大小写字母、数字、下划线、中划线						
维存配置	参数	1926頁:	资输入职值						
网络优化			取值不支持空格及中文文字及字符。						
命 访问控制			若需要添加/修改对应响应头,请输入取值。						
			若需要删除对应响应头,取值不填,置为空。						
			取加						

步骤四:编辑网络优化

1、选择安全与加速—域名管理,点击【域名列表】—【详情】进入域名配置页面;

2、单击【站点加速】—【网络优化】

配置项说明:

动态加速:

开启动态加速后,在套餐基础上,客户端用户与边缘节点的动态请求数将被计费。开启动态 加速后,需要选择【选路方式】和【动态回源策略】;

选路方式可以选择:

(1) 快速选路:适用于对访问速度要求比较高的客户,例如:金融、电商、娱乐资讯等客 户;

(2) 稳健选路:适用于对链路稳定性要求比较高,对时延要求相对不高的客户,例如:政 府、企业办公等客户场景;

(3)应用层选路:适用于大文件下载等对下载速率和首包时间等应用层性能要求比较高的 客户,适用于所有 http/https 加速的客户,可按需配置; 动态回源策略可以选择:

(1) 择优回源:优先回最快的源站,忽略权重;

(2) 按权重回源: 按照配置的权重回源;

(3) 保持登录:基于客户端 IP 哈希回源

Websocket:

开启后 WebSocket 协议支持服务端主动向客户端推送数据。开启后,默认超时时间 15 秒.

3.3.2 web 防护配置

3.3.2.1 域名规则

简介

安全与加速服务的 web 防护使用基于正则的规则防护引擎和基于机器学习的 AI 防护引擎, 进行 Web 漏洞和未知威胁防护。

Web 防护规则防护引擎,目前防护 Web 攻击包括:SQL 注入、XSS 攻击、恶意扫描、命令 注入攻击、Web 应用漏洞、WebShell 上传、不合规协议、木马后门等 17 类通用的 Web 攻击。

WAF 规则防护引擎,支持规则模板配置,用户可根据实际业务需要选择适合的模板,同时 提供基于指定域名 URL 和规则 ID 白名单处置策略,进行误报处理。

设置防护模式

 1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web防护】;
 2、防护模式:策略的生效动作(拦截/告警),或者可以关闭域名规则;

安全与加速	◎ > 安全与加速		城名切换 > 专家咨询 帮助文档										
< <u>20</u>	┃ Web防护 yuk1												
♥ 安全防护 へ	基础配置 圳	基地起置 地名和哈利 业务安全防护											
Weblittin	防护机式 • 普爾 · 拦截 · 关闭												
Ddos防护	域名规则	规则相	数: 敏感的护规则集					規則ID ~ 調輸入規	RID 総想設作				
CC防护 BOT防护 (陽奈)	规则白名单	規则白名单	规则旧	攻击类型	风险等级	CVE编号	规则开关	处理动作①	操作				
□ 站点加速 ~			1002	代理维存服务器漏洞	低	test	开启	拦截	编辑 加辛				
G2 访问控制							5100	数据库注入	高		开启	舌管	编辑 加加
			5101	数据库注入	商		开启	拦截	编辑 加田				
			5102	数据库注入	ĩĩ		开启	拦截	编辑 加白				
			5103	数据库注入	商		开启	拦截	AN INT				
			5104	数据库注入	ĨĨ		开启	拦截	编辑 加白				
			5105	数据库注入	窗		开启	拦截	编辑 加曲				
		# 515	冬 10条/西 🗸 📊	2 3 4 5 6	52 > 前往 1	a							

规则管理

 1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web 防护】;
 2、在"域名规则"页签内,可基于域名实现对单条规则的开启与关闭;

3、在"域名规则"页签内,单击【规则模板】,可以更换域名规则模板。

规则白名单或误报处理

1、登录边缘安全加速平台控制台, 在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面, 在左侧导航栏中选择【安全防护】—【web 防护】; 2、在"域名规则"页签内,单击规则列表中的【加白】,可以实现基于规则 ID 的加白名单及 误报处理,加白后的规则会展示在规则白名单页签里。

安全与加速	会 安全与加速	22、安全市加速、減名管理、安全防护、WetRithe 地名加速										地名切纳 💚	*****
()))	₩eb资理P yuititienieScen * #E微中												
· 安全防护	INFR .		A 1014	QAlbon						×			
Weologe	MARKIC O 1	18 O	拦截	加白规则ID;	1002								
DdosØ389		#0.01H#465	-	*匹配方式	匹配李段	逻辑符号		匹配内容	15	612	REDID - STAL		
COLIZIA	规则白名单				WHEN P	~ 筋造理		游临入		18	の理論的なの	摄作的	
BOT防护 (開先)			002				落加 还可以清加	4条、量多5条			Hes	45 305	
E alexanize					新增还可以添加4条,最多	5条							
@ 访问控制			100								行警		
			101						取油	82	拦截	MHR 2005	
			102		数据库注入	商		*	开启		巨戰	46 200	
					数据库注入	-			开启		in the second	-	

3.3.2.2 合规检测

简介

安全与加速服务的 web 防护可以根据用户实际配置的条件,检查 HTTP 协议头部,对 HTTP 请求信息中的方法以及参数长度等信息进行检测,对不符合的请求项进行拦截或告警。可以 对以下情况进行检测:

- 1、请求方法检测:只允许指定请求方法访问网站。
- 2、请求协议检测:只允许指定协议版本访问网站。
- 3、请求头部缺失检测:请求缺少指定头部禁止访问网站。
- 4、数据重复检测:针对头部重复,参数重复进行拦截,禁止访问网站。
- 5、请求数据长度限制:针对请求 URL,头部参数进行长度限制,禁止访问网站。

设置合规检测策略

注意: 域名新增时, 会有一条全站合规检测的默认策略, 可以通过【防护开关】来开启或者 关闭。

安全与加速	> 安全与加速 > 域名管理 > 安全防	8ª > Web®58ª				城名切换 🗸	专家咨询 帮助文档
< 380	● Web防却 ● 配搬中						2 9888M
♥ 安全防护 へ	基础配置 域名规则 合规检测	业务安全防护					
WebB5P	数护开关: ① 开启 ④ 关闭						
Ddos的种							新聞
CCB5#P	优先级 ①	规则名称	规则描述	开关	防护范围	操作	
BOT防护(限免)	1	all	全站合规性检测	关闭	全站	 Gill 209	
🖸 kkrittelille 🗸 🗸							
命 访问控制							

 1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web防护】;
 2、在"合规检测"页签内,单击【新增】按钮,可以新增一条合规检测策略。
 配置项说明:

防护模式:控制策略的处理动作,可以选择拦截、告警、关闭;

规则名称:设置规则名称;

规则描述:设置规则描述;

防护范围:设置要防护的路径;

允许 HTTP 请求方法: 设置允许的请求方法;

允许 HTTP 协议版本:设置允许的 HTTP 版本,限制非指定 HTTP 版本访问源站,保证源站 针对性服务,不受黑客攻击; '

HTTP 请求头部缺失:请求缺失对应头部则告警或拦截。针对 HTTP 请求的头部进行缺失防 护,当请求到达服务器时,检测到缺失头部时,进行相应处理动作

例外:如果有特殊的业务无法通过合规检测策略,可以进行加白,则请求不会进行合规检测 策略校验。

3.3.2.3 cookie 防护

简介

cookie 防护采用 cookie 加密、cookie 签名等方式对 cookie 字段的字进行加密或签名, 防止 敏感信息泄露以及防护一些使用 cookie 中的弱 key 进行权限绕过的漏洞利用, 也能在一定 程度上限制基于 cookie 修改的爬虫。

设置 cookie 防护策略

 1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web 防护】;
 2、在"业务安全防护"页签内,进入"cookie 防护"页面,可以配置 cookie 防护策略。

敏感词防护网页防篡改	条件:	* cookie key@: 游曲\koy@	
攻击挑战		防护方式 💆 加電 🧧 签名 * 👔 计选择 🗸	
		*防护动作: 〇 拦截 〇 満除	
		* 防护过渡期 ③ 请输入防行过渡期	
		cookie漏性: HTTP Only Secure	
		II 还可以质加4g、最多5g	

配置项说明:

防护开关:控制策略的处理动作,可以选择拦截、告警、关闭;

Cookie key 值: 设置需要防护的 Cookie 名称, Cookie 必须有参数值, 例如: set-cookie: SF_cookie_11=ENCRYPT_COOKIE1988262423afZ5ZEIzbEL%3D; Secure; SameSite=Strict, 只有 SF_cookie_11、SameSite 可配置为 key;

防护过渡期:在过渡期内,检测失败不会进行拦截,只会清除 cookie 值;

防护动作:拦截/清除(拦截:Cookie 值检测不通过将拦截请求;清除:Cookie 检测不通过 清除该 Cookie 回源)

防护方式:加密(对 Cookie 值进行加密,客户端查看到的值为加密后的内容)、签名(对 Cookie 值进行加密,客户端查看到的值为加密后的内容);

例外:如果有特殊的业务无法通过 cookie 防护策略,可以进行加白,则请求不会进行 cookie 防护策略。

3.3.2.4 敏感词防护

简介

敏感词防护功能支持对网站返回的内容进行脱敏展示,过滤内容包括敏感信息(如身份证、 手机号和银行卡等)。您可以根据实际需要设置敏感词防护规则,满足数据安全保护和等保 合规需求。

设置敏感词防护策略

1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】,
单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web防护】;
2、在"业务安全防护"页签内,进入"敏感词防护"页面,可以配置敏感词防护策略;

cookie防护	*防护开关:	● 关闭) 告答 () 脱敏						
敏感词防护 网页防算改	*防护范围:	匹配字段		逻辑符号			匹配内容		操作
攻击挑战		URI		包含	~ IERI		L*		删除
						漆加 还可以添加	104条,最多5条		
		新增条件 还可以	添加4条,最多5条						
	*匹配内容:	🗹 身份证	☑ 银行卡 ☑ 邮箱 ☑ 手	机带					
	例外:	手机号码:	支持填写多个,多个以英文分隔符;8	研					
		银行卡:	支持填写多个,多个以英文分隔符。	8开					
		身份证	支持填写多个,多个以英文分隔符系	8 71					
		由同籍:	支持填写多个,多个以英文分隔符,	朝开					

配置项说明:

防护开关: 设置敏感词防护策略的处理动作, 可选择关闭/告警/脱敏;

防护范围:需要检测的范围,默认为全站;

匹配内容:设置需要脱敏处理的内容,可选择手机号码/银行卡/身份证/邮箱 例外:当部分敏感词不需要进行脱敏时,可以配置例外,如果填写多个要使用分号隔开

3.3.2.5 网页防篡改

简介

网页防篡改功能用于保护网站核心静态页面,通过对比源站响应与媒体存储中心缓存的响应, 保护网站因为源站页面被恶意篡改带来的负面影响,同时您可以根据需要配置防篡改规则。 新增网页防篡改策略

1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】,单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web防护】;2、在"业务安全防护"页签内,进入"网页防篡改"页面,可以配置网页防篡改策略;

新增网页防篡改

*规则名称:	支持中文、英文、数字和下划线,最多支持30个字符	
*防护URL:	请输入需要防护的完整的URL,例如http://xxx/1.php,会自动	获取页面下的所有静态资
名是否有CDN加速:	● 否 ○ 是	

配置项说明:

防护模式:可以选择开启或者关闭策略;

规则名称:设置规则名称;

防护 URL:填写需要防篡改防护的完整 URL 地址,例如 http://www.xxx.com/。该功能会自动获取页面下的所有静态资源

处理动作:拦截/告警/返回 WAF 缓存页面

域名是否有 CDN 加速:您的域名如果有 CDN 加速,则需要填写请求协议、源站 IP、回源端口、回源 HOST。

编辑网页防篡改策略

1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】,
单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web防护】;
2、在"业务安全防护"页签内,进入"网页防篡改"页面,在操作列表中单击【编辑】按钮;

规则ID	规则名称	URL	防护模式	处理动作	文件缓存时间	操作
1	11111	http://cg0111-2.soc.com /test	开启	拦截	5	查看编辑删除

删除网页防篡改策略

1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】,
单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web防护】;
2、在"业务安全防护"页签内,进入"网页防篡改"页面,在操作列表中单击【删除】按钮;

3.3.2.5 攻击挑战

简介

攻击挑战指自动阻断在短时间内发起多次 Web 攻击(规则引擎触发)的客户端 IP, 一段时间内阻止所有请求, 阻断日志可以在 攻击日志 中查看, 可以快速拦截恶意攻击 Web 的 IP, 快速应对恶意扫描及代理、Web 攻击威胁等行为, 可提升攻防对抗效率。

设置攻击挑战策略

1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】,
单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【web防护】;
2、在"业务安全防护"页签内,进入"攻击挑战"页面,单击【新增】按钮;

* 攻击类型:	请选择						
* 触发条件:	在 1	分 🗸 之内,	请选择 ~	触发防护规则的次数达到	0	次,则执行	请选择 ∨
处理动作持续时间:	1	秒 ~					
例外的规则ID:	请输入需要	要例外的规则ID,多个	心以英文分隔符;隔	Ŧ			
例外客户端IP:	请输入需要	要例外客户端IP,多个	"以英文分隔符,隔	Ŧ			
描述:	最多支持:	200个字符					

配置项说明:

开关: 防护策略开关, 可选择开启或者关闭策略;

攻击类型:仅勾选的攻击类型会做统计。点击"全部"按钮就自动选中所有攻击类型; 处理动作持续时间:指客户端 IP 满足触发条件后,处理动作会持续的时间; 例外 ID:例外的规则 ID,规则 ID 可在域名规则中查询; 例外客户端 IP:不需要过攻击挑战功能的客户端 IP;

3.3.3 CC 防护

简介

CC 防护根据访问者的 URL,频率、行为等访问特征,智能识别 CC 攻击,迅速识别 CC 攻击 并进行拦截,在大规模 CC 攻击时可以避免源站资源耗尽,保证企业网站的正常访问。

设置长久模式 CC 防护策略

 1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【CC防护】;
 2、在"CC防护"页面内,单击【编辑配置】按钮;

3、【CC 防护】设置为开启, 【CC 防护模式】设置为长久, 则域名的每次访问都进行防护

校验;

CC防	ir in the second se	• 配置中						
	* CC防护:	关闭开启						
* CCR	护模式 ①:	长久 阈值						
防护	沖规则 ①:						请输入关键字进行全	文證素 新端規則
序号	规则ID	匹配条件 ①	GET防护策略 ①	POST防护策略 ①	验证方式	非html静态文件	处理优先级	操作
		粒度: URI (包含) 正则 "/.**						
1	38961	检度: HEADER (不包含) KEY: 正则 upgrade	第一策略: CC302 第二策略: 空	第一策略: CC307 第二策略: 空	cookie形式	检测	1	46 Bb
		VALUE: IERI WEDSOCKEI						

3、单击【新增规则】,可以自定义 CC 防护规则

匹配条件 🕛	匹配字段	逻辑符号		匹配内容			操作
	请选择	~ 请选择	~~	清榆入			删除
			添加还可	以添加4条,最多	5条		
GET防护策略 🕧	*第一策略	请选择	\sim	* 第二策略	请选择	~	
POST防护策略 🕕	*第一策略	请选择	~	* 第二策略	请选择	~	
* 验证模式	cookie形式	○ url参数形式					

取消 确定

配置项说明:

匹配条件:满足条件才进行防护校验,多条件之间与关系。可选字段如下:

- (1) IP: 客户端 IP, 比如: 192.168.1.1;192.168.1.2
- (2) PROTOCOL: 请求协议, 比如: HTTP/1.0;HTTP/2.0;HTTP/0.9
- (3) HEADER: 请求头部
- (4) GEO: 地域
- (5) ARGS: 问号后参数名
- (6) METHOD: 请求方式, 比如: GET; POST
- (7) REQUEST_URI: URI 包括问号后参数,比如: login.php?id=1
- (8) IPS: 客户端 ip 段,比如: 192.168.1.0/24;192.168.2.0/24

GET 防护策略:对 GET、COPY、OPTIONS、DELETE、HEAD 请求协议生效;

PST 防护策略:对 POST、PUT 请求协议生效;

验证模式:选择人机挑战设置参数的位置;

非静态 HTML 文件: 请求 Accept 头部 != text/html 或 text/* 并且 url 后缀 =css;js;xml;txt;ini;pjpeg;flv;mp4;mp3;wmv;wma;avi;apk;rpm;deb;tar;bin;ogg;mpg;mpeg;f4v;rm; 3gp;img;cur;jpe;ico;gz;bz2;zip;rar;jar;msi;cab;7z;pdf;aac;swc;doc;docx;xls;xlsx;ppt;pptx;rmvb;ip

a;sis;xap;m3u8;ts;gif;jpg;jpeg;swf;png;bmp;srt;plist;amr;spx;tex;mesh;m2b;animation;scene;ta; attach;lnk;svg;lua;dat;audio;atf;exe]

- (1) 不检测: 非 html 静态文件不过人机挑战校验
- (2) 检测: 非 html 静态文件过人机挑战校验

设置阈值模式 CC 防护策略

 1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】—【CC防护】;
 2、在"CC防护"页面内,单击【编辑配置】按钮;

3、【CC 防护】设置为开启, 【CC 防护模式】设置为阈值, 则域名访问达到防护条件时进 防护;

e5.com • 配置中		
关闭	开启	
长久	阈值	
5000		次
5		3
7200		秒
	e5.com •配量中 关闭 长久 5000 5 7200	e5.com • 配量中 关闭 开启 长久 阈值 5000 5 7200

配置项说明:

在【周期】内达到【阈值】则接下来【防护时长】内符合条件的请求均进行防护校验。

3.3.4 DDoS 防护

简介

DDoS 防护可有效防御 SYN Flood、ACK Flood、UDP Flood、ICMP Flood 等网络层攻击以及 SSL、DNS 等应用层攻击。

设置 DDoS 清洗阈值

- ① 登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】--【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【安全防护】--【DDoS 防护】;
- 2、 配置 DDoS 清洗阈值,当客户所有接入域名的带宽总和超过 DDoS 清洗阈值,则开始一次 DDoS 攻击防御。建议将阈值配置为正常业务带宽的 1.5 倍。若客户正常带宽为 50Mbps,则建议将阈值配置为 75Mbps。该阈值在任意域名下配置全局生效。

安全与加速	☆ > 安全与加速 >	は名管理 > 安全防护 > DDoS防护		
〈 返回	DDoS防机	• 已启用		
◎ 安全防护 へ	基础配置			
Web防护	* DDoS清洗阈值:	请输入DDoS清洗顽值	Mbps	(配置范围: 10~1000)
DDoS防护	说明: DDoS清洗阈	值针对所有域名的带宽总和,在任意域名下配置全	局生效	
CC防护				
BOT防护(限免)				
♂ 站点加速 ─ ~				
ै 访问控制				

3.3.5 访问控制

简介

访问控制可针对 IP,IP 段, URI, CI, METHOD, 请求地区, 请求参数, 请求头部, 请求协议 进行组合, 设置白名单和黑名单, 对请求进行拦截和放行, 保证客户网站不受未知访问。 设置禁止特定 IP 地址访问域名

 1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【访问控制】,单击【新增】 按钮;

2、在新增页面,输入规则名称(如拦截指定 IP),在匹配字段中选择一个字段(如 IP), 逻辑符号选择包含,匹配内容填入需要禁止访问的来源 IP(如 192.168.1.1),选择执行动 作(如拦截),填写完成后,单击确定,保存规则。

新増						×
*启用:						
*处理动作①:	○ 告警 ○ 加白	○ 攻击标记	●拦截	○ 丢弃		
*规则名称:	拦截指定IP					
规则描述:	请输入规则描述					
防护范围 ①:	匹配字段	逻辑符号		匹配内容		操作
	IP ~	包含	~	192.168.1.1		删除
			添加 还可以添加	四9条,最多10条		
					取消	确定

设置地域封禁

1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【访问控制】,进入"访问 控制"页签,单击【新增】按钮;

2、在新增页面,输入规则名称(如拦截指定地域),在匹配字段中选择一个字段(如GEO), 逻辑符号选择包含,匹配内容填入需要禁止访问地域(如欧洲),选择执行动作(如拦截), 填写完成后,单击确定,保存规则。

新增							
* 启用:							
*处理动作 ():	○ 告警 ○ 加白	○ 攻击标记	● 拦截	○ 丢弃			
*规则名称:	拦截指定地域						
规则描述:	请输入规则描述						
防护范围 🕕	匹配字段	逻辑符号		匹配内容		操作	
	GEO 🗸	包含	\sim	欧洲/德国 ◎ +56	~	删除	
	添加还可以添加9条,最多10条						
					取消	确定	

3.3.6 频率控制

简介

通过配置 IP,URL,ARGS,HEADER,COOKIE,UA,CI 等粒度,进行访问次数限制,防止客户资源被过度消耗。

设置客户端 IP 访问域名首页次数限制

1、登录边缘安全加速平台控制台,在左侧导航栏中选择【安全与加速】—【域名管理】, 单击域名列表【详情】进入域名配置页面,在左侧导航栏中选择【访问控制】,进入"访问 控制"页签,单击【新增】按钮;

2、在新增页面,输入规则名称(如单 IP 访问首页次数限制),选择统计粒度(如 IP),在 触发条件中设置触发条件(如在 59 秒内,低 5 个请求开始执行处理动作),选择处理动作 (如拦截),填写完成后,单击确定,保存规则。

新增				×
* 启用:				
*处理动作 (1):	○ 告警 🧿 拦截	○ 人机跳转	○ 丢弃	
*规则名称:	单IP访问首页次数限制			
规则描述:	请输入规则描述			6
* 统计粒度 ①:	IP 🛞	~		
触发条件:	0 时 0	分 59	秒 之内, 第 5 个请求开始执行处理动作	
*处理动作持续时间:	0 时 10	分 0	秒	
防护范围 ①:	匹配字段	逻辑符号	匹配内容	操作
	PATH ~	包含	×] [1	删除
			添加还可以添加9条,最多10条	
静态文件过滤:	支持添加多个后缀名,多	▶个请用英文分	高符:隔开	li
				取消 确定

3.3.7 BOT 防护

简介

边缘安全加速平台提供的爬虫防护,能够通过分布式架构形成云端 BOT 管理网络,提供 BOT 管理防护方案,协助客户积极管控肆虐的 BOT 流量,对抗 BOT 流量背后的黑灰产产业链,保 护客户的正常流量,缓解大量针对网站的爬取和异常注册登录行为。

Bot 防护开关

为爬虫防护的功能开关,提供拦截、告警、关闭三个选项,对具体防护规则有不同影响:

- 拦截:防护模式为拦截,具体防护规则按照其配置的处理动作生效
- 告警: 防护模式为告警, 具体防护规则处理动作为拦截也生效为告警
- 关闭: 防护模式为关闭,具体防护规则配置的处理动作都不生效

通用配置

- 客户端标识过期时间:默认 15 天,单位天,最大值 365 天;
- 监测静态文件后缀:即需要监测的静态文件,以后缀进行标识。若未填写的话,默认检测 js, css, jpg, jpeg;
- 客户端标识检测:客户端标识检测是第一检测策略,校验下发的 cookie 个数和完整性, 无客户端标识、客户端标识缺失、客户端标识解析失败都需要配置
 - (1) 无客户端标识。即针对请求没有 cookie 的情况进行处理;
 - 1) 处理动作: 拦截/告警/跳转/放行
 - 拦截: 拦截请求
 - 告警: 仅记录请求
 - 跳转: GET 请求启动 302 跳转策略, POST 请求启动 307 跳转策略
 - 放行:不对该异常做处理,另外不会再校验其他的 BOT 防护规则
 - 2) 统计粒度: 静态 cookie/IP+UA/IP

 3) 触发条件:达到触发条件的请求将对其执行处理动作,并支持配置处理动作 持续时长(触发规则后的惩罚时间)

- (2) 客户端标识缺失。即针对请求带回 cookie 个数小于下发的个数(最多会下发四个)进行处理;
- (3) 客户端标识解析失败。即针对失败解析 cookie 的情况下进行处理

● 白名单。即例外条件,符合条件的请求不进行功能检测

安全与加速-域名详情-BOT 防护-通用配置页

	云平台			当前工作区:安全加速 🗸 个人中心 🛛 📃
◎ 安全与加速	☆ > 安全与加速 > 域名管理 > 安全防 ☆	户 > BOT防护 (限免)		地名切换 >> 专家咨询 帮助文档
	BOT防护(限免) Intest0504.temie5.co	m • 已始用		2. \$\$\$\$\$500
□ □ 安全防护 へ	基础泥面			
(i) Web(5)P	Bot防护开关 ①: ③ 监控 〇 拦截	◎ 关闭		
DDoS防护	通用配置 通用配置:配置爬虫第	缩时,需要先开启域各开关并且能置通用能置项,策略才会生效,更	1週后会下发客户错标识,检测请求显否为爬虫	
CC防护	特性挑战 客户端标识过期时间:	1 天		
BOT防护(服务)	國值限制 监测静态文件后缀:			
♂站点加速 ~	爬虫陷阱		•	
8 访问控制		请输入需要监测的静态文件后端,多个请用:"分隔;若未填写任何后端。	// Mil.M2Mjs.css.jpg.jpeg	
	客户端标识检测 ①:	无詹户端标识 客户端标识缺失 客户端标识	峄析失败	
		如果请求带担的Ci个数为0,则认为显爬虫		
		*执行动作: 〇 拦截 ④ 告誓 〇 跳转) (kłi	
		* 统计粒度: ① 静态CI ① IP+UA ④ IP		
		*触发条件:在 1 町 > 之内,第 20	个验证失败的请求开始执行处理动作,动作持续 10	
	白名单:	匹配学校 逻辑符号	匹配内容	损作
		请选择 > 请选择	✓ 请输入	10 Dz

特性挑战

(1) 跳转挑战

功能介绍:跳转挑战通过 302、307 跳转去防护无法正常执行跳转的爬虫,还能通过图 片验证和一些 JS 挑战检验用户交互行为。

配置介绍:对触发防护策略的请求进行跳转处理,并提供多次验证机会,不放过恶意爬 虫请求,也避免误拦截正常请求

- 可信任时间:首次要求跳转后,在信任时间内不会要求再次跳转。时间单位支持天、
 时、分;
- 跳转方式:对于 GET 请求执行 302 跳转,对于 POST 请求执行 307 跳转,后续将支持图片验证码挑战、JS 跳转等多种跳转方式;
- 首次失败机会时间:对于跳转失败的请求提供再次验证,即机会时间内,跳转失败 次数不通过后面的条件计数;
- 处理动作:支持对触发防护策略的请求执行拦截、计数告警、跳转、放行的处理动作。处理动作为跳转、放行则无需配置触发条件;;
- 统计粒度:静态 cookie/IP+UA/IP;
- 触发条件:达到触发条件的请求将对其执行处理动作,并支持配置处理动作持续时 长(触发规则后的惩罚时间)

特性挑战	- mystek.at:
阈值限制	都和地观地到202。507期林克思护·万正江思地与锡林的规定,已经通过即计验室和一曲39地站地用户交互行为,开启指令下发期韩公
爬虫陷阱	步骤一:为探风影响游戏探问语田时间,可语田时间过后将可喜我动行动结构温影或的行为
	*可倍任时间: 在超过 2 分 > 开始协行跳转
	*期時方式 gnt環史 🕑 302指点
	postiĝis: 🛞 307184.6
	步佩二:老闆将失责,并抱定下方部的华条件,将对诸式执行效果动作
	* 韵次块玻机金时间: 超过 5
	*处理动作: 目前 (1) 计数态整 (1) 编转 (1) 放行

(2) 静态 cookie 特性检测

功能介绍: 主要针对盗用 cookie 的请求进行处理,即通过对 cookie 内容和请求内容的 对比可以从不同维度进行爬虫检测,主要包括 IP、UA、以及过期时间等 配置介绍

- 超时异常。静态 cookie 中包含了时间信息,若攻击者盗用 cookie,请求中获取 到的时间会与 cookie 中记录有所不同。
 - 初次验证阶段:对于超时的请求提供初次验证阶段。首次超时请求的【】时间
 后,达到第【】个超时请求将进入再次验证;
 - 处理动作:支持对触发再次验证防护策略的请求执行拦截、计数告警、跳转、 放行的处理动作。处理动作为跳转、放行则无需配置触发条件;
 - 统计粒度:静态 cookie/IP+UA/IP;
 - 触发条件:达到触发条件的请求将对其执行处理动作,并支持配置处理动作持续时长(触发规则后的惩罚时间)
- 2) IP异常防护。静态 cookie 中包含了上次访问下发的 ip 信息,若攻击者盗用 cookie, 请求中获取到的 ip 会与 cookie 中记录的不同。配置说明同上。
- 3) UA异常防护。静态 cookie 中包含了上次访问下发的 UA 信息,若攻击者盗用 cookie, 请求中获取到的 UA 会与 cookie 中记录的不同。配置说明同上

*静态cookie特性检 开启后,将会对不	测: 【】 同客户端下发客户端标识。1	和过对cookie内容和请求内容	的对比可以从不同维度进行爬生	由绘制,主要和SDP、UA、以及过期时间
超时异常	IP异常防护 🕚	UA异常防护 🌗	标识位异常 😗	
步骤一:配置初	次验证阶段的规则(初次	金证内的请求不处理)		
*初次验证阶段:	首次超时请求 10	砂 ~ 后, 至第	5 个超时请求	
步骤二:配置用	次验证阶段的规则 (初次)	金证失败后,将进入两次验	油阶段,验证失败 奥对请求	执行处理动作)
* 处理动作:	◎ 拦截 ◎ 计数	告警 🔘 跳转 🤄	放行	

(3) 人机识别。

功能介绍:针对无法正常加载 js、或者模拟交互行为(例如移动鼠标等)的爬虫进行人机挑战。

配置介绍(超时异常与记录异常都需要配置)

- 1) 超时异常。针对人机识别挑战成功但超过验证有效期的请求
 - 验证有效期:提供验证机会时间,时间内的请求不进行挑战;
 - 处理动作。支持对触发防护策略的请求执行拦截、告警、跳转、放行的处理动作。处理动作为跳转、放行则无需配置触发条件;
 - 统计粒度:静态 cookie/IP+UA/IP;
 - 触发条件。达到触发条件的请求将对其执行处理动作,并支持配置处理动作持续时长(触发规则后的惩罚时间)
- 2) 记录异常。针对人机识别挑战失败的请求
 - 处理动作。支持对触发防护策略的请求执行拦截、告警、跳转、放行的处理动作。处理动作为跳转、放行则无需配置触发条件;
 - 统计粒度: 静态 cookie/IP+UA/IP;
 - 触发条件。达到触发条件的请求将对其执行处理动作,并支持配置处理动作持续时长(触发规则后的惩罚时间)

*人机识别: 🛑
开出后,将会对不同将中域下发人机能战频识。人机能战逝过下发达代码捕获用户操作行为,如果用户设有通过挑战,则认为温趣虫。
* 验证有效期①: 7200 秒
超时异常 记录异常
* 处理动作: 🧕 拦截 💿 告警 💿 跳枝 💿 放行
41 ○ AU+41 ○ LO→68 ○ 2004 HIGE
* 触发条件: 有效期后的 1 时 ~ 之内,第 10 个验证失败的请求开始执行处理动作。动作持续 10 分 ~

阈值限制

功能介绍:防止攻击者盗用合法 cookie 进行大量请求,限制不同粒度的访问速率。

配置介绍(支持最多配置5个条件,多个条件为或关系)

- 处理动作:支持拦截、告警、关闭
- 统计粒度: IP/跳转 cookie/静态 cookie
- 触发条件:达到触发条件的请求将对其执行处理动作,并支持配置处理动作持续时长(触发规则后的惩罚时间)



爬虫陷阱

功能介绍:即在页面里面嵌入不可见链接,正常浏览器不可见;当访问到达设定的拦截深度 时,认为是爬虫行为并支持设置防护策略;

配置介绍(支持最多配置5个条件,多个条件为或关系)

- 防护开关: 支持拦截、告警、关闭
- 统计粒度: IP/IP+UA/静态 cookie
- 防护范围: 支持配置您要防护的请求范围, 支持匹配字段为 PATH、REQUEST_URI、 URI

通用配置	爬虫烙阱: 爬虫烙阱	开启后,会在页面里面嵌入不可见链接,正常浏览器	不可见;当访问到达设定的拦截深度时,认为是爬虫行为						
特性挑战	* 防护开关:	* 防P开关: ④ 关闭 ◎ 监控 ◎ 拦截							
阈值限制	* 始计物策 ④ 目 ● 11 ● 11 ● 11 ● 11 ● 11 ● 11								
爬虫陷阱	-70FT1828-								
	*防护范围:	匹配字段	逻辑符号	匹配内容	操作				
		PATH ~			删除				
		※ 10 还可以添加4条, 数多6条(多个条件为且的逻辑)							
		新 细 还可以添加4条,最多5条(多个条件为或的逻辑)							

3.3.8 证书管理

简介

客户在证书管理模块可以上传证书,查看证书详情、删除证书。

新增证书

1、登录边缘安全加速平台控制台, 在左侧导航栏中选择【安全与加速】—【证书管理】, 单击【新增】按钮;

2、您需要填写证书备注名、证书公钥以及证书私钥。其中公钥和私钥支持 PEM 格式。填写 完毕后,点击"确定提交"按钮。

0	请上传证书(请留意证书有效期)。 目前只支持PEM格式,其他格式请前往 该站点转换。	
*证书备注名	请输入证书备注名	
*证书公钥(PEM格式)	请输入证书公钥	
* 证书私钥(PEM格式)	请输入证书私钥	

查看证书

1、登录边缘安全加速平台控制台, 在左侧导航栏中选择【安全与加速】—【证书管理】, 单击证书列表【详情】查看证书;

2、可查看证书有效期;

↓ 证书管 HTTPS为C	<mark>7理</mark> DN的网络内容传输提供了更好的原源,客户颁在	极速访问内容的同时,可以更安全有效地浏览R	3站内容。				十派加自有证书
关键词:	证书编注名 ~	创建时间: 日 开始日期 至 《	惊日期	ł			
序号	证书备注名	证书通用名称	证书品牌	颁发时间	到期时间	创建时间	操作
1				2022-02-17 15:18:53	2032-02-15 15:18:53	2023-03-17 10:31:11	洋橋 翻除
2		10000	1000	2023-03-16 08:52:09	2024-03-15 08:52:09	2023-03-16 11:04:24	洋情 删除
3			1000	2023-03-15 18:05:52	2024-03-14 18:05:52	2023-03-15 18:07:42	洋橋 翻除
4				2023-02-15 14:18:16	0 2023-03-17 14:18:16	2023-03-15 17:15:20	洋情 删除
5				2022-02-15 08:00:00	9 2023-03-19 07:59:59	2023-03-15 17:14:07	洋橋 劉餘

证书删除

1、登录边缘安全加速平台控制台, 在左侧导航栏中选择【安全与加速】—【证书管理】, 单击证书列表【删除】删除证书;

2、删除证书的前提是,该证书没有关联域名;

3.3.9 刷新预取

缓存刷新用于客户对源站内容发生了变化的内容进行刷新,以便 CDN 缓存能尽快保持和 源 站内容的一致性。缓存刷新应该在源站内容发生了变化之后再提交刷新,避免没有刷新 成 功。 CDN 提供内容分发网络,常规下为最终用户访问后回源拉取,但部分内容文件较大, 且如 果访问量较大情况下集中回源对源站有一定压力,因此提供给客户预取功能,在用户 访问 前将文件预取到二级缓存节点上后发布访问下载路径,减少回源时间,规避源站影响。 注意:大批量的缓存刷新可能会引发高并发回源,如果源站出口带宽较小,建议分多次小批 量操作。

G 边缘安全加速平台 AccessOne	■ 刷新子分取 创建期新成数取任务,适用于测动资源更新和发布、违规资源清理、域名配置变更,降低源站压力提升用户体验。	十的課任等
○ 服务概告	URL 刷新 目录刷新 正则刷新 URL 预取	
	洗择时间 (> 2021.01.20.00.00.00 至 2021.01.20.23.49.59 提索条件 语给入主要结么否询	行条状态 请选择任务状态 >>
	編号 内容 提交时间	状态
14.55		
城口自注		
业 节 昌 建		
安主报表		
站点统计 🗸	暂无数据	
刷新预取		
≥。零信任服务 ~		
回。开发者平台 🗸		
🔄 运营管理 🛛 🗸		
③ 计费详情	共0条 10条/页 > 前往 1 页	
G 边缘安全加速平台	刷新预取 创建期新成组取任务、适用于课站资源更新和发布、违规资源清理、域名高置变更、降低源站压力提升用户体验。	+ (0)8(59)
	创建刷新预取任务	×
ᢙ服务概览		
○ 安全与加速	选择时间 ② 2023.4 「RFT Pack+」 Unit about 1 Unit about 1 してに about 1	任务状态 请法择任务状态 > 重面
概览	新考 內容 "任务内容. 1.CON节点的提存不定时更新,当您的游站内容更新后,需要用户我取到最新的资源,可以通过提交刷新任. 3.上和信仰的医师常常常的变形。"但你说我们们需要找到了需要的点。要你从多少点都是是你。	秋态 务:
域名管理	2. 六風道明動解開起可能加引後還开來已過,如果那些面口性素吸小,這次方享必小風重開行。 8. 每条URL一行(固年操行)一次最多50行,并注意区分URL中的字母的大小写,影新任务一般5-10分钟生效。 	
证书管理	请输入愿受局新的完整URL,每个ur1要以http://或https://开头,urhttp://www.etyun.com.c n/images/test.jpg,每条UR_一行(回车换行),请注意区分URL中的学校的大小写,错误的大小	
安全报表	写会导致副新无效:	
站点统计 🗸		
刷新预取		
🖳 零信任服务 🗸		.4
🖳 开发者平台 🗸		
□ 运营管理 ∨		
③ 计费详情	共0条 10条页 > 〈 1 > 前往 1 页	
这缘安全加速平台 AccessOre	刷新行效取 创建期新成绩和化务,适用于提达资源更新和收布,违规资源清理,或名配置变更,降低源达压力提升用户体验。	+ 81853
	创建刷新预取任务	<
局 服务概览		
	选择时间 ② 2023-4 FFF天王	任务状态は高速経営状态・ソークを抑
概览	第1 CON书点的是存不定时更新,当您的凝结内容更新后,需要用户获取到最新的资源,可以通过提交到新任务 2、大量数的制度得不定时更新,当您的凝结内容更新后,需要用户获取到最新的资源,可以通过提交到新任务 2、大量数的制度得过可能会引发高并发行源。如果发出口口需发现小、建设什么办小量是操作:	4464
域名管理	3. 每条URL一行(回车操行)一次量多50行,并注意区分URL中的字母的大小写,本功能自动描述子目录,无 雷填写下级目录,则新任务一般5~10分钟生效;	
证书管理	4.域名数认不应分协议概存,目录推送需统一规交http协议目录才能生效;如域名配置区分协议版存,需按实计制新需求分别规交目录制新。	
安全报表	请输入造要刷新的目录,目录要以http://或https://开头和/结尾。如http://www.ctyun.com.c n/immga/、每条目录一行(回车换行)。请注意区分IRU中的字母的大小写。错误的大小写会导致 IPWIIII和	
站点统计	49100.4233	
刷新预取		
回。零信任服务 ~		
□ 开发者平台 ~		
□ 运营管理 ∨	取消 电应用交	
④ 计费详情	共0条 10条页	



3.3.10 安全报表

简介

本节介绍安全与加速服务的安全报表模块,支持查看六个月内、最长时间跨度为一个月的已 防护域名的安全报表。主要内容包括 Web 安全报表、DDoS 安全报表以及 CC 安全报表,您可 以在这里查看实时或历史的攻击防护情况。

Web 安全报表

Web 安全报表模块为用户统计 Web 应用安全相关的分析与统计,用户可在查询栏,指定要分析的域名及时间范围。

统计模块主要包括:

- 总请求数
- Web 攻击次数
- 拦截次数
- 攻击源个数
- 攻击网站数
- Web 攻防趋势:支持查看总请求数、总攻击次数、拦截次数、告警次数的访问趋势,并
 支持选择时间粒度为5分钟、1小时、1天,默认时间粒度为5分钟;
- 攻击类型分布:支持查看域名遭受的攻击类型占比与攻击次数,并支持选择攻击类型, 查看域名受到该类型的攻击次数排行;
- 攻击 IP TOP: 支持查看发起攻击次数最多的源 IP 排行,支持获取攻击 IP、IP 归属地、 攻击次数、占比等字段信息;
- 受攻击情况: 支持查看受到攻击次数最多的域名及 URL 排行情况, 支持获取域名/URL、 受攻击次数、占比等字段信息;
- 全国攻击分布:支持查看全国的攻击分布情况,不同颜色代表不同范围的攻击次数。并
 支持查看攻击地区排行情况

	5平台 B#	Q. 当前工作区:安全加速 > 个人中心 💦
	▲ > 安全与加速 > 安全版表	
AccessOne	↓ 安全报表 支持自義六十月94, 最快时期回题力──十月的已起99年会回来	
日間服券概約	域名接入	
● ⑤ 安全与加速 へ	已防护域名 30个 未防护域名 11个 开启地炉	
• 概先	Web安全报表 DDoS安全报表 CC安全报表	
域名管理	162 All y BHGT ALL HEAL HEAL HEAL HEAL ALL CHUY	
证书管理		
安全报表	会 总请求数 (Web攻击次数 // 単載次数 // 攻击源个数	(攻击网站数
站点统计 ~	· · · · · · · · · · · · · · · · · · ·	🥯 1个
刷新预取	Web攻防趨势 ##2 (20)	町同職粒度 1天 🗸 ⊻
IPv6检测	次数 -〇- 忠康末数 -〇- 忠敬太政 -〇- 臣敏次数 -〇- 臣敏次数 -〇- 臣敏次数	
□ 零信任服务 ~		
② 边缘接入服务	2,000	
回 开发者平台	1,500 2023-04-11 00:00:00 2023-04-11 00:00:00 金属素化 2,016	
◎ 运营管理 ~	1,000 ● 急攻击次数 198 ● 三脳次数 0	
⑧ 计费详情	500 0 白質次数 0	
		······································
	2023-04-06 0000000 2023-04-10 0000000 2023-04-14 0000000 2023-04-18 0000000 2023-04-22 0000000 2023-04-26 000000 202	023-04-30 00:00:00 2023-05-04 00:00:00

DDoS 安全报表

DDoS 安全报表模块为用户统计 DDoS 网络层攻击相关的分析与统计,用户可在查询栏,指定要分析的时间范围。

统计模块主要包括:

- 攻击事件数:展示 DDoS 网络层攻击事件数,单位:次
- DDoS 防护峰值:展示攻击带宽峰值,单位:kbps
- DDoS 攻击峰值时间:展示 DDoS 防护峰值对应的时间
- 攻击趋势:展示总攻击、SYN Flood、ACK Flood、UDP Flood、ICMP Flood及Other的 攻击趋势,并支持拖动时间轴调整分析事件范围
- 攻击类型分布:展示攻击类型的占比
- TOP 攻击源 IP: 根据攻击峰值大小对攻击源 IP 进行排序,展示攻击源 IP、IP 归属地、 运营商、攻击峰值字段信息;该功能默认关闭,可提交工单进行开启。
- 全国攻击分布:展示 TOP 攻击源 IP 的城市分布以及攻击来源地区的排行;该功能默认 关闭,可提交工单进行开启。

 A state i de la sete de la sete		云平台 谜:: Q 当前工作容: 安全加速 ∨ 个人中心
	9	▲ > 安全与加速 > 安全很表
Bit BARREN Statistic In Statistic Statistic I	 B 经经济规模安全加速学台 AccessOne 	■
© 오 소 나 내 # • ▲ 2014 # • ▲ 2014 # • ▲ 2014 # • ● ▲ 2014 # ● ▲ 2014 # ● ▲ 2014 #	88 服务概览	Here J
#S Websitikk DoSSelitikk CSakitk #SR	B ⑤ 安全与加速 ^	4x4130X このか 未起炉場名 11个 月日回20 ¹
Market	B 概览	Web安全服表 CC安全服表 CC安全服表
u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge u tagge	域名管理	
Verset 02 mm 02 mm <t< th=""><th>证书管理</th><th></th></t<>	证书管理	
Modify Read Docs559*441 Pocs559*441 Pocs59*59*451 Pocs59*59*59*59 Pocs59*59*59*59 Pocs59*59*59*59*59 Pocs59*59*59*59*59	安全报表	0.2 mm
вклад I x±abs x I x±abs I x±abs I x±abs I x±abs x I x±abs I x±abs <t< th=""><th>站机税计</th><th>改進専作数 通 D0xs防が場面 2023/01-17 D0xs防が場面 D0xs防が場面 D0xs防が場面</th></t<>	站机税计	改進専作数 通 D0xs防が場面 2023/01-17 D0xs防が場面 D0xs防が場面 D0xs防が場面
Indexist Indexist Indexist I	刷新预取	
I \$\frac{1}{2}\$ \$\frac{1}{2}\$\$ \$\frac{1}{2}\$\$\$ \$\frac{1}{2}\$	IPv6检测	文面絶労
(3) 边缘队 服务 150.00% ps (3) 边缘队 服务 150.00% ps (3) 边缘队 服务 120.00% ps (3) 边缘体 mps 100.00% ps (3) 边缘体 mps 0.00% ps (3) 边缘 mps 0.00% ps (3) Us 0.00% ps <th>□3 零信任服务 ~</th> <th>Back - Shirthead - Alkertead - Multi-tead - Multi-te</th>	□3 零信任服务 ~	Back - Shirthead - Alkertead - Multi-tead - Multi-te
田 开发者中台 120.00% ps 日 万次者中台 2023-04-17 1857.00 ● 出版: 第48.46% ps 90.00% ps 0.00% ps ● 注页管理 90.00% ps 0.00% ps 0.00% ps ③ 注页管理 90.00% ps 0.00% ps 0.00% ps ③ 注页管理 90.00% ps 0.00% ps 0.00% ps ③ 近常管理 0.00% ps 0.00% ps 0.00% ps ③ 近常管理 0.00% ps 0.00% ps 0.00% ps ③ 近日: 0.00% ps 0.00% ps 0.00% ps ○ 10.00% ps 0.00% ps 0.00% ps 0.00% ps ○ 201.00% ps 0.00% ps 0.00% ps ○ 201.00% ps	(1) 边缘接入服务	150.00/tops
© ISTNET 90.00Mops	同开发表图台	2023-04-17 16:37:00 120.00/https
Comps Comp Comps		90.00%ps
33.00% tps 33.00% tps 2023 04 10 (4010) 2023 04 10 (4010) 2023 04 10 180220 2023 04 17 080100 2023 04 20 222000 2023 04 20 15500 2023 04 20 155700 2023 05 85 855600		60.00M/aps
	(1) 11 921+10	30.0M/tps
		0.00001/2 0.00001/2 0.0000 2002-04-10 18:02.00 2002-04-17 08:01:00 2002-04-20 22:00:00 2002-04-20 11:59:00 2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-2002-04-20-20-20-20-20-20-20-20-20-20-20-20-20-

CC 安全报表

CC 安全报表模块为用户统计 CC 防护相关的分析与统计,用户可在查询栏,指定要分析的域 名及时间范围。

统计模块主要包括:

- 攻击事件数:展示 CC 攻击事件数
- CC 攻击峰值
- 峰值取值时间
- CC 攻击网站数:展示被攻击的网站数量
- 攻击趋势:展示请求量 QPS 趋势
- TOP 攻击域名:展示攻击最多的域名排名,按照请求数进行排序

- TOP 攻击源 IP: 展示 TOP 攻击源 IP 及攻击源 IP 的区域、运营商及攻击次数
- 全国攻击分布:展示 TOP 攻击源 IP 及攻击源 IP 的区域、运营商及攻击次数

	平台		澄素	Q 当前工作区:安全加速 > 个人中心	2
Ð	ᢙ > 安全与加速 > 安全报表				
B CALL UN 文王加速于日 AccessOne	■ 安全报表 支持面看六个月内、最长时间商意为一个月的已防护场名的安全探表				
88 服务概念	域名接入				
B ⑤ 安全与加速 ^	已防护域名 30个 未防护域名 11个 开启防护				
D 根览	Web安全报表 DDoS安全报表 CC安全报表				
域名管理					
证书管理	NK名 2010 ~ 时间 今大	近3大 近/大 近16大 近一个月			
安全报表	4 *	12 OPS	2023-04-11 16:11:00	1	
站成统计	攻击事件数	CC攻击峰值	峰值取值时间	CC攻击网络数	
刷新预取	攻击趋势			2	ź.
IPv6检测	QPS		-O- QPS線值常吃		
L2 零信任服务 ~	12				
@ 边缘接入服务	10				
园 开发者平台	6				
◎ 运营管理 ~	4				
④ 计费详情					
	2023-04-06 14:02:00 2023-04-08 15:48:01	2023-04-10 17:34:00 2023-04-12 19:20:00	2023-04-14 21:06:00 2023-04-16 22:52:00 2023-04-19 00:38:00	2023-04-21 02:24:00 2023-04-23 04:10:00	
	(

3.3.11 站点统计

3.3.11.1 用量查询

功能说明: 该模块可供客户查看带宽流量、回源统计、请求数、命中率、状态码等指标。 **操作指引:** 登陆天翼云边缘安全加速控制台,进入【站点统计】-【用量查询】功能模块, 即可通过筛选项进行组合查询带宽流量、回源统计、请求数、命中率、状态码等指标。筛 选项包括产品类型、域名、运营商、地区、时间。

1、带宽流量

界面中展示的是您所选范围、域名、运营商、地区、时间范围内的带宽和流量统计图表,可 通过切换"带宽"和"流量"的按钮查看带宽和流量图,带宽图中包括了带宽峰值和 95 带宽峰值; 流量图中展示总流量。同时会给出查询时间范围内每日总流量、带宽峰值、峰值时间点、回 源带宽峰值、回源峰值时间点。点击"导出 CSV"可以将选定条件的查询数据导出为 CSV 格式 的表。

边缘安全加速平台 AccessOne	■ 用量查询 支持一年内、最长时间跨度为一个月的用量数据查询。			
 ○ 服务恒進 ◇ 安全与加速 ◇ 仮応 城名管理 延子管理 		C5時 PV/UV 地区运营商 Unit/FigTin → 全部時区 → Unit/FigTin → 全部時区 → Unit/FigTin → 全部時区 →	SETTEMBRE: 0.00bes	
安全报表 站点统计 ~ 用量造词 热门分析 用户分析	Hrggerigg 0.000ps 0.05-00-0.050-00 High Maps 1 0.8 0.6 0.4 0.2 0 0.520 01-20 03-20 0.510 02-20 0.510 02-20 0.51	01-20 01-20 01-20 01-20 01- 05-50 07-30 09-10 10-50 12-	0 01-20 01-20 03-20 03-20 0 14-10 15-20 13-20 03-20 0 14-10 15-20 17-30 15-10	2 1 1 0 Hercsv
First DAR Set Dar	日間 0 2023-03-20	А⊐деща(ме) 0.00	启带宽峰值(Mbps) 0.00	岸崎価労団点 2023-03-20 23:55:00

2、回源统计

界面中展示的是您所选范围、域名、运营商、地区、时间范围内的回源带宽和回源流量统计 图表,可通过切换"回源带宽"和"回源流量"的按钮查看回源带宽和回源流量图,回源带宽图 中包括了带宽峰值和 95 带宽峰值;回源流量图中展示了总回源流量。点击"导出 CSV"可以 将选定条件的查询数据导出为 CSV 格式的表。

Ge 边缘安全加速平台 AccessOne	■ 用量查询 支持一年內、最长时间跨度为一个月的用量数据查询。			
☆ 服务概覧	带宽流量 回源统计 请求数 命中率 状	你的 PV/UV 地区运营商		
🔍 安全与加速	范围 安全与加速 ~ 请选择域名	~ 9.000 ~		
概览	时间 今天 昨天 近7天 近30天 自定义 🗇	993		
域名管理	回游市方 回源法量			
证书管理	带宽峰值: 0.00bps 2023-03-20 23:55:00		95带宽峰值: 0.00bps	
安全报表	mtiz: Mbps 1			0110
站点统计 ~	0.8			
用量查询	0.4			
热门分析	0.2			
用户分析	03-20 03-20 03-20 03-20 00:00 01:40 03:20 05:00	03-20 03-20 03-20 03-20 06:40 08:20 10:00 11:40	03-20 03-200	8-20 03-20 03-20 0:00 21:40 23:20
刷新预取	(7) 30(40(2) WHO			7
🔍 零信任服务 🗠	LEY VICE HE BY SPE			
🔃 开发者平台 🗸	日期 🗢	回源流量值(MB)	回源带宽峰值(Mbps)	回源峰值时间点
同运营等期	2023-03-20	0.00	0.00	2023-03-20 23:55:00
wanad v				
② 计费详情				

3、请求数

界面中展示的是您所选范围、域名、运营商、地区、时间范围内的请求数和 QPS 统计图 表, 可通过切换"请求数"和"QPS"的按钮查看请求数和 QPS 图,请求数图表中包括了 总请求数、 动态 http 请求数、动态 https 请求数、静态 http 请求数、静态 https 请求 数, QPS 图表中 包括了总 QPS、动态 http QPS、动态 https QPS、静态 http QPS、静态 https QPS,点击"导 出 CSV"可以将选定条件的查询数据导出为 CSV 格式的表。

M Media Maximum Mining Market <	G 边缘安全加速平台	▶ 用量查询 支持一年内、最长时间跨成为一个月的用量数据查算。					
ALC NU Image: Single Sing	⑦ 服务概览 ② 安全与加速	带放流量 回源统计 清末收 命中 范围 请法师加强类型 > 请法所场行	率 状态码 PV/UV 5 、 読みがに対応	地区运营商			
	概范 域名管理	協議 は 新校					
Right A B/D/D/F A <	证书管理 安全报表 站点统计 ~	miQ: 2% 1 0.8	-〇- 忠靖宋数 -〇	→ 静态http请求数 -O- 动态http请求数	O- 静态https请求数: ──	100	6 1 1 0
用デザボ	用量查询 热门分析	0.4 0.2 0.5.20 0.5.20 0.5.20	03.20 03.20 0	3.20 03.20 03.20	03-20 03-20 03-20	03-20 01-20 03-20	03-20
事業 日期 自連次 静参htp直求数 动参htp直求数 動参htp直求数 動参htp直求数 動参htp直求数 动参htp直求数 の参htp直求数 の参htpa素数 の <htpa素< th=""> の<h< th=""><th>用户分析 刷新预取</th><th></th><th>0500 0640 0</th><th>820 1000 11340</th><th>15:20 15:00 16:40</th><th>1820 2000 21340</th><th>23:20</th></h<></htpa素<>	用户分析 刷新预取		0500 0640 0	820 1000 11340	15:20 15:00 16:40	1820 2000 21340	23:20
回应管数理 1 2005000 0 <t< th=""><th> 民 零信任服务 ~ 民 开发者平台 ~ </th><th>序号 日期</th><th>总请求数</th><th>静态http请求数</th><th>动态http请求数</th><th>静态https请求数</th><th>动态https请求数</th></t<>	 民 零信任服务 ~ 民 开发者平台 ~ 	序号 日期	总请求数	静态http请求数	动态http请求数	静态https请求数	动态https请求数
	 □ 运营管理 ○ 计费详情 	,, 汇总请求数	0	0	0	0	0

4、命中率

界面中展示的是您所选范围、域名、运营商、地区、时间范围内的命中率。点击"导出 CSV" 可以将选定条件的查询数据导出为 CSV 格式的表。

会 边缘安全加速平台 AccessOne	月還宣句 文持一件內,最於時間成为一个月的用量數面面與。
🗟 服务概览	帝変流量 回源统计 请求数 <u>30中</u> 年 状态码 PV/UV 地区运营商
○ 安全与加速 へ	128 AANTARAA V MANTARA V 12000 V
概览	1992 Warmbaces v Warmbaces v
域名管理	时间 今天 非天 近7天 近30天 白菜又四 角浜
证书管理	<u>发生命十年</u> 男子由十年
安全报表	流量命中寧峰值: 100% 2022-03-20 23 55:00 単位:% としてつ
站点统计	100
用量查询	60
热门分析	40 70
用户分析	0 01.20 01.20 01.20 01.20 01.20 01.20 01.20 01.20 01.20 01.20 01.20 01.20 01.20 01.20 01.20 00.00 01.40 01.40 05.40 07.20 07.10 11.00 11.20 11.40 11.40 11.20 01.20 01.20 01.20 01.20
刷新预取	
🖳 零信任服务 🚽 🗸	
🖳 开发者平台 🚽	
回 运营管理	
③ 计费详情	

5、状态码

界面中展示的是您所选范围、域名、运营商、地区、时间范围内的状态码统计图表,可通过 切换"所有状态码"、"2XX"、"3XX"、"4XX"、"5XX"的按钮查看不同状态码的图表,并显示查 询时间范围内的总状态码量,同时展示状态码占比表和状态码占比饼图。点击"导出 CSV" 可以将选定条件的查询数据导出为 CSV 格式的表。

G 边缘安全加速平台 AccessOne	■ 用量量的 235-4494、最佳时间的成分→个月的用量数量高级。	
 ・ 服务概定 ・ ・ ・	(中広花屋 回遊社) 請求数 企中年 代表前 PV/UV 地区道音商 関連 前点目200天光 ジ 前点目146 ジ (前点目50天点) ジ 金田県区 関連 今天 前天 前子天 前30天 前22 回 005 修成式650 2xx 3xx 4xx 5xx 防枕売用量: 0次 車位: 次	8 55 0
刷新预取		0
🖳 零倍任服务 🚽	状态码占比表统计	
回。开发者平台 🗸	状态明名称 状态明文数 单位:次) 占比(单位:%)	
□ 运营管理 ↓	智无规调	
⑦ 计费详情	教泰明占比树墨锦计	

6、PV/UV

PV 即页面浏览量,统计响应状态码非 0 且小于 400,默认类型包括:htm、html、php、asp、shtm、shtml、aspx、xml、xhtml、xsl、cfm、htx、htmls、phtml、jsp、 perl、hph3、txt、wml、 lhtml、pl、 cgi、 cfm 、 acgi 、 srch 、 qry 的 页 面 请 求 数, 结 尾 以 "/" (例 如 http://www.test.com/abc/)或找不到"."的 (例 如 http://www.test.com/abc)也计入 PV。 UV 即 独立访客,相同 IP 的多次访问只能算 1 个独立访客,不同 IP 的多次访问算为多个 独立访客。控制台的统计分析栏可展示您所选范围、域名、运营商、地区、时间范围内的 PV 和 UV 信息,每 5 分钟统计一次 5 分钟内的总 PV 和总 UV 值,如下图所示,展示查询区 间的 PV 和 UV 趋势图,并显示查询区间的 PV/UV 峰值、PV/UV 总量。同时提供按天粒 度统计的 PV 和 UV 数据。

公 边缘安全加速平台 AccessiOne	▶ 用量查询 支持一年內,量长时间跨意为一个月的用量数据新闻。		
☆ 服务概覧	带宽流量 回源统计 请求数 命中率 状态码 14/10/ 地区运营部		
○ 安全与加速 ^	范围 请选择加速失望 ~ 请选择经8 ~ 全部地区 ~		
概览	时间 今天 昨天 近7天 近30天 自定义言 前院		
域名管理	PV UV		
证书管理	PV峰值(1小时统计): 0次	PV总量: 0次	
安全报表	舉位:次		8 1 1 0 O
站点统计			
用量查询			
热门分析			
用户分析	Ā		
刷新预取			
🖳 零信任服务 🗸	天粒度数据统计		
回。开发者平台 ~	序号 日期	浏览量(PV)	访问量(UV)
		智无数据	
wannie V			
④ 计费详情			

7、地区运营商

控制台的统计分析栏可展示您所选范围、域名、运营商、地区的用量排名, 默认按照 峰值 带宽降序排列, 也可点击流量、请求数后面的箭头更改为使用流量或请求数排行。

G 边缘安全加速平台	■ 用量查询 支持一年内、最长时间跨度为一个月	的用量数据查询。					
☆ 服务概覧	带宽流量 回源统计	请求数 命中率 状态码 PV,	ロマ 地区运营商				
🔍 安全与加速 🔷	范围 请选择加速类型	→ 読み詳細名 → 読み詳	言言語 ~ 全部地区				
概览	时间 今天 昨天 近	7天 适30天 自定义目 查询					*
域名管理	地区	峰值带宽(Mbps) 🌣	流量(MB) ≑	流量占总比	请求数 ◎	请求数占总比	
证书管理	中国其他	0.00	0.00	0	0	0	
安全报表	北京	0.00	0.00	0	0	0	
站占统计	天津	0.00	0.00	0	0	0	
SUMBER	河北	0.00	0.00	0	0	0	
用量查询	山西	0.00	0.00	0	0	0	
热门分析	内蒙古	0.00	0.00	0	0	0	
用户分析	辽宁	0.00	0.00	0	0	0	
国銀行石作用2	吉林	0.00	0.00	0	0	0	
NDIN12SOAK	黑龙江	0.00	0.00	0	0	0	
回、零信任服务 ~	上海	0.00	0.00	0	0	0	
🖳 开发者平台 🚽	江苏	0.00	0.00	0	0	0	
□ 运营管理 ~	浙江	0.00	0.00	0	0	0	
《 计数详续	安徽	0.00	0.00	0	0	0	
U H MITH	福建	0.00	0.00	0	0	0	
	江西	0.00	0.00	0	0	0	

3.3.11.2 热门分析

功能说明: 支持三个月内、最长时间跨度为一个月的热门数据统计,包括 TOP 100 URL、 TOP 100 回 源 URL、热门 Referer、热门域名、TOP 客户端 IP 统计,可根据访问次数优先和 流量优先 两种维度的排列。并支持数据下载导出,表格内容与页面一致。 **操作指引:** 登陆控制台,进入【统计分析】-【热门分析】功能模块,即可选择产品类型、 域名、状态码、时间范围,按照"流量优先"或"访问次数优先"的策略查询热门排行。

1、热门 URL

热门 URL 可展示 TOP100 的 URL 及对应的流量、流量占比、访问次数、访问占比。选择 "流 量优先"时按照流量大小排序,选择"访问次数"时按照访问次数排序,并支持表格导出。

C 边缘安全加速平台 AccessOne	执门分析 支持三个月内、最长时间跨成为一个月的热门数据统计。	
	执门URL (回源) 执们Referer 域名排行 TOP客户端IP 请法择加速失型 > 请法择状态码 > (濃度优先) 访问次数优先	
★ 安全与加速 概览	今天 昨天 〇 2023-03-19 00:00:00 至 2023-03-19 23:59:59 創刊	<u>+</u>
域名管理	排行 URL	
证书管理	智无数据	
安全报表		
站点统计 ~		
用量查询		
热门分析		
用户分析		
刷新预取		
🖳 零信任服务 🛛 🗸		

2、热门 URL (回源)

热门 URL (回源) 可展示 TOP100 的回源 URL 及对应的流量、流量占比、访问次数、访问 占 比。选择"流量优先"时按照流量大小排序,选择"访问次数"时按照访问次数排序,并 支持表 格导出。

这缘安全加速平台 AccessOne	执行分析 文列二个月内。最长时间跨度为一个月的热门数据统计。
ᢙ服务概览	热门URL 热门URL (回源) 热门Referer 域名排行 TOP客户端IP
○ 安全与加速	请选择加速类型 > 请选择城名 > 请选择状态码 > 流量优先 访问次数优先
概览	今天 昨天 ③ 2023-03-19 00:00:00 至 2023-03-19 23:59:59 ④ 查询
域名管理	排行 URL 流量 流量占比(%) 访问次数 访问占比(%)
证书管理	暂无数据
安全报表	
站点统计	
用量查询	
热门分析	
用户分析	
刷新预取	
🗟 零信任服务 🗸	

3、热门 Referer

热门 Referer 可展示 TOP Referer 及对应的流量、流量占比、访问次数、访问占比。选择"流量优先"时按照流量大小排序,选择"访问次数"时按照访问次数排序,并支持表格导出。

边缘安全加速平台 AccessOne	Ⅰ 执门分析 实持三个月内、最长时间跨度为一个月的热口数据统计。	
☆ 服务概览	热门URL 热门URL (回源) <u>热门Referer</u> 域名排行 TOP客户端P	
会安全与加速 ~		±
域名管理	排行 Referer 流量 流量占比(%) 访问次数 访问占比(%)	
证书管理	暂无数据	
安全报表		
站点统计 人		
用量查询		
热门分析		
用户分析		
刷新预取		
◎2. 零信任服务 ~		

4、域名排行

域名排行可将域名按照"流量"或者"访问次数"进行排序,同时展示域名对应的流量、流量占比、访问次数、访问占比。并支持表格导出。

这缘安全加速平台 AccessOne	热门分析 支持三个月内、最长时间跨度为一个月的热门	发掘统计。					
 · 服务概览 · · ·	熱了URL 熱了URL (回源) 請选择加速失型 ~ 3	热门Referer <mark>域名排行</mark> 选择域名 ~	TOP客户端IP 流量优先 访问次数优先				
概览	今天 昨天 近7天 近30天 排行 城名	 2023-03-19 00:00:00 3 法書 	至 2023-03-19 23:59:59 溶量占比(%)	查询	能们在 只十交日	访问次数	<u>*</u>
域名管理 证书管理	LEDAN ELER	D'ILANN.	新 新 日(13) 暂无数据	TO ACCORDING	*** LEUN 3 (K)	ARV/C*IC#	
安全报表							
站点统计 へ							
热门分析							
用户分析							
刷新预取							

5、TOP 客户端 IP

TOP 客户端 IP 可将客户端 IP 按照"流量"或者"访问次数"排序,并展示客户端 IP 对应 的流量、 流量占比、访问次数、访问占比。并支持表格导出。

公 边缘安全加速平台 AccessOne	■ 執门分析 支持三个月内、最长时间跨度为一个月的热门数据统计。	
☆ 服务概览	热门URL 热门URL (回源) 热门Referer 域名排行 TOP答户端P	
○ 安全与加速 ~	→ 満造得加速発型 > 」 満造得域名 > 」 请选择状态码 > 〕 ★館地区	· 流量优先 访问次数优先
概览	今天 昨天 近7天 近30天 〇 2023-03-19 00:00:00 至 2023-03-19 23:59:59 查询	<u>*</u>
域名管理	排行 IP	流量访问次数
证书管理	暂无数据	
安全报表		
站点统计 ~		
用量查询		
热门分析		
用户分析		
刷新预取		
🖳 零信任服务 🗸		

3.3.11.3 用户分析

功能说明: 用户分析可展示用户的区域分布、运营商分布、独立 IP 访问数。并展示每个区域/运营商的 带宽、流量、访问次数。

操作指引:登陆天翼云控制台,进入【统计分析】-【用户分析】功能模块,即可选择产品 类型、域名、时间范围进行查询。并可以切换带宽、流量、访问次数等指标进行展示。如 下图:

→ 边缘安全加速平台 AccessOne	用户分析					
⑥ 服务概览 ※ 安全与加速	范囲 全部総名 ジョン ヴィー 時天 近7天 近30天 自定文目 255 ざた河田内なびは公在 ■ 100万円 10					
概览		用户所在区域	带宽bps			
域名管理	MICI -	中国其他	0.00			
证书管理	and	北京	0.00			
安全报表	10日 - 10日 - 10日 日本日 - 日本日 -	天津	0.00			
ALC MARKED	南市田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	河北	0.00			
站点统计		山西	0.00			
用量查询		内蒙古	0.00			
热门分析	24 FB / 15 / 167	辽宁	0.00 ±			
用户分析	低	第1页/共5页 《 >				
IN OF YELDS	▲ 独立IP访问数 坐	访问运营商分布 蒂宽 流量 访问次3				
MINTIKAX	独立IP访问峰值(1小时统计): 0次 日活跃IP总量: 0次	用户所在区域	带宽bps			
🖳 零信任服务 💛	单位:次 1		智无数编			
🗟 开发者平台 🗸		10				
山 运营管理 🌱						

1、访问区域分布

根据用户所在区域,分别展示每个省份的带宽、流量、访问次数,并在地图中用不同的颜色 进行展示。

2、访问运营商分布 根据用户所属运营商,分别展示每个运营商的带宽、流量、访问次数信息。

3、独立 IP 访问数 可展示独立 IP 访问数的趋势图,并展示独立 IP 访问峰值和日活跃 IP 总量。

3.3.12 IPv6 检测

简介

支持 IPv6 支持度检测功能,能够针对 IPv6 域名解析、网站首页 IPv6 访问、网站二级/三级 链接 IPv6 支持度进行检测,并输出检测结果以及改进建议。

检测对象

- 检测网址:可以从域名列表选择需要 IPv6 检测的网址,也可以自定义输入网址,支持 输入域名或 URL 格式;
- 自定义 Host: 支持指定到一个 v6 节点来进行检测

检测项

- IPv6 域名解析: 支持检测域名是否支持 IPv6 解析, 若不支持, 则建议前往域名列表开 启 IPv6 解析功能;
- 网站首页 IPv6 访问: 支持检测网站首页是否支持 IPv6 访问, 若不支持, 则建议开通站 点外链替换功能, 实现 IPv6 访问;

- 网站二级链接 IPv6 支持度:支持检测网站二级链接是否支持 IPv6 访问,若不支持,则
 建议开通站点外链替换功能,实现 IPv6 访问;
- 网站三级链接 IPv6 支持度:支持检测网站三级链接是否支持 IPv6 访问,若不支持,则
 建议开通站点外链替换功能,实现 IPv6 访问

检测次数

不同套餐版本支持的检测次数有所不同。

- 免费版: 支持一个月检测1次;
- 高级版: 支持一个月检测 20 次;
- 企业版:支持一个月检测 30 次;
- 旗舰版:支持一个月检测 40 次

安全与加速-IPv6 检测页面

大阪ご CDN:云平台 提案 Q 当前工作区:安全加速 ∨ 个							
₿							
(#) 	AccessOne	IPv6检测 IPv支持保险测,能够为您输出详细的绘测结果,包括IPv6支持度,不支持IPv6的组很明细等,并支持生成IPv6位测照告					
9	品 服务概览]	检测历史记录			
æ	⑤ 安全与加速 🔷	本月朝余位起灭载: 1次					
۲	概览	* 检测网址 请选择或者输入要检测的网站地址,如域名II的Htps://www.test.com////////////////////////////////////					
	域名管理	自定义Host: 支持填写一个IPv6 host					
	证书管理	32.8Pt合300					
	安全报表						
	站点统计 🗸	0% 安全与加速将为防提供全方位IPV6检测					
	刷新预取						
	IPv6检测	检测项 检测结果					
	『 零信任服务 ~	IPv6號名解析					
	(1) 边缘接入服务						
	🔤 开发者平台	网站首页IPv6访问					

检测历史记录

支持查看历史的检测任务,能够获取任务状态、各项检测结果等信息,并支持点击【查看详 情】查看二三级链接不支持 IPv6 访问的统计报表;支持点击【导出】,将以 excel 的形式 导出不支持 IPv6 访问的链接明细。

安全与加速-IPv6 检测-检测历史记录页面

G	日本語言	CD	N: 云平台				按	_ģ Q	当前工作区:安全	加速… > 个人中心	2
8	(公 道 Ao	IPv6检	》历史记录							×	
e O	88 服务	检测时	间: ③ 2023-04-05 18:28:	31 至 2023-05-05 18:28:31		任务状态: 请选择	2	∨ 提交人: 请选择			
₿	⑤ 安全	重	调清空								
۵	概	序号	检测时间	域名	任务状态	IPv6域名解析	首页IPv6访问	二级链接IPv6支持度	三级链接IPv6支持度	操作	
	域	1	2023-04-27 19:20:59		成功	不支持	不支持	0.00%	0.00%	查看详情 导出	
	ίĬ	2	2023-04-19 14:46:25		失败	不支持	不支持	0.00%	0.00%	查看详情 导出	
	安	3	2023-04-19 09:48:31		失败	不支持	不支持	0.00%	0.00%	查看详情 导出	
	站 風	4	2023-04-18 17:20:53		成功		支持	99.22%	98.27%	查看详情 导出	
	IP	5	2023-04-18 17:02:51		成功	°)	支持	100.00%	99.63%	查看详情导出	
	L ² 零信	6	2023-04-18 16:44:08		戓功	不支持	不支持	0.00%	0.00%	查看详情 导出	
	@ 边缘	7	2023-04-18 16:25:16		成功	不支持	不支持	0.00%	0.00%	查看详情 导出	
	园 开发										

3.4 购买零信任服务

3.4.1 开通边缘安全加速平台

开通天翼云边缘安全加速平台—零信任服务,需首先注册天翼云账户。

开通步骤如下:

步骤 1、注册并登录天翼云 <u>http://www.ctyun.cn</u>

2-1 天翼云官网登录页面



热门产品分类

步骤 2、未实名认证的用户请按提示完成实名认证才能开通服务
温馨提示
参敬的客户,您好:
《中华人民共和国网络安全法》第二十四条规定:网络运营者为用户办理网络接入、域名注册服务,办理固定电话、移动电话等入网手续,或者为用户提供信息发布、即时通讯等服务,在与用户签订协议或者确认提供服务时,应当要求用户提供真实身份信息。用户不提供真实身份信息的,网络运营者不得为其提供相关服务。
为保证您天翼云服务的正常使用,请您尽快完成实名认证,感谢您对天翼云的理解支持,谢谢。

实名请超链接:

× ==

	ecloud	官埋中心			搜索	ų	忌宽	消息	账户	订甲	上甲	商業	合作	
۲	个人中心		身份认证								@		,早上好	
• • •	个人中心 基本信息 修改资料 身份认证 修改密码 更换手机		身份认证	学生认证	使用 天 5 ;		二维码,技 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		成认证		 基本信息 基本信息 第6000 第6305 		, 見上好)	

2-3 完成实名认证

步骤 3、实名认证后进入边缘安全加速平台—零信任产品详情页快速了解产品,之后单击【立即

开通】;

2-4 产品详情页



步骤 4、在购买页面选择适合的套餐和扩展服务,勾选并阅读服务协议,确认无误后点击"立即

- 开通",边缘安全加速平台—零信任服务即开通;
 - 2-5 产品开通页

		(現家 Q 当前工作区: 网站安全… ∨ 个人中ら 🛃	
	▲ 套餐开通	Pade Pate Par	1
8	安全与加速 零	红锅劳 动律统入服务 开发孢平台	
8 8	■ 基本信息 计费模式 使用范围	協動計畫 開內	
H H	套餐范围		
थ ®	會發洋情站成加速		
	一级域名数量	1个 域名规题: - 0 +	
0	沈厳	81	
	静态加速		
	动态加速	zje nazarstvan zazaratelomile, o cizare, Bibulk environskande men	
1	IPV6(5)/4)	The National Back And	
	WebSockets	NU/A展时的101156	
8	QUIC:	交持	

步骤 5、边缘安全加速平台—零信任服务开通后,便可以根据操作手册去控制台开始接入您要防护的企业应用。

3.1.2 续订

支持续订操作,登录官网订单管理-产品-产品视图-产品续订,提交您的续订需求,续订规 则详见如下链接:

https://www.ctyun.cn/document/10000038/10303747

G	大翼云 拉制	中心						QB	影响		费用 工	单 备案	支持 合f	⊧ 3 8*		ש (9 5	72 J
8	费用中心		续订管理	/ 手动续订													资源被	锁定0
0	总宽 订单管理			产品名	称	资源ID			资源池	资源状态	倒计时	续订周期	时间			操作原	后续订周	期
0	我的订单 待支付订单			边缘安全 ~ 任	:加速平台-零信	549e03fc2a0	04c2a970b74	8d06e516df	-	在用	366 天	-	⑤ 创建:20 ⑤ 到期:20	23-03-15 09:1 24-03-15 09:1	9:17 9:12	3个月		
හ ශ ශ	续订管理 进订管理		2	绿安全加速平	台-零信任													
0	资金管理	•	•															
	撤单管理		续订周	期: 💻		-0												_
	账单管理			1个月	2个月	3个月	4个月	5个月	6个月	7个月	8个月	9个月 1	0个月	1个月	1年	2年	E.	3年
	产品视图	•											续订金额	1:		¥ 1,	020.	00
	发票管理														确定提交		取消	
	合同管理														提示:]	最终费用以	计费出账	为准
	成本管理	*																
	卡券管理	•																
	按需试用																	

3.1.3 变更

您如果有变更套餐的需求,您可以登录天翼云官网,在订单管理-产品中找到您的订单,点

击"订购"提交您的变更需求。目前套餐变更只支持升级套餐,不支持降级套餐的操作。

操作改	产品价格 产品文档 产品深层
4版务	
HRR/C Daile Honoral	
The second s	
(FREE)	
###25## 0x3#5	
道用场景。 道用于大型集团企业多分支办公安全协同及定制化放弃 服务	
被 计传	
终端数: 10个	
企业监查额网络交易10个传输。展出部分传输5万元增加月收费	
Shi+沉扁斑路。800-60月	
内侧结网: 支持	
桌面终端 支持	
AAAKURIONI 236	
日志明计 支持	
观园学认证: 支持	
自然开致·支持	
行为情景 支持	
0.01/0.01/001 034	
Mirion 31	
Marine 314	
	00.00
33 の供用 10	62.08 ¹¹⁸

3.1.4 退订

产品支持退订服务,登录官网-订单管理-产品-产品视图-退订管理,找到您要退订的订单,

进行退订;客户套餐退订后,扩展服务也会一起退订

产品退订页面

总览		L	应定可以近110 八 七天无珪田超来						
订单管理			立只夕秋	次语行	次语动	恣语伊太	Betria	立只会師	司退订今朝
我的订单			/ 0010 17	页标记	风标心	凤胡柏	10101	1 00 202 894	可应可亚额
待支付订单			> 边缘安全加速平台	ba0661e633f9460ab50870a3283602f1	**	在用	© 创建:2023-03-14 15:41:05 ⑤ 到期:2024-06-14 15:41:01	744,663.78 元	741,411.79 元
续订管理									
退订管理			边缘安全加速平台			边缘安全与加速-	DDOS防护		
资金管理	•	4	边缘安全与加速-Bot管理						
撤单管理									
账单管理	*								
产品视图	•		* 请选择退订原因:						产品金额: ¥744,663.
发票管理			● 购买 二服务时洗错参数(配)	f. 时长、台数等)				泪江今郊,	¥741 411 70
合同管理			○ 云服务功能不完善,不满足	业务需求				赵门立创,	+/+/,+/1./5
成本管理	Ŧ		其他云服务商的性价比更高				-		
卡券管理	•		○ 云服务故障无法修复				∠ 3	龙已端认平次退订	金额和相关费用 <u>食有)</u>
按需试用			○ 其他						退订 取消

按用中心		退订管理								资源被锁定❷
总览		() 第3	还可以进行 0∶	次七天无理由過款						
订单管理	•									
我的订单		谱	输入产品名称	搜索 ~ 请输入订单号	搜索					
待支付订单				产品名称	资源ID / 订单号	资源池	资源状态	倒计时	时间	操作
续订管理										
┃退订管理			~ 🗹	边缘安全加速平台-零信任	549e03fc2a004c2a970b748d06e516df (20230315093550526572)		在用	458 天	© 创建:2023-03-15 09:19:17 © 到期:2024-06-15 09:19:12	退订
资金管理	¥ '	-								
撤单管理		过	2缘安全加速 ³	平台-零信任						
账单管理	*	-								

3.5 零信任服务

3.5.1 用户设置

AccessOne 零信任服务提供安全客户端,将企业办公终端相关应用的访问流量引流到天翼云 最近的服务节点。未安装安全客户端的办公终端将无法受到零信任策略的管控。本文介绍如 何设置企业认证标识、设置企业保留网段。

3.5.1.1 设置企业认证标识

背景信息

在使用 AccessOne 零信任服务客户端之前,您需要设置企业认证标识。企业认证标识是您 企业员工成功登录 AccessOne 零信任服务客户端的重要凭证,首次登录控制台,需要配置 企业认证标识。

配置方式

在左侧导航栏【用户设置】的企业认证标识区域,设置企业认证标识。 建议您使用企业名称等方便企业办公终端用户记忆的信息作为企业认证标识。终端用户首次 使用 AccessOne 零信任服务客户端时,需要手动输入该企业认证标识进行企业标识绑定。

账户设置			
展示账户相关设置信息	并进行管理		
企业认证标识			
终端用户使用零信任用	服务需要输入企业认证标识。		
建议你使用企业名称	在一个小小小公共的一个小小公司。	金业计证标识	
建以必使用正亚石小、	新学业的名誉通知,它们的担密计。		
*企业认证标识	请输入企业认证标识	编辑	

3.5.1.2 设置企业保留网段

背景信息

此项为非必须配置项,主要用于企业内部网段和零信任服务网段冲突的时候,进行配置。因为零信任服务会使用私有网络 IP 范围进行路由跳转,我们的路由范围网段将尽量避开常用的网络范围,目前零信任服务使用如下默认网段:,

配置方式

若您的企业内部网络涉及该网络范围,为避免零信任服务的私有网络 IP 范围和企业内部网络使用的内网网段发生冲突,请在左侧导航栏【用户设置】的企业保留网段区域,配置企业保留网段。

企业保留网段				编辑
可在此配置企业专用网络// 避免和零信任服务的局域网	局域网网段。 网段产生冲突。			
企业禁用IP段 ①	127.0.0.1 +新增	1	掩码	

3.5.2 应用管理

AccessOne 零信任服务平台提供的应用管理功能,帮助您管理企业的应用或资源。本文介绍 如何配置应用或资源,以及对应用进行相应的授权策略配置。

3.5.2.1 应用配置

背景信息

当您为企业员工配置办公需要员工访问的企业应用和资源时,可以使用 AccessOne 零信任 服务提供的内网应用功能。企业员工安装 AccessOne 零信任服务客户端,并通过身份与安 全策略校验,便可以访问对应的局域网应用或资源。

3.5.2.2 应用配置-应用标签

1.管理应用标签

功能说明:标签是作为应用的分类分组标识,通过对标签可以对应用进行分组管理,根据不同的应用类型和标签分类,实现对应用的快速筛选和授权选择。 配置方式:在左侧导航栏零信任服务--应用管理--应用配置栏,点击标签列表分页进行标签的管理,包括标签的添加,编辑,删除操作。 点击添加标签按钮,进行对应的标签添加。

	I				搜索	Q 注销 👮					
⊛		> 零信任服务 > 应用管理 > 应用配置									
	边缘安全加速平台 AccessOne	应用配置									
	☆ 服务概览	使用零倍任频略保护彻应用程序。只有符合忽频略的用户才能访问您配置的应用系统资源。									
۲	🔍 安全与加速 🛛 🗸	应用列表 标签列表									
⊛	🖳 零信任服务 🛛 🔿										
B	应用管理	输入标签关键字 Q				添加标签					
इ	应用配置	标签名称	数量	应用管理员	最后修改时间	操作					
- ®	应用访问策略	lljweb	14	-	2023-02-28 17:45:57	编辑删除					
⊛	零信任策略 🗸	lljapp	5	-	2023-02-28 17:45:51	编辑删除					
®	账户设置										

输入标签名称,通过选择应用管理员,可以根据标签给应用管理员划分权限。

添加标签		×
* 标签名称	请输入标签名称	
应用管理员	请选择应用管理人员	~
	应用管理员仅具备对应标签下的应用管理权限	
	取消 确认	

在左侧导航栏零信任服务--应用管理-应用配置栏,点击应用列表分页进行应用的管理,包括应用的添加,编辑,删除操作。

3.5.2.3 应用配置-应用添加

点击添加应用按钮,进行应用的配置。

										注销 📃
8	🖍 边缘安全加速	.	> 零信任服务 > 应用管	理 > 应用配置						
	AccessOne		应用配置							
	☆ 服务概览	☆ 服务概览 使用零倍任策略保护您应用程序,只有符合您策略的用户才能访问您配置的应用系统资源。								
₿	🔍 安全与加速	~	应用列表 标签列表							
\$	🖳 零信任服务									
	应用管理	~	请输入应用名称或应用出	也 ○ 应用标签 ~	应用类型 🗸					添加应用
P P	应用配置	1	应用ID	应用名称	应用地址	应用类型	应用标签	最后例	8改时间	操作
	应用访问	策略	mo5x	0317app	111.com	APP	lljapp	2023-	03-17 15:34:10	编辑 删除
æ	零信任策略		v3uk	iiii Iljweb0316	http://yingyong.com	WEB应用	lljweb	2023-	03-17 11:43:42	编辑 删除
æ	能白沿景		to7c	test3	http://222.com	WEB应用	lljweb	2023-	03-17 11:30:37	编辑图除
۲			6i4t	itest2	http://223.com	WEB应用	lljweb	2023-	03-17 11:29:53	编辑删除
۲	网络管理		qyo0	i test1	http://111.com	WEB应用	lljweb	2023-	03-17 11:29:23	编辑 删除
۲	身份管理	×	ehcq	iiii Iljweb123	http://ww.com	WEB应用	lljweb	2023-	03-16 16:46:20	编辑删除
*	信任分析	~	2nt8	iiiapp0316	www.domain1.com	APP	lljapp	2023-	03-16 15:42:45	编辑删除
۳ ھ	终端管理	~	xbne	🛃 组织应用	http://22.com	WEB应用	lljweb	2023-	03-01 16:07:37	编辑 删除
8	🖳 开发者平台	~	me5f	🔀 用户应用	http://38.com	WEB应用	lljweb	2023-	03-01 16:07:19	编辑删除
8	🔄 运营管理	~	50t4	🥦 测试应用	http://1.com	WEB应用	lljweb	2023-	03-01 15:50:26	编辑删除
æ	④ 计费详情		共 19 条 10条/页	√ 〈 1 2 〉 前往	1 页					

添加应用为两个步骤:

步骤 1: 添加应用信息,包括应用名称,应用描述,应用标签,应用类型,应用系统图标。 应用标签:指应用的自定义标签,方便您对应用进行分类、搜索和管理。您可以在应用配置 -标签列表添加标签。

应用类型:WEB站点应用系统(http, https, ws, wss协议类型应用)请选择WEB应用类型,其他协议类型资源请选择APP类型。

应用系统图标,支持图片上传对应图标,也可以从待选图标里面选择图标。

配置图标后, 该图标将作为该应用在客户端的展示图标。企业员工用户通过终端点击该图标 实现 WEB 类型应用快捷访问。

 油肉肉人物味可 	7.42	> 零信任服务 > 应用管理 > 应用配置										
AccessOne	**	应用配置										
☆ 服务概览		使用零值任質戰保护您应用程序、只有符合您策戰的用戶才能访问您配置的应用系统表面。										
🔍 安全与加速		添加应用										
🖳 零信任服务												
应用管理	~	1 应用信息	2 应用配置									
应用配置												
应用访问策略	略	* 应用名称	请输入应用名称									
零信任策略	~	应用描述	请输入应用描述									
账户设置		* 应用标签	请选择应用标签 >									
网络管理	~	* 应用类型 🕛	WEB应用 ~									
身份管理		应用ID	系统自动生成									
信任公拆		应用系统图标	选择图标 上传图标	图标预定								
1012.2010			0.请上传燕清图片	品								
终端管理			①108*108像素,支持JPG;大小不超过300KB									
🖳 开发者平台												
山 运营管理			下一步 取消									

步骤 2: 应用配置: WEB 类型应用如下配置: 应用地址:指应用访问的 URL,填写后,将作为客户端该应用图标快捷访问的入口地址 子应用地址:应用地址需要访问到的跨域地址以及该应用涉及的其他地址,支持通过 URL、 域名、泛域名、IP、端口、端口段信息配置应用地址。

添加应用
✓ 应用信息 ② 应用配置
• comet-tu
应用访问的URL,填写后,将作为客户端该应用图标快捷访问的入口地址
https://www.baidu.com
请输入应用地址
子应用地址
应用地址需要访问到的跨域地址以及该应用涉及的其他地址,支持通过URL、域名、泛域名、IP、端口、端口段信息配置应用地址

可以通过如下三种方式配置子应用地址:

1. URL 信息

支持通过 URL 配置子应用地址

URL信息 支持通过URL影篮子应用地址		~
子应用地址	子应用名	
https://www/baidu.com	baidu	M1 2
+ 8638		

2. 域名信息

支持通过域名、泛域名、端口、端口范围配置子应用地址

域名信息 支持通过域名、顶域名、编口、编口范围配置子应用地址		<u></u>
城名	罐□ http协议端口号请入80, https端口号请输入443, 其他端口范围请自定义输入	
*.baidu.com3gwww.baidi	第日 ~ 0-65535	删除
+ 810		

3. IP 信息

支持通过 IP、端口、端口范围配置子应用地址

IP信息 实为治理产 第二、第二、第二、第二、第二、第二、第二、第二、第二、第二、第二、第二、第二、第							
IP地址	端口						
IP ✓ 127.0.0.1 ∫ 32	NC V 0-65535	MISR.					
+ 858							

APP 类型应用:

应用配置:可选通过域名信息或者 IP 信息进行配置应用地址 域名信息:支持通过域名、泛域名、端口、端口范围配置应用地址

IP 信息:支持通过应用的 IP、IP 段、端口号、协议配置应用地址

透血应用 	
 应用信息 2 成用配置 	
域名信息	_
支持通过域名、泛域名、端口、端口范围配置应用地址	
域名	协议
	暂无数据
+ 8510	
P信息 支持通过府田的IP, IP码, 续门号, 续过配置府田此社	
旧地址	
	暂无数模
+ 新增	
	<u>上</u> ーサ 構定 取3月

3.5.2.4 应用授权策略

应用授权策略功能帮助您管控企业员工、企业合作伙伴对应用和资源的访问权限。当您添加 完应用或资源,您需要通过零信任策略对访问企业应用或者资源的员工、终端设备进行检测 和管控。

前提条件 已添加需要管控的应用。更多信息,请参见应用配置。 已添加策略生效的用户信息。更多信息,请参见身份管理。

背景信息

您可以创建多条策略,目前创建的策略数量不限制。

点击左侧导航栏应用管理-应用访问策略,添加策略按钮。

	1								<u>ax q</u> ±w 💥	
⊜		> 零信任服务 > 应用管理 >	应用访问策略							
	Contrast a local to the	应用访问策略	应用访问策略							
	◎ 服务概定	使用零倍任策略保护总应用程序。	只有符合意識是的电户才能認然意識	的应用程序。						
۲	○ 安全与加速 ~	NAMBER O NEH							attemas	
0	回、零信任服务 へ	策略名称	策略描述	策略模型	应用	用产组	组织装约 界	电产 更新时间	15.66	
	应用管理	1232		按磁织模型	0317app 1		1009-5249 H	2023-03-17 16:02:11	400 800	
२ @	自用配置	123		脫纖切模型	iljapp1		mon .	2023-03-17 11:38:28	84.89	
	零信任策略 ~	456		按磁织模型	lijapp1			2023-03-17 01:39:14	818 819	
8 8	账户设置									
60	网络管理									

步骤1:添加基础配置,填写策略名称,策略描述,点击下一步。

应用访问策略 使用零信任策略保护	回用访问策略 使用考试任道确保护态应用程序。只有符合忽道集的用户才能动吗忽起置的应用系统资源。							
添加策略								
1 基础配置	(2) 法释应用 (3) 生效范围							
*策略名称	消除入照照合称							
描述	· 建铁合金 · · · · · · · · · · · · · · · · · · ·							
动作	 ·							
	7-9 EA							

步骤 2:选择应用范围

通过筛选和搜索,确认选择的应用范围。

添加策	這加策略								
	Silken 3 2xila								
应用	(19)								
调输	入应用名称、地址、域名、IP Q 应用类型	◇ 広用板笠 ◇			●已添加((0)				
	应用ID	应用名称	应用地址	应用类型	应用标签				
	mo5x	0317app	111.com	APP	lijapp				
	v3uk	lljweb0316	http://yingyong.com	WEB应用	lljweb				
	to7c	test3	http://222.com	WEB应用	lljweb				
	6i4t	test2	http://223.com	WEB应用	lljweb				
	qyo0	test1	http://111.com	WEB应用	lljweb				
	ehcq	lljweb123	http://ww.com	WEB应用	lljweb				
	2nt8	Iljapp0316	www.domain1.com	APP	lijapp				
	xbne	组织应用	http://22.com	WEB应用	lljweb				
	me5f	用户应用	http://38.com	WEB应用	lijweb				
	50t4	测试应用	http://1.com	WEB应用	lijweb				
共 19 ;	条 10条页 ~ < 1 2 >	前往 1 页							
			上一步 取消						

步骤 3:选择生效范围

支持三种维度的用户范围勾选,包括按用户粒度进行选择,按组织架构进行选择,按用户组 进行选择。

请选择其中一种维度进行生效范围勾选,只支持保存一种维度的类型,若切换其他维度进行 重新选择,保存时将只保存当前维度范围的内容。

添加策	海加県等							
	✓ 基础配置 ジ 这并应用 3 生效范围							
请选择	一种维度: ○ 按用户选 (中一种维度进行生效范围勾)	按组织选择 按相户组选择 法,只支持保存一种维定的类型,若切换其他维度进行重新过	8择。保存时将只保存当前组度范围的内容。					
<mark>ا</mark> Æ	户(15)					●已添加(0) 搜索账号/姓名/手机号/邮箱 ○		
	姓名	账号	所属组织	用户组	来源	状态		
	ē	jujingyi	明星组织		0	正常		
	III.	jiangjinfu	om.cn 明星组织 3时星	-	0	正常		
		chenjing	nI平民组织		0	正常		
		luojin	icom.cn 明星组织 二线明星 二线男明星	-	0	正常		
		xiaoming	wcom.cn 平民组织 厦门半民	-	0	正常		

3.5.3 身份管理

通过动态身份验证的方式来标识客户端用户身份。通过设置身份源,您可以将企业的身份源 服务器与 AccessOne 零信任服务连通。AccessOne 零信任服务为您提供单身份源和多身份源 功能。本文介绍如何配置身份源信息。

背景信息

AccessOne 零信任服务以身份驱动下发安全策略,所以在使用 AccessOne 零信任服务之前,您需要完成与企业的身份管理服务对接。完成身份对接后,管理员可以按照企业组织架构下发安全管控策略。企业用户可使用与企业身份一致的账号体系登录 AccessOne 零信任服务客户端办公。

通过添加身份源配置,您可以将企业内部身份信息导入到 AccessOne 零信任服务,便于后续设置相关策略。

3.5.3.1 用户与组织

1、支持通过手动创建进行用户与组织关系构建。

2、支持通过表格模板批量导入进行用户与组织关系构建。

3.5.3.2 用户与组织-手动创建

在左侧导航栏-身份管理-用户与组织,查看用户与组织列表。 点击用户分页,添加用户按钮。

	1										22		Q	注钥	1
\$	动缘安全加速平台	> 零信任服务 > 身份管理 > 用户与组织													
	AccessOne	用户与组织													
	☆ 服务概览	管理您允许使用零信任服务的用户信息。													
₿		组织结构		WODY	v101@chinat	alacom cn							用户数	下级组织数	
8	🖳 零信任服务 🔷	 werxy191@chinatelecom.cn BB/B389 	윪	♥ETIX	组织: wenxy191@	chinatelecom.cn							15	12	
	应用管理 🗸	▶ 平民組织 加長規約	用户组织	ą.											
থ	零信任策略 🗸	Service and the service of the servi	管理您允许使	用零信任服务的	用户信息。										
⊛	账户设置		添加用户	用户批量导入	搜索姓名/张号/	(却箱/手机号码	查询						🛛 展示7	-级节点的用户	
8	网络管理 💛		账号	姓名	手机号码	邮箱		所属组织		用户组	来源	状态	操作		
9 8	身份管理 へ		jujingyi	ē 3	137****8888	d***@qq.com		编码时代	atelecom.cn[8]	明星组、平民组	系統	9禁用	启用 编辑	删除	
\$	用户与组织		jiangjinfu	莱	135****4444	a**@163.com		2E3E3R()550	itelecom.cn间	明星组	系统	© 正 %	禁用 编辑	删除	
B B	用户组管理		chenjing		136****4466	c******@qq.com		民組织	natelecom.cn 平		系統	©正常	禁用 編編	删除	
P	信任分析 ~		luojin	7	135****5465	3****@qq.com			ecom.cn间		系統	© 正 常	禁用 编辑	删除	
⊛								100-1447(1)	- mail						

填写用户基本信息

用户与组织 繁荣感光计使用率强任服务的用户国意。									
← 用户新增	- 用户新增								
基本信息									
18 Th At th									
▲ 鐵信息	(油油)) 世史 ((((((((((((((((((
2010									
用户组	请选择 ~								
归属组织信息									
归属组织	m.cn Q								
联系信息									
手机号码	请供写手机号码 邮箱 请供写邮箱								
	477 1 001								

点击组织分页,添加组织按钮,填写信息,添加对应的组织。创建组织默认在企业根节点组 织下。

← 组织新增				
基本信息	请输入组织名称		*上级组织	٩
组织ID	系统自动生成			
		保存	取消	

3.5.3.3 用户与组织-批量创建

在左侧导航栏-身份管理-用户与组织,查看用户与组织列表。 在用户分页,点击用户批量导入按钮,创建用户。 进行导入模板下载,填写内容。 上传导入模板内容,解析导入数据。

用户与组织 管理能允许使用考虑征服务的用户信息。	
批量导入用户	
祖一步:下载导入模纸 导入的用户个数量小子100,所有允许导入的信息学段请参考模拟:	下都得入模板 之
猫二步:上传数缀文件 目前支持的文件类型为"sala, *salax;	這種文件 □
	±10 10.74
在组织分页,点击组织批量导入按钮, 进行导入模板下载,填写内容。	创建组织。

上传导入模板内容, 解析导入数据。

用户与组织 管理意先许使用导语任服务的用户信息。	
批量导入组织	
猫一步: 下载导入模纸 导入的组织个数面小子100,所有允许导入的信息学段语参考细版:	下载导入摄纸 土
第二步:上传数据文件 目前支持的文件类型为*ada、*adax;	选择文件 D
20	82.96

3.5.3.4 用户组管理

进行用户组管理,用户组可用于便捷授权。您可创建项目组、地理划分组、岗位组等,并通 过将多个用户关联到组中,并以组为单位进行权限管理。

B	> 零信任服务 > 身份管理 > 用户组管理								
这缘安全加速平台 AccessOne	用户组管理								
□ 服务概覧	用户细可用于便捷授权。您可创建项目组、地理划:	分组、岗位细等,并通过将多个用户关取到组中	, 并以組为单位进行权限管理。						
副 ── 安全与加速 ──	援索用户组名称 Q	用户组: 明星组 🖉 🗇							用户数
▶ 🖳 零信任服务 🗠	20.5.10	9組內成员将继承用户组所拥有的权限							4
应用管理 〜	平氏组	添加用户					提索账号/姓名/部	(称)手机号码	宣询
♀信任策略 ~		账号	姓名	手机号码	邮箱	所屬組织	来源	状态	操作
● 账户设置		jujingyi	翱娟祎	137****8888	d***@qq.com	com.cn 明星组	系统	禁用	•
 9 网络管理 ~ 8 自む新聞 		jiangjinfu	蒋劲夫	135****4444	a**@163.com	telecom.cn)明星组 3NI—现明星	系统	正常	0
B		xalogen	小根	135****4746	d***@qq.com	atelecom.cn	系统	正常	0
用户与组织		xaiogen3	小根	135****4742	3****@qq.com	m.cn	系统	正常	0
用户组管理									
B 信任分析 ~									
▶ 終端管理 ∨									
□ 开发者平台 ∨									
> 运营管理 ~									
④ ⑦ 计费详情	创建用户组								

点击创建用户组按钮,管理员可以手动创建组。创建后,即可向组内添加成员账户,并以组 为单位统一授权。

新增用户组		Х
● 管理员可	[以手动创建组。创建后,即可向组内添加成员账户,并以组为单位统一授权。	
* 组名称	请输入组名称	
	组的名称,例如项目组、地理划分组、岗位组等。	
用户组ID	系统自动生成	
描述	请输入用户组描述	
	取消	定

添加对应用户组后,可以对用户组进行用户添加。

▶ 明星组织 ▶ 平民组织	待选人 搜索 只展示	员(5) 账号/姓名/手机 ⁺ 示当前组织的用	号码/邮箱 查询 户列表,下级组织的用户列署	長需左側进一步展开勾选		已选人员(0) 清空
领导组织		姓名	账号		所属组织	
		小根	xaiogen		atelecom.cn	
		小根	xaiogen3		∋com.cn	
		小李	xiaoli4		com.cn	
		小根	xaiogen6		om.cn	
		打蜡	dala		cn	
		打蜡	dala	_	cn	

3.5.4 网络管理

您可以通过 AccessOne 零信任服务配置连接器功能连接组网,实现使用 AccessOne 零信任服务终端访问企业内部业务。本文介绍了配置连接器的具体操作。

应用场景

本地连接器:目前支持 Docker 容器化部署连接器,您需要在您的 VPC 网络中准备服务器用于安装连接器,并将所需路由到该连接器流量的应用信息配置到连接器上,实现客户端通过 连接器连通对应的内部网络。

在在网站的上阶站自住,在这面自住,一口,了这些自正亚/小约百时在这面外衣	在左侧导航栏网络管理	-连接器管理栏目,	可以查看企业所纳管的连接器列表。
--------------------------------------	------------	-----------	------------------

							超索	Q 2±81	<u>×</u>
8	🧢 边缘安全加速平台	> 零信任服务 > 网络管理 > 连接	器管理						
	AccessOne	连接器管理							
	☆ 服务概覧	通过连接翻将您的基础设施和零信任服务	的边缘节点建立安全连接。						
۲	🔍 安全与加速 🚽	新增 清输入连接器名称、连接	图ID、路由列表ip或城名 〇						
8	🗟 零信任服务 🔷	新增连接器并配置应用资源,将连接器安装	在图的vpc网络中,实现安全访问您的原	7用系统。					
	位田等国	连接器名称	连接器ID	连接状态	路由列表	状态	更新时间	操作	
	零信任策略 🗸	456	9ceec8eb 251	9b2cb6ae 未激活		◎启用	2023-03-21 10:36:42	停用配置删除	
	账户设置	123	0c83- ea129	3d5a8 未激活	111.baidu.com	◎启用	2023-03-21 10:35:16	停用配置删除	
B	网络管理 へ	werxytest22	f8 8d126	1e89644 未激活		●停用	2023-03-16 15:50:34	启用配置删除	
8	连接器管理	werxytest20	a78 02b1f	7260c3 未激活	12.12.12.12/32	●停用	2023-03-16 15:49:07	息用配置 删除	
8 8	身份管理 ~	werxytest21 \star	2ab1 19 5f244	b288c9f5c 未激活		◎启用	2023-03-16 15:49:01	停用配置删除	
8 P	终端管理 🗸 🗸								

创建一个连接器,将 HTTP web 服务器、SSH 服务器和其他协议安全地连接到零信任服务。 点击新增按钮,进行连接器的新增。

步骤1:基本信息配置,填写连接器名称,描述。

用您想连接的网络信息来命名你的连接器,我们推荐每个网络、数据中心只创建一个连接器 进行使用。第一个创建的连接器将作为默认连接器使用。

连接器管理 通过连接器将您的	凝缩设施和零信任服务的边缘节点属立安全进建。	
创建连接器 创建一个连接器,料 基本信息 > 安装	\$HTTP web服务员。SSH服务器和其他协议变金地法接到零位任服务。 装饰报器 > 配置路由应用	
基本信息 用態想连接的网络 • 连接器名称 描述	输出意来命名你的连接器,我们准容等个网络、数据中心只创建一个连接器进行使用。 供给入选择器名称 请给入选择器描述	
启用 (默认连接器
		RUM

点击保存按钮,将自动生成连接器 ID 和连接器安装命令。请将连接器安装命令复制在服务器终端进行一键安装,安装成功后,平台将展示连接器的安装状态,未安装的连接器为未激活状态。安装成功的连接器将展示为激活状态。

步骤 2:

将连接器安装到您的专属网络 VPC 中,并配置通过该连接器访问的应用系统资源,实现流量路由管理和安全访问。

请将以下命令复制粘贴到终端窗口中,实现连接器的安装和运行。

安装连接器测试连接器名称	
书选接接安装到包的专属网络VPC中,并配置置过该走接着动向的成用系统资源,实现注题路由管理和交生协问。	
基本信息 > 安裝连接器 > 配置語由应用	
安装连接器 目前尺式HOoder安装。	
请将以下命令复制私贴到终端窗口中,实现连接器的安装和运行。	
docker pull ehub.ctcdn.cr/security-waf/sec-sigentListest && docker run -dname sec-connector-0B6007c342ce/3d6aac64c4c8edac138privileged=trus -v /etc/hosts/etc/hosts -e \$ TOKEN-ey.l02XWbbnRfaW0GU3MTbv72NZm01IwV29bumVjd3g9X28kjoIMDZZDA9Y3M0MmNJkDNkkmFhY2Y0YzRjkmX+YWMAMzgLGJzZWNyZXGOJJkk/zMyMmZN5000TQ zLTQyYTAYmRkZ02YTE0MJJGWY4NGII/Q==' ehub.ctcdn.cn/security-waf/sec-agentListest	
7-9 88	

3.5.4.2 连接器配置

配置连接器的路由管理,点击新增WEB类型按钮,配置对应路由应用。

配置路由应用测试连接器名称								
通过自注接器器加公共主机名或专用网络来题曲流量。忽可以随时相后添加更多主机名或网络。								
基本信息 > 安装连接器 > 配置路由应用	Ð							
WEB类型 APP								
根据域名搜索				新增WEB类型				
序号 域名	模式	解析iP	操作					
		暂无数据						
		L-#						

将要通过该连接器进行访问的域名进行填写,并选择解析模式。支持配置 DNS 服务器 IP, 使用 DNS 解析模式自动获取域名解析的 IP 地址,也支持直接配置静态解析模式,按照指定的 IP 进行域名解析。

支持域名代理功能: 若该域名和其他域名解析到相同 IP 地址, 可通过开启域名代理功能避 免其他域名也走该连接器访问。

£	新增WEB类型		×
	* 域名	请输入域名	
-pa	*解析模式	请选择	~
	域名代理①		
		與 /月 《明 /2	-

3.5.5 零信任策略

支持零信任策略配置,目前开放访问控制功能,实现对不同的访问进行监控,拦截,丢弃处 理。

3.5.5.1 访问控制

点击左侧导航栏-零信任策略-访问控制可以查看访问控制列表。

		> 零信任服务 > 零信任	策略 > 访问控制					
AccessOne	平台							
□ ●仲仁四夕		访问控制						
凹点 夸相相比的		展示访问控制规则,并且可以	\进行新增、编辑、删除					
应用管理	~	规则ID 请输入规则	D 规则名称 请输	入规则名称				
零信任策略	^							新博
访问控制		规则ID	规则名称	处理动作①	防护状态	防护优先级①	操作	
账户设置								
网络管理	~				2			
身份管理	~			-				
信任分析	~							
终端管理	×				雪无数据			
🔍 开发者平台	~							
山 运营管理	~							

点击新增按钮,进行访问规则新增。

支持通过不同的条件进行规则匹配,	组合,	实现多维度访问控制。	

51	新增					×
:1)万 :1) 「	* 规则名称	请输入规则名称		*防护状态		
909	规则描述	请输入规则描述				li.
IJIC	*匹配条件①	匹配字段	逻辑符	匹配内容		
		请选择 ~	请选择 ~	请输入匹配内容		删除
		+新增条件				
	*处理动作①	● 拦截 ○ 监控	○ 丢弃			
					取消	确定

3.5.6 信任分析

信任分析目前展示终端登录日志和威胁防护日志,其中终端登录日志将记录并展示每一次终 端登录的信息,攻击日志用于用于展示攻击防护日志。

3.5.6.1 终端登录日志

终端登录日志,在展示用户的登录日志,可以对应搜索对应的日志列表。支持导出功能。

8	▲ 油棉中会加速变分	> 零信任服务 > 信任分析 >	终端登录日志					
	AccessOne	终端登录日志						
	应用管理 🗸 🗸	终端登录日志将记录并展示每一次	冬端登录的信息					
⊛	零信任策略 🗸	用户 请选择		输入查找IP 登录时间	⑤ 2023-03-15 15:08:43 至 202	3-03-22 15:08:43		
₿	账户设置			查询 重置			导出	
	网络管理 🗸	用户	所属组织	жор	晉录方式	晉录状态	晉受时间	
Ŷ	身份管理 🛛 🗸		2 11 100 PM (P)				11000310	
_	たたいた							
8	161±35147 ^							
B B	1日日25°47 人				1:			
8 8 8	8端登录日志 威胁防护日志				:			
8 8 8 8	语比方析 不 终端登录日志 威胁防护日志 终端管理 ~			it.	2011年1月1日			
8 8 8 8	1日は230年 ~ 終端登录日志 成励防护日志 终端管理 ~			e e e e e e e e e e e e e e e e e e e	2018			

3.5.6.2 威胁防护日志

威胁防护日志支持查看攻击时间,规则 ID 等信息。

● 计模式公司法可公	> 零信任服务 > 信任分	分析 〉 威胁	防护日志						
AccessOne	威胁防护日志								
应用管理 🗸	提供并展示攻击防护日志								
零信任策略 🗸									
账户设置	攻击时间 🕒 2	023-03-15 15	:14:11 至	2023-03-22 15:14:11	用户	请选择	✓ 攻击IP	请输入查找IP	
网络管理 🛛 🗸	规则ID 请输入	、查找规则ID	目标域	载名或IP 请输入查找目	标地址				
身份管理 🗸				8	山				等出
信任分析 へ	攻击时间	规则ID	用户	攻击IP	攻击IP归属	目标域名或IP	规则类型	状态码	处理动作
终端登录日志	2023-03-22 14:39:38	145	g g	10.0.	unknownunknown unknown	j.com	EAO_ACB	443	丢弃
威胁防护日志	2023-03-22 14:38:12	145	nwan g	10.	unknownunknown unknown	w\ com	EAO_ACB	443	丢弃
终端管理 🗸	2023-03-22 14:37:14	145	g n	10.0.128.1	unknownunknown unknown	wv n	EAO_ACB	443	丢弃
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	2023-03-22 14:05:41	-	/3	10.0.0.2	unknownunknown unknown	de	-	403	
	2023-03-22 14:05:41	-	3 3	10.0.0.2	unknownunknown	de 1.cn	-	403	

3.5.7 终端管理

终端管理提供终端设备列表展示,客户端下载功能。

3.5.7.1 终端设备管理

终端设备列表将全面、直观地展示企业用户终端接入的信息,通过终端管理,展示字段为终 端设备,操作系统,用户,所属组织等。

▲ 边缘中众加速亚台	> 零信任服务 > 终	端管理 〉 终端设备管理					
AccessOne	终端设备列表						
应用管理 🗸	终端设备列表将全面、	直观地展示企业用户终端接入的作	自息				
零信任策略 🗸			_				
账户设置	最后一次登录时间	· 2023-03-15 15:19:35	全 2023-03-22 15:19:35		请选择用户 >	登录状态 请选择状态	~
网络管理 🗸			查询	重置			导出
身份管理 🗸	终端设备	操作系统	用户	所属组织	MAC地址	登录状态	最后一次登录时间
信任分析 🗸							
终端管理 へ					•		
终端设备管理					•		
音广靖下载				新子数据			

3.6 运营管理

3.6.1 告警管理

简介

网站接入后,您可以通过设置告警策略,当网站请求流量到达边缘节点时,若检测到攻击事件、异常流量并触发告警策略时,将向您发送告警通知,帮助您及时掌握业务的安全状态。 本文介绍如何设置告警策略和查看告警记录。

设置告警策略

 1、登录边缘安全加速平台控制台,在左侧导航栏中选择【运营管理】--【告警管理】--【告 警策略】页面;

2、单击【新增】按钮,可以根据需要配置适合的告警,支持配置的告警类型有 Web 防护告警、CC 防护告警、DDoS 防护告警、BOT 防护告警、访问控制告警;

告警配置新增页面

0		::5	平台			提索		Q 当前工作区: tes	II作区> 个人中心 🛛 🙎
⊛			ᢙ > 运营管理 > 告警管理						
® ®	AccessOne		■ 告警管理 支持自助配篇攻击告警,支持的攻击类型为web						
æ	88 服务概览			新增告警策略		×			
۲	⑤ 安全与加速		告警策略告警记录	* 告警名称:	你 诺输入营营名称		_		
@	🖾 零信任服务		域名: 全部 ✓	*告警状态:	ā: 💽		~	查询 新增	
•	@ 边缘接入服务		告警名称	*服务类型:	型: 安全与加速			告警状态	操作
@	📼 开发者平台		testback001	* 告警类型:	型: 请选择				2046 (Sell) 1813
	◎ 运营管理		test-cc-控制台	*告警通知问隔:	隔: 5				直有 编辑 服除
	告警管理			勿扰时间:	周: ○ 23:55:57 至 00:55:57 ⊙				
	日志管理		ddos告警测试123	通知方式:	此 邮件: 支持输入多个,多个用关文分隔符;隔开		i.cn		立石 编辑 無除
	攻击事件		ddosaaa			11			1976 SHI 1939
	态势感知 国 计费详情		控制台-cc告警 dddd		短信: 支持输入多个,多个用英文分隔符;隔开		com.cn		立石 编辑 删除
			控制台-cc告警				:com.cn		at an so
					NC 3	尚定	com.cn		
					we	mxy191@chinatel mxy191@chinatel	ecom.cn ecom.cn		
			11 25 St. 1047 (55	2 3 4	N mit 4 m				

配置项	说明
告警名称	自定义告警名称
告警状态	是否开启告警
服务类型	目前安全与加速服务支持配置告
	警策略
告警类型	安全与加速服务支持配置以下 5
	种告警类型: Web 防护告警、CC
	防护告警、DDoS 防护告警、BOT
	防护告警、访问控制告警。
	告警条件:
	(1) Web 防护告警。支持选择多
	个域名与多个攻击类型,在n分
	钟内产生 m 次攻击则产生告警;
	(2) CC 防护告警。支持勾选多条
	告警条件,当满足任一条件均会
	产生告警;
	(3) DDoS 防护告警。支持勾选多
	条告警条件,当满足任一条件均
	会产生告警;
	(4) BOT 防护告警。支持选择多
	个域名与多个攻击类型,在n分
	钟内产生 m 次攻击则产生告警;
	(5)访问控制告警。支持选择多

	个域名,支持选择攻击类型为访
	问控制与频率控制,在n分钟内
	产生m次攻击则产生告警
告警通知	当产生相同告警时候,可设置告
间隔	警通知间隔减少告警次数
勿扰时间	配置的时间内不产生告警
通知方式	支持邮件与手机号的通知方式,
	建议最多配置 5 个

查看告警记录

在告警记录列表中可查看己告警记录,包括:告警时间、告警名称、域名、服务类型、告警 类型、通知方式及告警原因。

告警记录页面

3.6.2 日志管理

业务日志

i.

控制台可选择域名和时间范围查询日志,并支持单个日志下载和批量下载。选中单个域名 后面的文件下载键进行单个日志文件下载;第一列选中多个域名,并点击【批量下载】可 进行批量日志下载。

AccessOne	 业务日志 对安全与服务已生效域名提供节点访问日志数据下载,支出 	寺近15天内的日志下载。数据字段以及更多说的	明,请查看业务日志日志文档。		
☆ 服务概览	选择域名 请选择	选择时间 📄 2023-03-06 至 20	223-03-20 查询 批量下载		
○ 安全与加速	编号 域名任务	提交时间	完成时间	文件大小	文件下载
🖳 零信任服务					
回、开发者平台 、					
□ 运营管理					
告警管理					
日志管理			暂无数据		
业务日志					
攻击日志					
操作日志					
态势感知					
计费详情	共0条 10条页 ~ (1)	前往 1 页			

3.6.3 态势感知

简介

边缘安全加速平台的态势感知页面,帮助用户全方位掌握业务安全的整体态势。

态势感知首页

首页为具备动态科技感的边缘安全加速平台拓扑图,主要功能有:

- 若统计期间内有攻击流量产生,此页面将出现红色告警提示并有红色线条指向对应的安
 全边缘节点,绿色线条则为正常流量;
- 标题:标题支持自定义,支持输入中英文字符,最多可输入 20 个;
- 提供五个大屏的入口,分别为:安全与加速、DDoS 态势感知大屏、CC 安全态势感知大 屏、Web 安全态势感知大屏、BOT 安全态势感知大屏,点击对应的大屏悬浮框,将跳转 至新页面为您展示安全态势。



安全与加速态势大屏

安全与加速态势大屏支持从安全、性能、业务数据三个维度对客户的数据进行统计分析,实时展示客户业务整体的安全与加速情况。

主要包括:受攻击情况、威胁事件分析、各地访问性能的平均首包时间、响应时间、域名访问趋势、状态码分布、访问用户区域分布等统计信息。

标题支持编辑最多15个中英文字符;点击右上角菜单按钮,支持切换至其他大屏页面。



Web 应用安全态势大屏

Web 应用安全态势根据客户维度,实时展示客户业务受 Web 应用攻击的整体情况。 主要包括:全球攻击情况、攻击来源 IP、攻击 TOP URL、攻击域名 TOP 排行、攻击类型分 布、攻击类型趋势、攻击来源 TOP 排行、攻击趋势和滚动式的安全威胁信息等。 标题支持编辑最多 15 个中英文字符;点击右上角菜单按钮,支持切换至其他大屏页面。



网络层 DDoS 安全态势

网络层 DDoS 安全态势根据客户维度,实时展示客户业务受 DDoS 攻击的整体情况。 主要包括:攻击时长分布、DDoS 攻击类型分布、攻击趋势、攻击带宽峰值分布、攻击事件 列表的安全威胁信息等。



标题支持编辑最多15个中英文字符;点击右上角菜单按钮,支持切换至其他大屏页面。

CC 安全态势

CC 安全态势根据客户维度,实时展示客户业务受 CC 攻击的整体情况。

主要包括: CC 攻击趋势、攻击来源地区分布、攻击源 IP 排行、受攻击情况排行、CC 攻击事件信息的安全威胁信息等。

标题支持编辑最多15个中英文字符;点击右上角菜单按钮,支持切换至其他大屏页面。



BOT 安全态势

BOT 安全态势根据客户维度,实时展示客户业务受 BOT 攻击的整体情况。

主要包括: BOT 攻击请求趋势、恶意 BOT 攻击源地区排行、访问类型排行、受攻击情况排行、 攻击 IP 排行、攻击策略分布、搜索引擎访问分布、IDC 厂商 IP 访问排行及分布情况、攻击 事件分析的安全威胁信息等。

标题支持编辑最多15个中英文字符;点击右上角菜单按钮,支持切换至其他大屏页面。



3.7 计费详情

根据3月要上线的模块写

G		电信天到	霍云-CDN+		Į	_{要索} Q	概览 个人中心	当前工作区:安全加速	i v 📘		
۲	边缘网络控制	川台	首页>计费详情	首页 > 计费详情							
₽ ¢	⑥ 服务概览		↓费详情 支持产品退订和套餐变更								
8	A 快速入门		套餐详情 超量	计费 增值服务	订购历史						
B B	A 安全与加速	~	服务类型	套餐与用量	用量	开始时间	续订/结束日期	条款	操作		
ø	 ◆ するに加劣 ✓ 边缘接入服务 ◇ 开发者平台 ๗ 运营管理 	*	安全与加速	高级版 (流量)	流量: 700/500GB 请求数: 155.4万/200万次 一级域名数: 1/1个 D0oS防护次数(40Gbps): 1/2次 访问控制: 19/20条 频率控制: 18/20条	2023年2月1日	自动续订日期 2024年2月1日	3800 元/月 外加使用量	详情 升配退订		
	③ 计费详情		零信任服务	企业版	终端数: 8/10个 防护流量: 340/500GB	2023年2月15日	自动续订日期 2024年2月15日	550元/月 外加使用量	详情 退订		
			应用安全加速网	基础版	应用加速域名: 1/1个 DDos防护次数: 0/1次	2023年2月15日	自动续订日期 2024年2月15日	2000元/月 外加使用量	详情 退订		
			开发者平台	高级版	 函数: 32 / 50 个 満求数: 200000/100000 存储用量: 8.54/10GB Readgi: 94.557/100万次 Write数: 4.5万/10万次 Delete数: 1.8万/10万次 List数: 5.5万/10万次 	2023年2月1日	自定续订日期 2024年2月1日	40 元/月 外加使用量	详情 退订		

边缘安全加速平台—安全与加速服务客户控制台的【计费详情】页面,客户可以进行查

看购买的套餐版本和扩展服务,以及可用域名的数量:

计费详情页面

云WAF 控制台	首页 > 计费详情											
	套餐名称	変観名称										
概览 · 域名管理 · · · · · · · · · · · · · · · · · · ·	套餐内容	套氨 内容 套 氨详情		生效时间		到期时间	到期时间		状态			
医全分析 统计分析	Web应用防火墙(边缘云版) 高級版	业务带宽峰值:50Mbps 域名个数:主域名个数1;子5	50Mbps 2021-11-08 名个数1;子域名个数 9		2051-12-08		服务中					
◎ 日志管理 ~	拓展名称											
⑦ 告警管理 ∨	拓展功能	拓展详情	洋情 生效时间		到期时间		状态		操作			
☑ 计费详情 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	智能负载均衡	*	2021-11-08		2021-12-08		服务中		宣看详情			
(二) 址书書理	安全VIP服务	÷	2021-11-08		2021-12-08		服务中		查看详情			
	带宽扩展	业务带宽拓展: 1Mbps	2021-11-08		2021-12-08		服务中		查看详情			
	CC防护	CC防护:50000QPS	2021-11-08		2021-12-08		服务中		查看详情			
	WAF域名扩展	域名拓展: 9个	2021-11-08		2021-12-08		服务中		查看详情			
	Bot管理		2021-11-08		2021-12-08		服务中		查看详情			
	大屛服务	÷.	2021-11-08		2021-12-08		服务中		查看详情			

4 最佳实践

4.1 安全与加速接入配置最佳实践

步骤1:网站业务梳理

建议您对所需接入安全与加速业务情况进行全面梳理,帮助您了解当前业务状况和具体数据,为

后续配置防护策略提供依据。

梳理项	说明
网站和业务信息	
网站/应用业务每天的流量峰值情况,包括 Mbps、QPS	判断风险时间点,并且可作为WAF实例的业务带宽和业务QPS规格的选择依据。
业务的主要用户群体(例如,访问用户的 主要来源地区)	判断非法攻击来源,后续可使用地理位置访问控制功能屏蔽非法来源地区。
业务是否为 C/S 架构	如果是 C/S 架构,进一步明确是否有 App 客户端、 Windows 客户端、Linux 客户端、代码回调或其他环 境的客户端。
源站服务器的操作系统(Linux、Windows) 和所使用的 Web 服务中间件(Apache、 Nginx、IIS 等)	判断源站是否存在访问控制策略,避免源站误拦截 WAF 回源 IP 转发的流量。
域名使用协议	判断所使用的通信协议 WAF 是否支持。
业务端口	判断需要防护的业务端口是否在 WAF 支持的端口范 围内。 标准端口: 80: HTTP 对外协议默认使用端口
	•
	443:HTTPS 对外协议默认使用端口
	•
	非标准端口
	80/443 以外的端口
业务是否使用 TLS 1.0 或弱加密套件	判断业务使用的加密套件是否支持。
业务交互过程	了解业务交互过程、业务处理逻辑,便于后续配置针 对性防护策略。
活跃用户数量	便于后续在处理紧急攻击事件时,判断事件严重程度, 以采取风险较低的应急处理措施。

业务及攻击情况	
业务类型及业务特征(例如,游戏、棋牌、 网站、App 等业务)	便于在后续攻击防护过程中分析攻击特征。
单用户、单 IP 的入方向流量范围和连接情况	帮助后续判断是否可针对单个 IP 制定限速策略。
用户群体属性	例如,个人用户、网吧用户、或通过代理访问的用户。
业务是否遭受过大流量攻击、攻击类型和 最大的攻击流量峰值	判断是否需要增加 DDoS 防护服务,并根据攻击流量 峰值判断需要的 DDoS 防护规格。
业务是否遭受过 CC 攻击和最大的 CC 攻击 峰值 QPS	通过分析历史攻击特征,配置预防性策略。
业务是否已完成压力测试	评估源站服务器的请求处理性能,帮助后续判断是否 因遭受攻击导致业务发生异常。

步骤 2: 站点接入

此步骤需要进人控制台,添加加速域名,然后配置 CNAME,详情参见操作指导—WAF 接入

5 常见问题

5.1 计费类

Q1

购买边缘安全加速平台—安全与加速服务套餐后, 套餐内包含的带宽和域名数量不够怎么办?

A1

如果套餐内包含的用量不够, 可以通过扩展服务来补充, 扩展服务购买成功后, 计费和域名数量

总使用量是套餐内的量和扩展服务用量之和。

Q2

边缘安全加速平台—安全与加速服务套餐,是否支持变更?

A2

目前套餐支持升级,暂时不支持降级,本月升级,次月生效。

Q3

边缘安全加速平台—安全与加速服务的计费项有哪些?

A3

边缘安全加速平台—安全与加速服务的计费项为套餐包和扩展服务中的计费项,都是预 付费方式。

Q4

边缘安全加速平台—安全与加速服务的是否按需收费?

A4

边缘安全加速平台—安全与加速服务暂时不支持按需收费,之支持预付费。

5.2 开通类

Q1

怎么样开通边缘安全加速平台——安全与加速服务服务和使用?

A2

边缘安全加速平台—安全与加速服务服务的开通首先需要注册天翼云官网的账号,通过 产品栏目找到边缘安全加速平台—安全与加速服务,点击开通;开通后会跳转到 CTWAF 控制台,在控制台上配置边缘安全加速平台—安全与加速服务的域名,配置成功后天翼 云边缘安全加速平台—安全与加速服务会提供域名对应的 cname,客户切入 cname 后, 开始使用天翼云的边缘安全加速平台—安全与加速服务服务。

Q2

欠费后安全加速服务会被关停吗?

A2

账户余额不足以支付服务费用将导致欠费,发生欠费后,边缘安全加速平台—安全与加 速服务服务的域名将被关停。

Q3

关停边缘安全加速平台—安全与加速服务后怎样重新开启服务?

Α3

客户补足欠款后,客户的天翼云账号恢复使用,被停止的域名需要客户到 CTWAF 控制 台域名管理模块,点击启用域名,开启被停用的域名,当域名状态变更为已启用后,支 持客户随时切换到边缘安全加速平台—安全与加速服务服务进行安全防护。

Q4

边缘安全加速平台—安全与加速服务配置完成后大概多久生效?

A4

边缘安全加速平台—安全与加速服务的域名接入配置在 CTWAF 控制台完成配置后一般 120 分钟内生效,若 120 分钟后仍未生效,请提交工单处理;如果是安全防护配置一般 配置 5 分钟内生效,若 5 分钟后仍未生效,请提交工单处理。

Q5

接入边缘安全加速平台—安全与加速服务服务的域名有什么要求吗?

A5

接入边缘安全加速平台—安全与加速服务服务的域名,需要在工信部完成 ICP 备案,且 源站的业务内容必须合法。

Q6

100

关闭边缘安全加速平台—安全与加速服务服务后,域名配置会保留吗?

A6

欠费导致服务关闭,域名配置会保留,但不会继续为所配置域名提供安全防护服务。

Q7

删除边缘安全加速平台—安全与加速服务域名后,域名配置会保留吗?

A7

删除域名后,其配置将不会保留。

Q8

域名被封禁如何解封?

A8

请您提交工单。

Q9

边缘安全加速平台—安全与加速服务服务被暂停了,为什么?

A9

业务被暂停有以下几种情况:

欠费

未备案或备案已过期

内容违规

套餐包过期

5.3 操作类

Q1

如何判断边缘安全加速平台—安全与加速服务配置生效?

A1

可 ping、dig 所添加的域名,若转向到*.ctycdn.com,即说明配置成功,边缘安全加速 平台—安全与加速服务已经接入服务,可以自定义配置安全防护功能。

Q2

使用天翼云边缘安全加速平台—安全与加速服务服务后,需要对部分恶意 IP 进行屏蔽, 以保护站点数据和流量负载,可以通过控制台进行自助配置吗?

A2

天翼边缘安全加速平台—安全与加速服务可以通过配置访问控制的功能实现,以及使用 API的接口进行封禁。

Q3

天翼云边缘安全加速平台—安全与加速服务服务支持 https 的协议吗?

A3

天翼云边缘安全加速平台—安全与加速服务服务是支持 https 协议的。只需根据提示将 SSL 证书及私钥上传,WAF 即可防护 HTTPS 业务流量

Q4

天翼云边缘安全加速平台—安全与加速服务服务支持特殊端口服务吗?

A4

天翼云边缘安全加速平台—安全与加速服务服务购买企业版以及以上版本的客户,是支持特殊端口服务的,并支持在 CTWAF 控制台配置,但是仅限于控制列出的支持范围内选择。

用户可以查看网站的攻击情况吗?

A5

可以的,用户可以通过 CTWAF 控制台查看网站的攻击情况,安全报表中可以查看攻击的概览,日志管理中可以查看具体的攻击日志。

5.4 使用限制

Q1

用户是否可以直接订购套餐包进行使用?

A1

可以,用户订购套餐包后,即可通过 CTWAF 控制台接入服务,如果套餐包的服务不能 满足业务需求,并支持通过购买扩展服务来丰富安全能力和用量。

Q2

用户可以直接购买扩展服务进行使用吗?

A2

用户不能直接订购边缘安全加速平台—安全与加速服务服务的扩展服务,订购扩展服务 的前提是必须订购可套餐包

Q3

套餐包和扩展服务的有效期之间是否有关联?

A3

是的,扩展服务的有效期是根据套餐包的有效期一致的,如果用户的套餐包过期,扩展 服务的功能也随之失效。