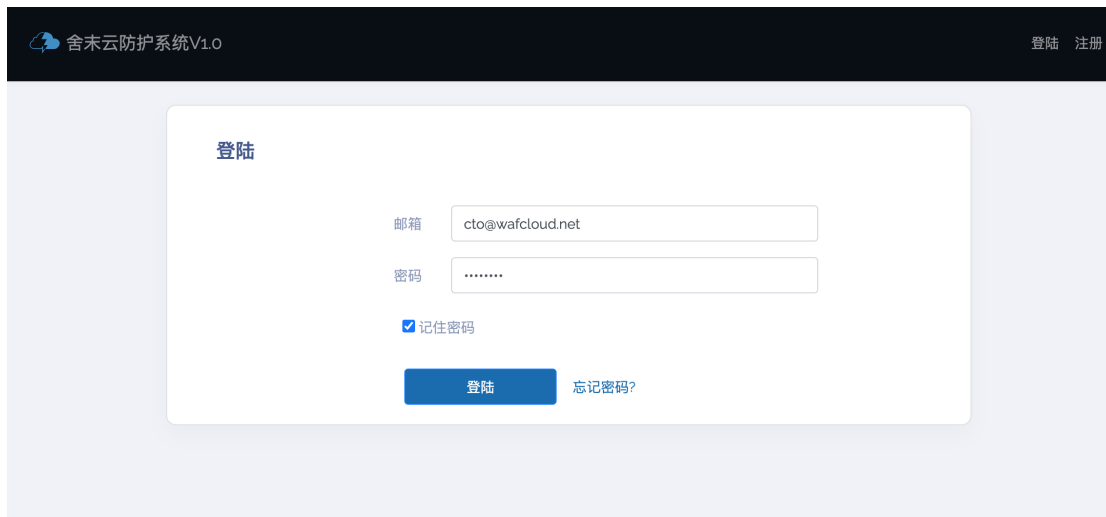


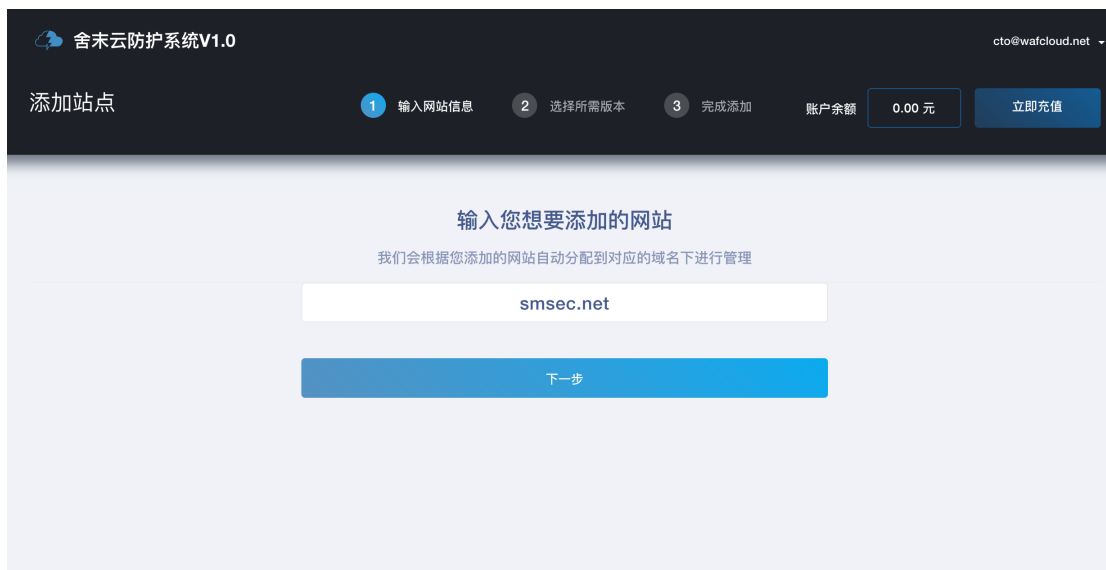
《操作手册》

1. 首先登录舍末云防护系统 V1.0

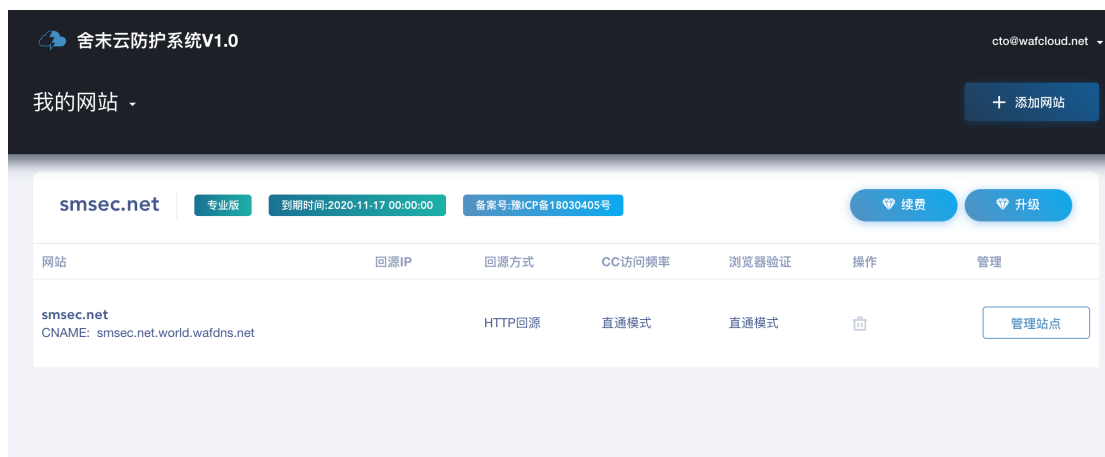


2. 添加一个网站并设定正确的源站信息

- 如果您是第一次使用舍末云防护系统 V1.0，请在下图所示位置输入您的网站并点击对勾添加



- 当您添加网站后我们会帮您自动跳转到我的网站:



- 然后再点击网站管理进入源站设定页面



- 您需要将您源站 IP 填写到“IP 地址或域名”下，选择您的回源协议，系统会自动帮您填写对应端口号。

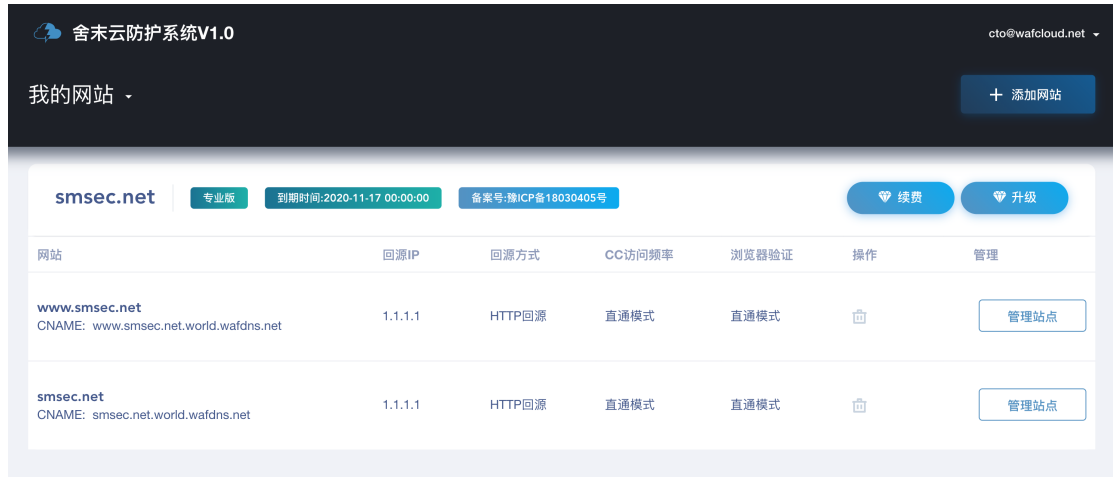
3. 激活网站并添加 CNAME 解析

当您添加站点后，在我的网站页面您可以看到我们为您生成的激活码和 CNAME 信息，您需要将激活码和 CNAME 信息添加到您的 DNS 解析记录中，来激活站点同时使用舍末云防护系统 V1.0 的服务。

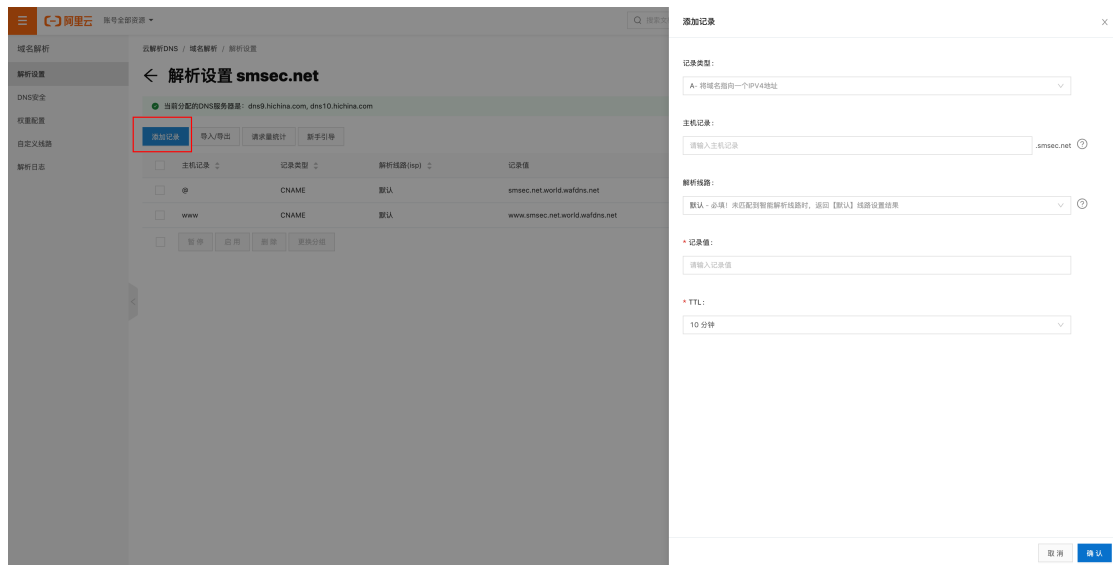
下面我们以使用阿里云 dns 的用户来举例，使用其他 DNS 解析服务的用户同理进行配置即可

4. 添加网站

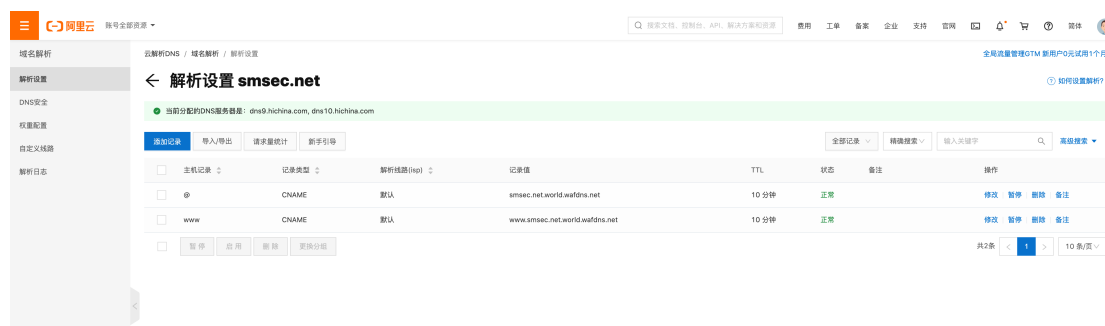
- 1. 在您激活域名之后，您可以看到每个站点所对应的 CNAME，点击 CNAME 右边第一个按钮复制 CNAME 信息。



- 2. 进入阿里云 DNS 管理后台，点击添加记录



- 3. 记录类型选择 CNAME，记录值填写您之前复制的 CNAME 记录



- PS:我们的防护服务和您添加的站点是一一对应的，所以您如果添加的是 example.com ,我们只会对 example.com 进行处理,并不会对 www.example.com 等其他子域名进行处理。所以您需要将 www.example.com 等之类等站点全部添加进来，我们才会对您添加的站点进行服务。

5. 开始使用舍末云防护系统 V1.0

- 好了，现在您的网站已经可以享受到舍末云防护系统 V1.0 的服务了，开始全新的云防护体验吧！

CC 防护模式详解

功能描述

CC 安全防护可以拦截机器恶意 CC 攻击，并提供不同模式的防护策略：访问频率、浏览器验证、客户端人机验证。将网站接入舍末云防护系统 V1.0 后，您可以为其开启 CC 安全防护，并根据实际需求调整相应防护策略。当您为网站开启 CC 防护后，舍末云防护系统 V1.0 将以关闭连接的方式帮您阻断检测出的 CC 攻击请求。

smsec.net

流量统计CC拦截CC记录WAF记录DDOS记录优化设置防护设置证书设置源站设置其它设置

DDOS防护

说明

企业级防DDOS集群，能够将乌云盾 BGP 高防包一键应用到网站，具备大流量 DDOS 防护能力

默认开启

智能防护模式

建议

当发现网站响应、流量、CPU、内存等指标出现异常时，则会触发 浏览器中验证(Javascript校验)，校验通过则可正常访问，校验不通过则直接拒绝，网站恢复正常时则自动切换为直通模式。

专业版以上享有

CC访问频率

说明

限制单个IP在规定时间内访问网页的频率(已排除静态资源)，将超过该阈值的IP进行阻断并拉黑，从而达到访问限制的目的，在实际场景中，您可以根据自身业务需求调整检测时间和触发防护的阈值，并选择合适的阻断模式，以达到更有针对性、更精细化的防护效果

直通模式

保存

浏览器验证

说明

此模式在访问频率模式的基础上，增加了对客户端Javascript执行能力的检测，通过Javascript加密并验证Cookie，能拦截大部分CC攻击，浏览器验证的目的是校验请求是否来自于真实浏览器(而非自动化工具脚本)，适用范围仅限于网页/H5，不适用于原生APP、API等环境

直通模式

保存

客户端人机验证

建议

reCAPTCHA 使用高级风险分析引擎和自适应，来防止自动化软件在您的网站上进行滥用活动，让您的网站彻底杜绝恶意爬虫，在高防节点边缘，化解CC攻击等恶意请求，申请reCAPTCHA Keys <https://www.google.com/recaptcha> 仅支持 (reCAPTCHA v3)

专业版以上享有

Web应用防火墙

说明

内置多种防护策略，可防护SQL注入、XSS跨站、Webshell上传、后门隔离保护、命令注入、非法HTTP协议请求、常见Web服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等安全防护，避免网站服务器被恶意入侵，保障业务的核心数据安全

1. CC 访问频率

- 在大规模 CC 攻击中，单台傀儡机发包的速率往往远超过正常用户的请求频率。这种情况下，直接针对请求源限速拉黑是有效的办法。
- 默认开启规则(60/分)这条规则的策略为：当一个 IP 在 60 秒内访问本域名下动态请求超过 60 次，则封禁该 IP 的请求 4 个小时，该规则可以作为一般中小型站点的预防性配置。

- 限制单个 IP 在规定时间内访问网页的频率(已排除静态资源)，将超过该阈值的 IP 进行阻断并拉黑，从而达到访问限制的目的，在实际场景中，您可以根据自身业务需求调整防护路径和触发防护的阈值，并选择合适的阻断类型，以达到更有针对性、更精细化的防护效果。
- 例如，为了预防登录接口被恶意高频撞库，60 秒内超过 20 次动态请求则进行封禁。
- 建议：默认使用此模式。此模式误杀较少，只针对特别异常的请求进行拦截。
- 适用范围： 网页/H5、原生 APP、API 等环境

2. 浏览器验证

- 此模式在访问频率模式的基础上，增加了对客户端 Javascript 执行能力的检测,通过 Javascript 加密并验证 Cookie，能拦截大部分 CC 攻击，浏览器验证的目的是校验请求是否来自于真实浏览器(而非自动化工具脚本)。
- 对于很多资讯类网站（如征信、租房、机票、小说等），大量的爬虫往往会造成带宽增大、负载飙升等异常，以及数据泄露等问题。针对爬虫问题，如果上述手段不能够很好的防御，推荐您使用浏览器验证，更有针对性的防御爬虫。
- 建议：当发现有 CC 访问频率模式无法拦截的 CC 攻击，并出现网站响应缓慢，流量、CPU、内存等指标异常时，可以选择浏览器验证模式。此模式拦截 CC 攻击效果较强。
- 适用范围仅限于网页/H5，不适用于原生 APP、API 等环境

3. 客户端人机验证

- 对于网页环境（包括 H5）中的一些关键接口，如登录、注册、投票、短信验证码等，推荐您使用[客户端人机验证]进行防护。
- 人机验证在关键接口页面中插入 JS 代码，采集用户在页面上的操作行为和环境信息，综合判断发送至关键接口的请求是否来自于真实的用户（而不是自动化工具脚本）。人机风控判定的依据主要来自于人机识别的结果，跟发送请求的频率、来源 IP 并没有关系，针对一些低频、分散的攻击请求有很好的效果。
- 适用范围仅限于网页/H5，不适用于原生 APP、API 等环境

在使用 CC 防护时，请注意以下事项

- *浏览器验证* | *客户端人机验证* 的目的是校验请求是否来自于真实浏览器（而非自动化工具脚本），适用范围仅限于网页/H5，不适用于原生 APP、API 等环境。针对原生 APP、API 等环境。
- 针对有可能被 CC 策略误伤的接口或 IP，您可以通过联系我们技术人员，根据客户端 IP、请求 URL 其统一加白。

说明

- 如果发现开启了 CC 防护仍然漏过较多攻击，建议您检查流量来源是否为舍末云防护系统 V1.0 云防御回源 IP。如果发现有攻击直接攻击源站，建议您联系舍末云防护系统 V1.0 技术人员，以确保源 IP 安全

6. 使用完毕后-退出-舍末云防护系统 V1.0



退出成功

