MCDN用户后台操作手册5.4

文档修订记录

版本号	修改日期	内容
5.1.0	2025.04	编写本文稿
5.4.0	2025.11	1. 概览页增加显示七层网站请求数图标、增加展示当前封禁IP 2. 七层网站组批量设置功能改版 3. 七层网站组增加支持关闭WAF和CC功能 4. 购买套餐页面改版

一、基本概述

1. 编写目的

为了使本产品使用人员熟悉总体产品操作流程和功能用途，遵循项目总体方案设计规范，特编制《MCDN系统后台操作手册》。

通过学习本手册，MCDN系统运维人员可以了解如何增加边缘服务器、日常故障排查、设置套餐、设置私享CNAME域名、协助用户排查使用问题、设置订单已付款等，为操作MCDN系统提供帮助。

2. 基本面向对象

本文档为MCDN的系统后台使用手册，适用于使用本产品运维人员、研发人员、客服人员等。

3. 术语及定义

术语	定义
源站	指您的用户运行业务的网站服务器，是加速分发数据的来源。 源站可用来处理和响应终端用户请求，当CDN节点没有缓存用户请求的内容时，CDN节点会从源站获取资源数据并返回给终端用户
CDN	（Content Delivery Network，内容分发网络）是通过将源站内容分发至靠近终端用户的加速节点，使终端用户可以就近获得所需的内容，解决Internet网络拥挤的状况，提高终端用户访问的响应速度和成功率，从而提升您的用户的业务的使用体验。 您的用户可以在CDN管理控制台添加加域名，然后前往域名服务商处配置CNAME解析，即可启用CDN加速。还可以根据业务需要，为加域名进行缓存、安全、性能优化配置，优化加速效果、缓解源站压力。
	（英文：HTTP Status Code），是用来表示HTTP响应状态的数字代码，可用来判断和分析服务的运行状态。当客户端（例如浏览器）向服务器发出请求时，服务器会返回一个包含HTTP状态码信息头来响应客户端的请求，通过状态码告诉客户端当前请求响应的状态。 HTTP常见状态码分类：

HTTP状态码	1xx：消息 2xx：成功 3xx：重定向 4xx：客户端错误 5xx：服务器错误
管理节点	负责跟边缘节点通讯，向边缘节点下发指令的服务器。
边缘节点	负责给用户提供网站加速服务的服务器，定时从管理节点获取指令。最终接入的用户之间具有较中间环节的网络节点，对最终接入用户有相对于源站而言更好的响应能力和连接速度。
WAF	Web应用防火墙（Web Application Firewall，简称WAF）
CC 攻击	CC 攻击是通过大量正常请求耗尽目标服务器资源的攻击方式。
主IP	服务器厂商提供的第一个IP
从IP	服务器厂商提供多个IP时非第一位的IP
加速域名	接入CDN用于加速、终端用户实际访问的域名。
CNAME记录	指域名解析中的别名记录，用来把一个域名解析到另一个域名（CNAME域名），再由CNAME域名来解析到需要访问的服务器IP地址。
CNAME域名	是CDN生成的，当您在MCDN控制台添加加速域名后，系统会为加速域名分配一个9位随机字符开的CNAME域名。
DNS	（Domain Name System）即域名解析服务，主要功能是将域名解析为网络可以识别的IP地址，域名解析。
SSL/TLS	（Secure Sockets Layer）即安全套接层协议，SSL协议位于TCP/IP协议与各种应用层协议之间，可以有效协助Internet上的应用软件提升通讯时的资料完整性及安全性。IETF将SSL标准化后名称改为TLS（Transport Layer Security），即传输层安全协议，因此通常将两者并称为SSL/TLS。
DNS时间	指从浏览器终端发起的访问请求开始，到浏览器终端获得最终访问主机IP地址所消耗的时间。
TCP时间	指客户端与目标服务器建立TCP连接所消耗的时间。
SSL时间	指客户端和Web服务器建立安全套接层（SSL）连接的消耗时间。
建连时间	建立连接时间，简称为建连时间。如果CDN节点使用HTTP协议加速客户业务，建连时间包含“DNS时间+TCP时间”；如果CDN节点使用HTTPS协议加速客户业务，建连时间包含“DNS时间+TCP时间+SSL时间”。建立连接的时间长短，可以反映CDN服务的节点资源覆盖的丰富程度以及调度能力。
响应时间	指浏览器发出HTTP请求后，Web服务器进行后台处理以及响应的时间。
下载用时	指用户收到Web服务器返回的第一个数据包，到完成下载的总时间。
首包时间	指从客户端开始发送请求到收到服务器端返回的第一个HTTP协议数据包之间所需要的时间，首包间可以反映出CDN服务节点的整体性能。
回源HOST	即CDN节点回源时实际请求的域名。当源站服务器上提供多个域名服务时，您可根据业务需求指CDN节点回源时访问的具体域名。具体配置，可参见配置默认回源HOST。
回源协议	指CDN节点回源时使用的协议，有可能与客户端访问资源时使用的协议相同，也有可能不相同。
缓存过期时间	指资源在CDN节点上缓存的时长。资源过期后会自动从CDN节点删除，用户向CDN节点发起的访请求会被判定为未命中缓存，CDN节点会自动回源站获取最新资源返回给用户，并缓存到CDN节点。
CDN缓存命中率	包括字节命中率和请求命中率，缓存命中率越高，性能越好。
HSTS	（HTTP Strict Transport Security，HTTP 严格传输安全），是一种网站用来声明它们只能使用全连接（HTTPS）访问的方法。网站可通过声明HSTS，来强制客户端（如浏览器）只能使用HTTPS与服务器连接，拒绝所有的HTTP连接并阻止用户接受不安全的SSL证书，降低第一次访问

	求被拦截的风险。

二、MCDN概述

1. 什么是MCDN?

MCDN，全称 MasterCDN，是一款强大的自建高防CDN产品。能够让用户在短时间内架设一个全局自主可控的高防CDN系统。

MCDN从立项到上线，经历三年多专注的研发以及严苛的生产环境测试。我们自主开发了防CC攻击系统、优化回源算法、简化防火墙的操作、制作更便捷的节点管理系统、制作节点攻击状态监控系统，力求让整套系统操作简单、稳定好用。

2. MCDN的优势

安全防护

集WAF防护、CC防护、DDoS 防护等多种安全防护策略于一体，为您的业务保驾护航

极速稳定

配置策略秒级生效，即使站点数量繁多也能保持稳定

性能优越

智能缓存及多种优化技术，结合自研拥塞加速算法，提升网络负载，降低源站负载压力，保障访问质量

便捷易用

灵活的缓存策略，丰富、便捷的自助配置功能，轻松应对各类复杂的场景需求

三、操作指南

1. 注册及登录

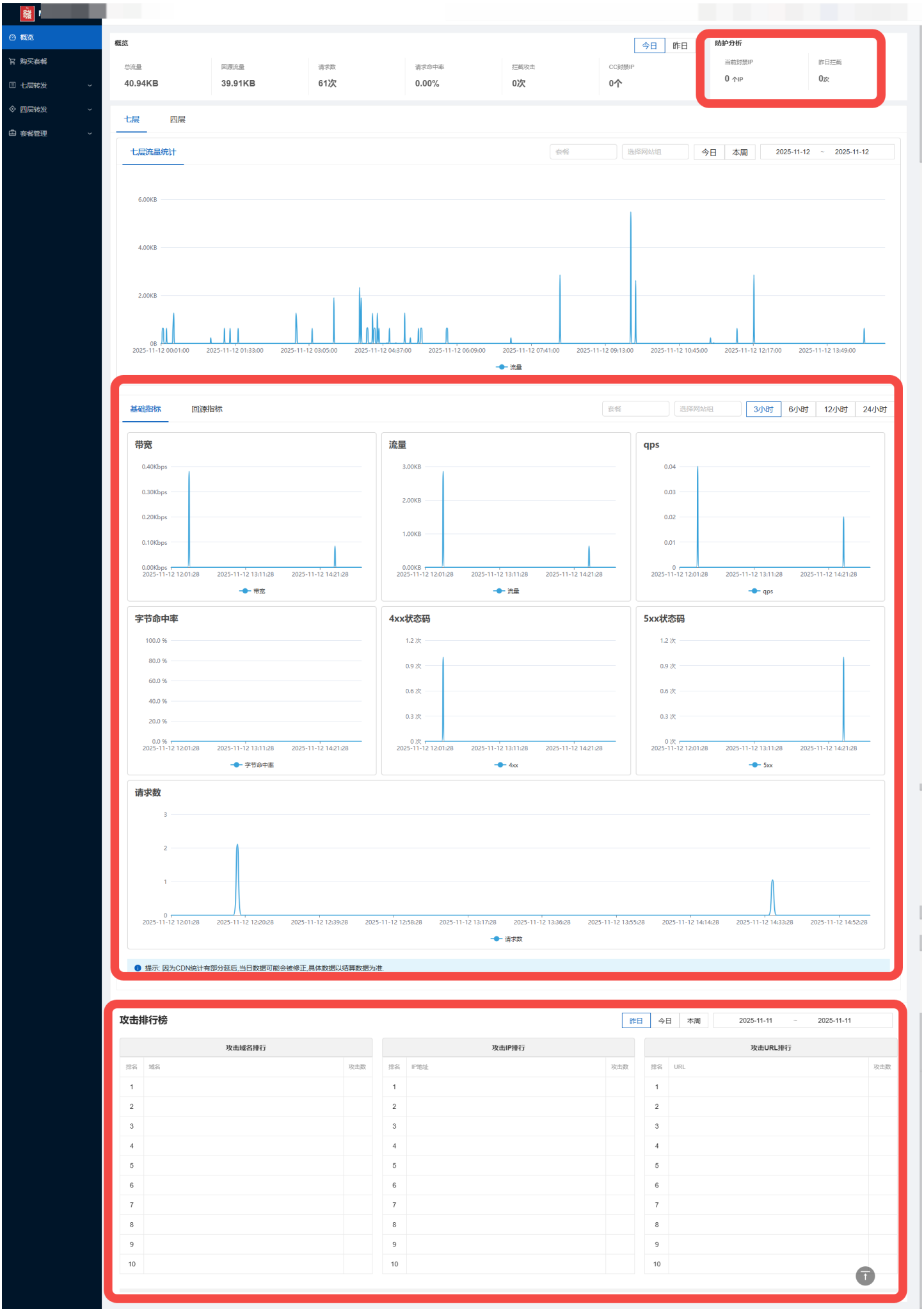
1.1 注册

系统开放注册，注册时天下邮箱号、接受邮件验证码、输入密码即可完成注册。

1.2 登录

输入用户名及密码，即可登录系统。

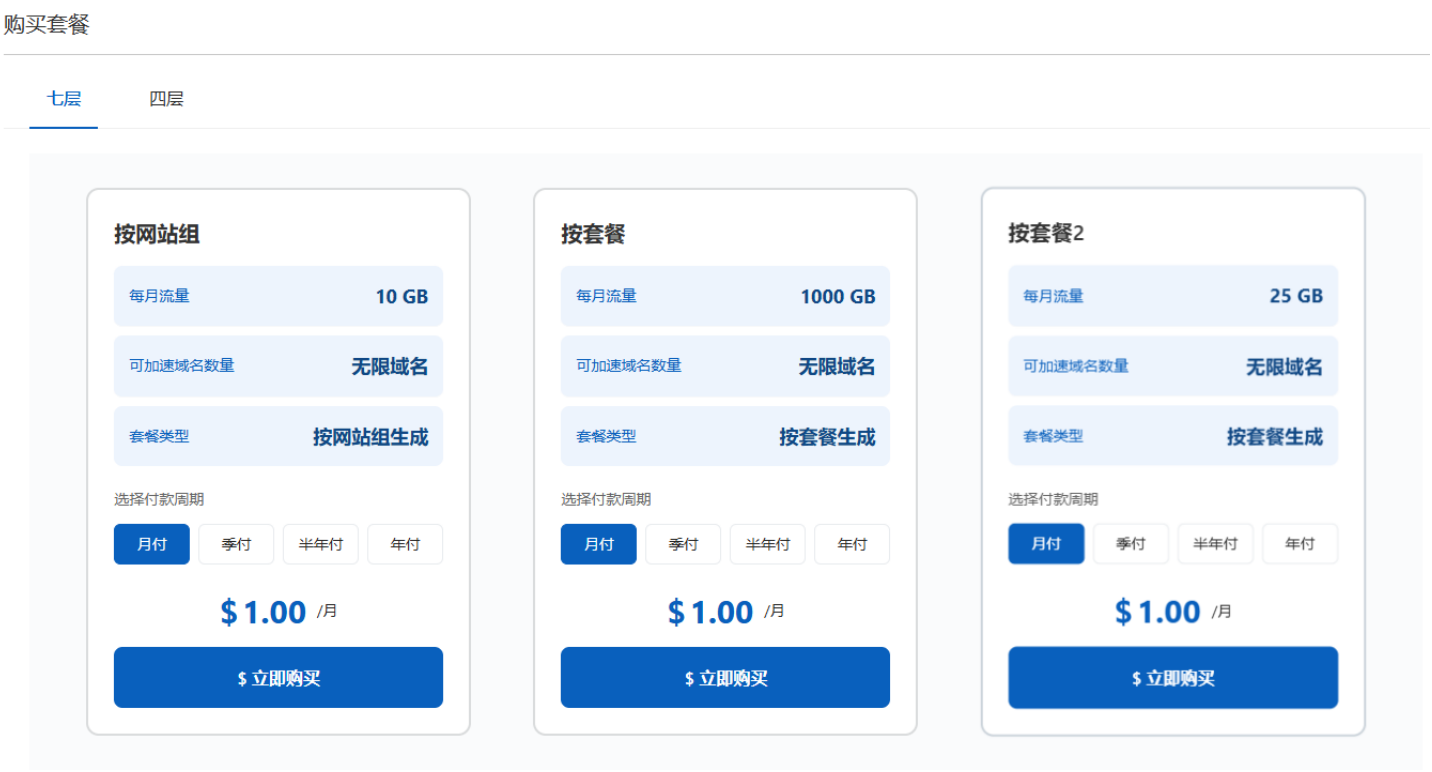
2. 概览


概览
购买套餐
七层转发
四层转发
套餐管理
概览
今日
昨日
总流量
40.94KB
回源流量
39.91KB
请求数
61次
请求命中率
0.00%
拦截攻击
0次
CC封禁IP
0个
防护分析
当前封禁IP
0 个IP
昨日拦截
0次
七层
四层
七层流量统计
套餐
选择网站组
今日
本周
2025-11-12 ~ 2025-11-12
6.00KB
4.00KB
2.00KB
0B
2025-11-12 00:01:00
2025-11-12 01:33:00
2025-11-12 03:05:00
2025-11-12 04:37:00
2025-11-12 06:09:00
2025-11-12 07:41:00
2025-11-12 09:13:00
2025-11-12 10:45:00
2025-11-12 12:17:00
2025-11-12 13:49:00
流量
基础指标
回源指标
套餐
选择网站组
3小时
6小时
12小时
24小时
带宽
0.40Kbps
0.30Kbps
0.20Kbps
0.10Kbps
0.00Kbps
2025-11-12 12:01:28
2025-11-12 13:11:28
2025-11-12 14:21:28
带宽
流量
3.00KB
2.00KB
1.00KB
0.00KB
流量
qps
0.04
0.03
0.02
0.01
0
qps
字节命中率
100.0 %
80.0 %
60.0 %
40.0 %
20.0 %
0.0 %
字节命中率
4xx状态码
1.2 次
0.9 次
0.6 次
0.3 次
0 次
4xx
5xx状态码
5xx
请求数
3
2
1
0
2025-11-12 12:20:28
2025-11-12 12:39:28
2025-11-12 12:58:28
2025-11-12 13:17:28
2025-11-12 13:36:28
2025-11-12 13:55:28
2025-11-12 14:14:28
2025-11-12 14:33:28
2025-11-12 14:52:28
请求数
提示: 因为CDN统计有部分延后,当日数据可能会被修正,具体数据以结算数据为准.
攻击排行榜
昨日
今日
本周
2025-11-11 ~ 2025-11-11
攻击域名排行
排名
域名
攻击数
攻击IP排行
IP地址
攻击URL排行
URL

登录后如果没有购买过套餐系统会引导购买套餐，如果已经购买了套餐系统会进入概览页面，如上图。

系统分为七层和四层展示各运营数据，也支持按套餐、按网站组展示流量数据。

3. 购买套餐



MCDN的套餐是按月计算流量，你可以按照您的流量和时间需求进行购买，也可以联系客服定制一个专属套餐。

点击 立即购买 按钮后，进入支付界面，如下图：

您可以选择您适合的付款方式，然后点击确认支付即可完成购买。

支付成功之后系统会引导您进入 我的套餐 页面，如下图：

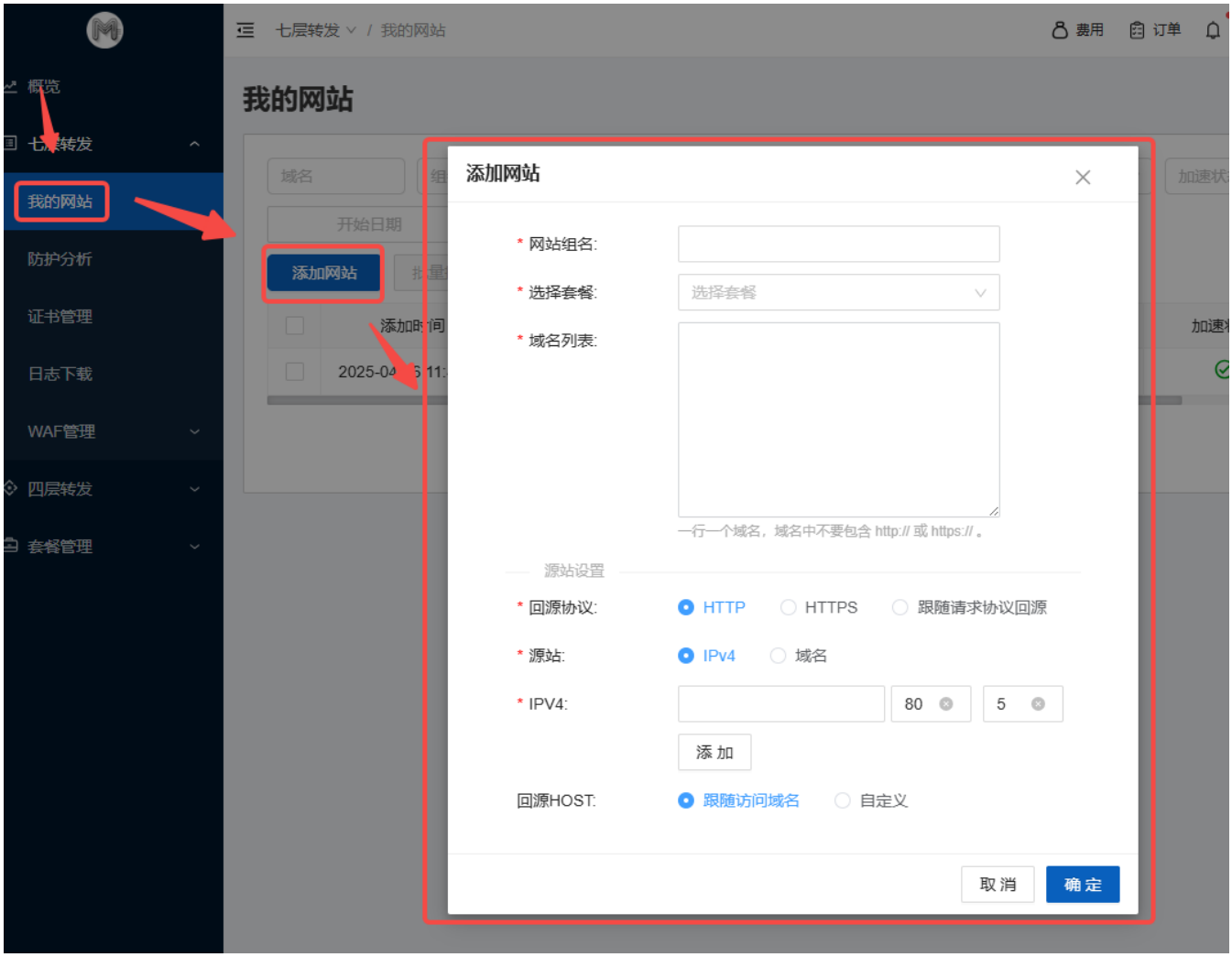
4. 七层转发

4.1 我的网站

该页面提供全部七层网站组添加及管理功能。

4.1.1 新增网站组

购买套餐可以添加网站组，点击 七层转发-我的网站-添加网站，即可弹出下图所示窗口。

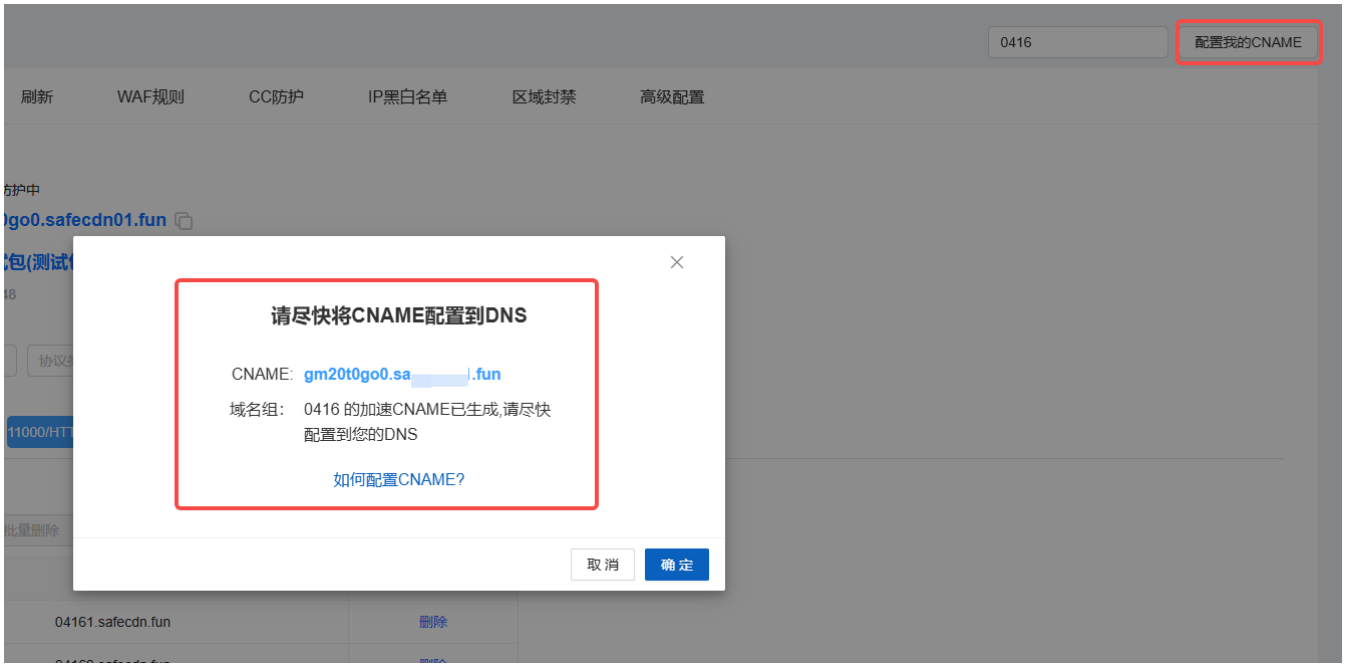


- 网站组名：该网站组名称，支持中英文及数字。
- 选择套餐：选择已购买好的套餐即可。
- 域名列表：输入域名，一行一个，支持批量输入。例如：abc.com
- 回源协议：支持三种回源协议，http、https、跟随请求协议。
- 源站：源站支持两种类型，IPv4或域名形式。
- （源站）IPV4：源站IP地址（目前仅支持IPv4协议），端口，权重（1-10之间，数字越大权重越高）
- （源站）域名：源站域名（不要包含http://或https://），端口，权重（1-10之间，数字越大权重越高）
- 回源HOST：支持两种形式，1，跟随访问域名（即加速域名是abc.com则回源host也是abc.com），2，自定义（支持用户设置一个回源host）

4.1.2 配置CNAME

添加网站组后进入该网站组的管理，如下图：

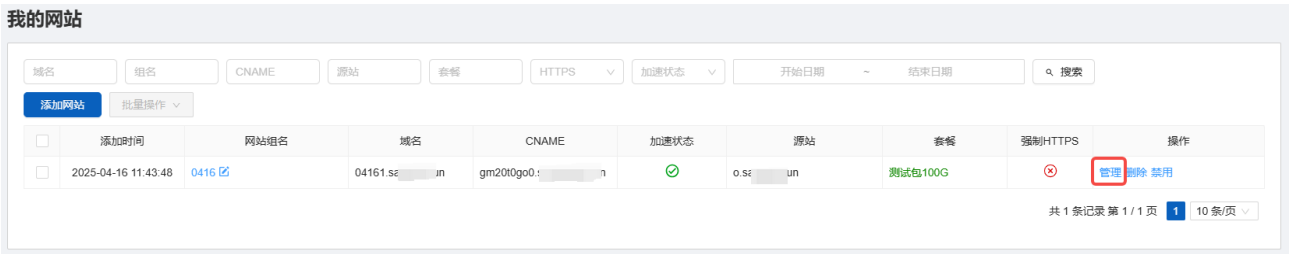
点击管理，点击右侧 配置我的CNAME 按钮，弹出下图：



按照界面提示将对应的cname值放入你的域名DNS解析中，如下图：

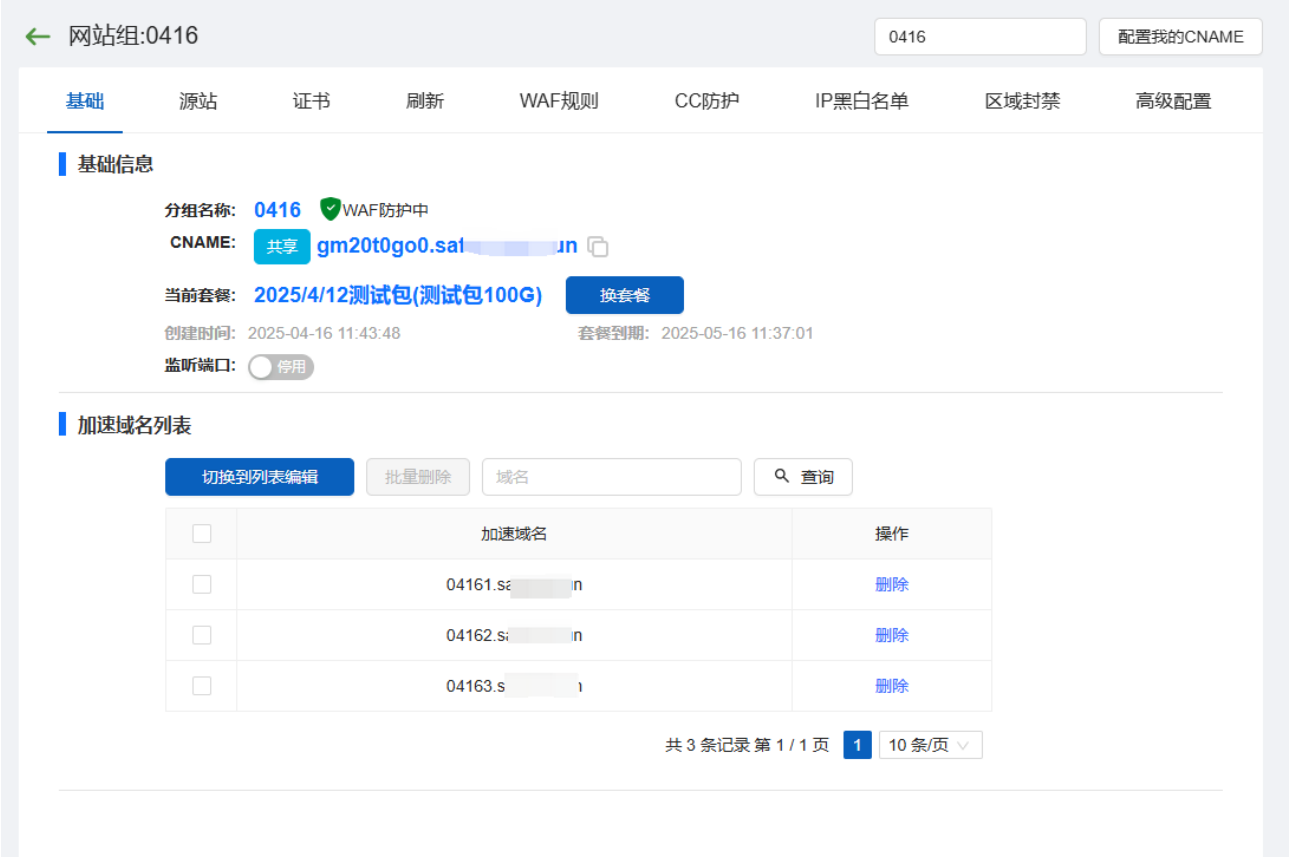
即可完成加速。

4.1.3 管理网站组



点击管理可以进入网站组的详细管理界面。

4.1.3.1 基础



基础中包含两部分：基础信息和加速域名列表。

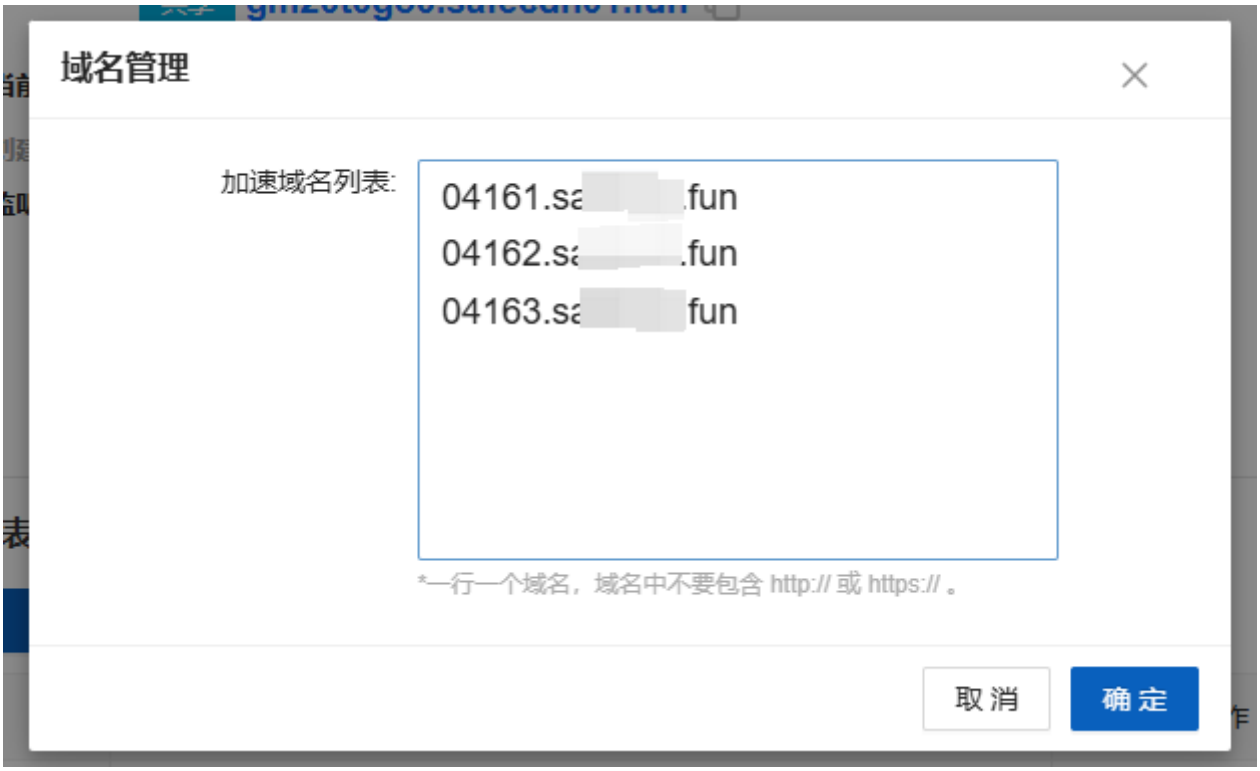
4.1.3.1.1 基础信息

- 分组名称：该网站组的名称
- CNAME：系统签发给该网站组的CNAME，用户可以用该CNAME配置到其加速域名的DNS上实现网站加速。CNAME分为共享CNAME和独享CNAME，具体根据套餐的不同而不同。
- 当前套餐：当前使用的套餐，可以支持更换套餐。更换套餐后对应的加速节点、流量扣除都会以新套餐的所包含的权益为准。

- 监听端口：该项默认为不开启。当监听端口不开启时，系统支持通过80和443两个端口访问该加速网站。如果开启监听端口时，系统支持按照用户的设置来访问网站。以上图为例，上图仅支持 http://abc.com:8899 和 https://abc.com:11000 这两个URL访问加速。

4.1.3.1.2 加速域名列表

你可以单独删除某条加速域名，也可以点击切换到列表编辑可以批量增加和删除加速域名列表，点击后如下图：



在列表框中，您可以批量添加加速域名，一行一个，删除同理。

4.1.3.2 源站

点击源站页签，即可进入源站信息的编辑界面。如下图：

点击右侧的 设置 按钮，即可进入对应的设置。

4.1.3.2.1 源站配置

你可以在这个界面配置源站类型、源站地址、回源协议。

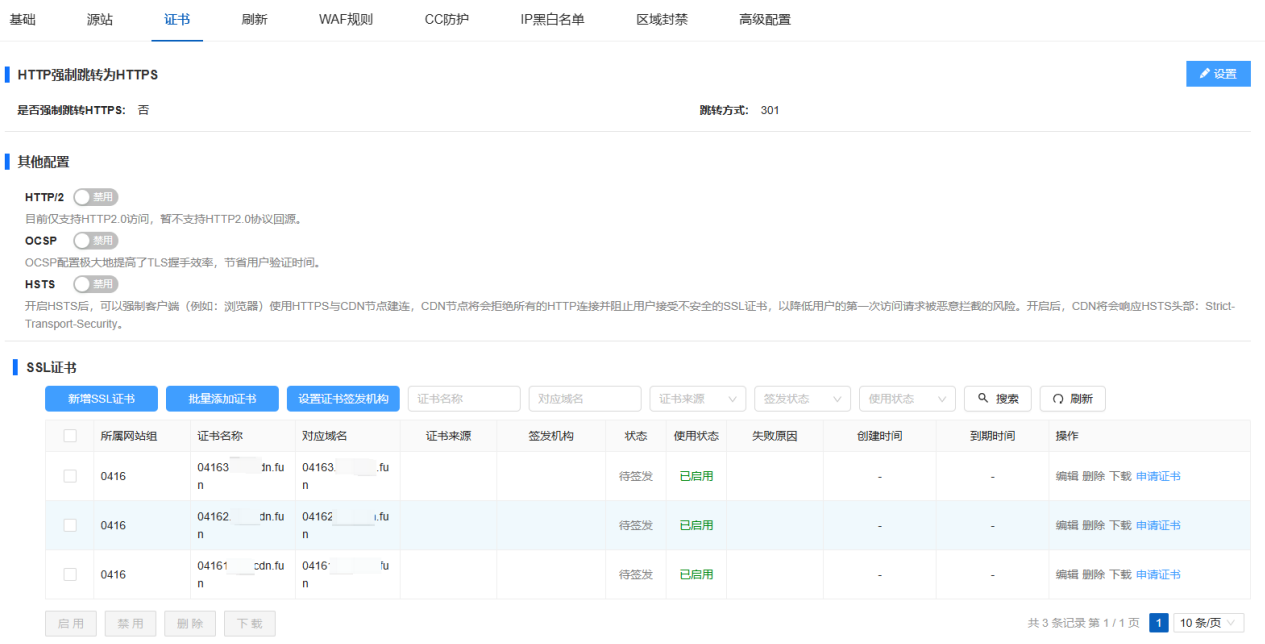
- 回源超时：设置源站的回源超时时间，建议默认为0即可。

- 连接超时：设置源站的连接超时时间，建议默认为0即可。

4.1.3.2.2 回源HOST

回源HOST支持设置为跟随访问域名和自定义两种形式。

4.1.3.3 证书



系统会自动给所有已经配置好了CNAME的加速网站申请证书，无需用户操作，只需要通过https访问一次即可。

例如，加速网站的域名是 abc.com 已经配置好了系统签发的CNAME，这时仅需要通过浏览器访问： https://abc.com 一分钟后证书就会显示签发成功。

4.1.3.3.1 HTTP强制跳转为HTTPS

点击设置，弹出如下窗口：

4.1.3.3.2 其它配置

- HTTP/2：目前仅支持HTTP2.0访问，暂不支持HTTP2.0协议回源。
- OCSP：OCSP配置极大地提高了TLS握手效率，节省用户验证时间。
- HSTS：开启HSTS后，可以强制客户端（例如：浏览器）使用HTTPS与CDN节点建连，CDN节点将会拒绝所有的HTTP连接并阻止用户接受不安全的SSL证书，以降低用户的第一次访问请求被恶意拦截的风险。开启后，CDN将会响应HSTS头部：Strict-Transport-Security。

4.1.3.3.3 SSL证书

系统支持用户自己添加单个证书，也支持批量添加证书，点击上方蓝色按钮即可。

系统支持用户选择证书签发机构，如下图：

目前仅支持 Let's Encript 和 Zero SSL 两家之间选择。

在配好CNAME之后点击 申请证书 或者直接以https访问一次该域名，稍等一下即可看到该域名的证书已经申请成功，如上图。

用户可以点击右侧按钮下载该证书。

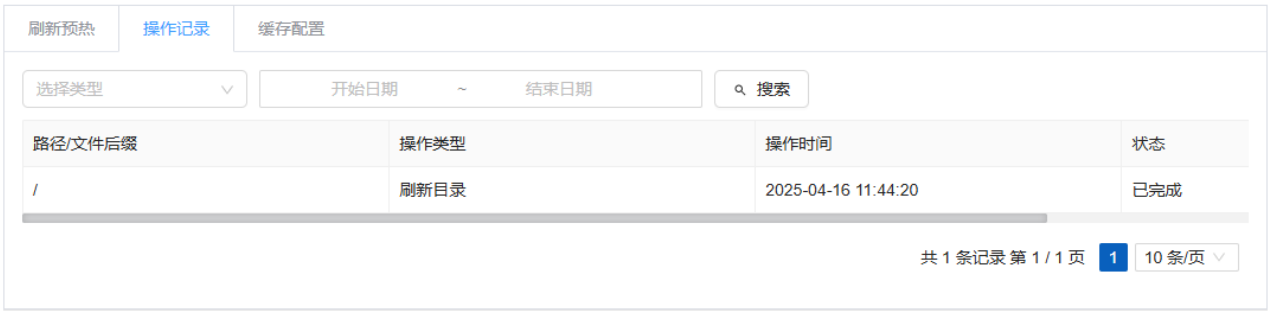
4.1.3.4 刷新

刷新即刷新该网站组的缓存，也可以设置缓存规则，如下图：

4.1.3.4.1 刷新预热

- 刷新目录：输入一个或多个目录（写相对路径，例如：“/”代表整个网站组，"/mulu/"代表网站组根目录下面的mulu文件夹），每行一个，点击即可清除该目录的缓存。
- 刷新URL：输入一个或多个URL（例如:"/apage.html"），每行一个，点击即可清除该URL的缓存。
- 预热：输入一个或多个需要加入的文件地址，例如："/download/game.apk"。

4.1.3.4.2 操作记录



所有的刷新操作都会在操作记录中记录下来并返回操作状态。

4.1.3.4.3 缓存配置

所有网站都是默认开启了网站缓存，如果不需要仅将CDN的加速节点用作转发，可以关闭网站缓存。

4.1.3.4.4 添加缓存配置规则

- CDN节点缓存网站内容的规则，支持按照目录、文件拓展名、单个路径、首页来设置。
- 支持设置缓存过期时间，如果为0表示不缓存。

- 权重介于1到10之间，数值越大，执行的优先级越高。

4.1.3.4.5 复制规则

如果用户有其它网站组，已经设好了自己独有的缓存规则，那么可以选择那个网站组的规则直接复制过来，免去用户重复设置的麻烦。

4.1.3.4.6 设置缓存生成方式

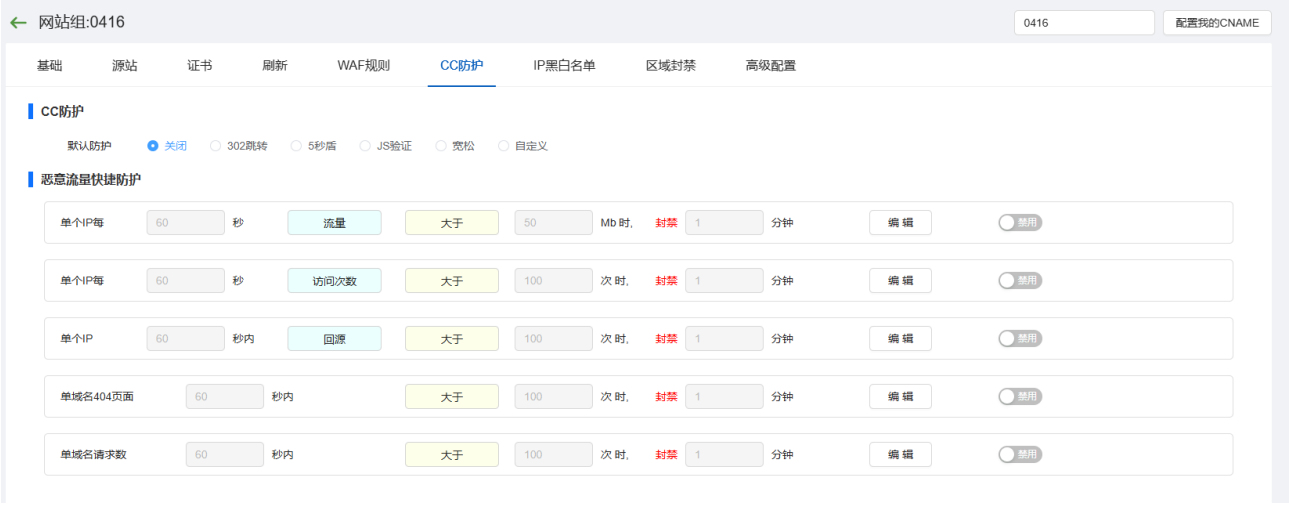
MCDN支持一个网站组设置多个域名，所以用户可以配置是否单个网站组中的所有域名都用同一份缓存还是按照不同域名生成不同缓存。

一般默认设置为按域名生成缓存。

4.1.3.5 WAF规则

用户可以在这里设置某个网站组专用的WAF规则。点击右侧选择WAF规则即可将该规则应用到这个网站组。具体WAF规则参见后面防护分析中的waf规则设置。

4.1.3.6 CC防护



系统提供CC防护功能，你可以设置详细的CC规则（参见后面防护分析中CC规则模块），也可以设置恶意流量快捷防护。

用户可以直接按照界面上的逻辑简单开启恶意流量屏蔽规则。

4.1.3.6.1 关于单个网站设置CC防护时的可选项说明：

- **关闭**
  - 不开启CC防护。
- **302跳转**
  - 检查请求是否是通过浏览器访问，如果不是浏览器，或者不支持跟随跳转，该请求将被拦截。
  - 具体参数：匹配器为匹配所有资源；过滤器为302跳转60秒内总请求不超过10次；动作为封禁。
  - 意思是如果60秒内出现10次以上的302跳转错误，该IP将被封禁30分钟。
- **5秒盾**
  - 每个请求都将等待5秒钟倒计时。
  - 具体参数： 匹配器为匹配所有资源；过滤器为5秒盾，60秒内最大出现次数不超过5次；动作为封禁。
  - 意思是如果60秒内出现5次以上的5秒盾跳转错误，该IP将被封禁30分钟。
- **JS验证**
  - 每个请求都将接受JS验证。
  - 具体参数： 匹配器为匹配所有资源；过滤器为浏览器识别，60秒内最大失败次数不超过10次；动作为封禁。
  - 意思是如果60秒内出现10次以上的JS验证错误，该IP将被封禁30分钟。
- **宽松模式（建议使用）**
  - **适合大部分站点的规则**，但不一定适合全部。

- 具体参数： 匹配器为匹配所有资源；过滤器为请求速率2秒内总请求不超过800次，单个URL不超过300次；动作为封禁。
- 意思是如果2秒内单个IP发起的请求次数超过800次，或者对某一个URL的请求数超过300次，该IP将被封禁30分钟。

4.1.3.7 IP黑白名单

IP白名单是所有规则中最优先的，如果一个IP在白名单中，那么所有的WAF规则、区域封禁、CC规则都不会对其生效。

点击右侧按钮可以添加IP黑白名单。如下图：

按图所示添加即可。

4.1.3.8 区域封禁

区域封禁默认是关闭的，如下图：

开启之后，如下图：

点击上面页签可以选择封禁中国境内还是中国境外，点击编辑，即可勾选对应要封禁的区域。

4.1.3.9 高级配置

高级配置中包含：是否启用GZIP、是否启用WebSocket、是否启用跨域访问、URL转向四个模块。

4.1.3.9.1 是否启用GZIP

Gzip 是一种数据压缩算法，开启后 CDN 会对传输的文件（如 HTML、CSS、JavaScript、JSON 等文本类型文件）进行压缩处理。能一定程度上提升网站访问速度。

4.1.3.9.2 是否启用WebSocket

如果需要启用WebSocket功能请开启。

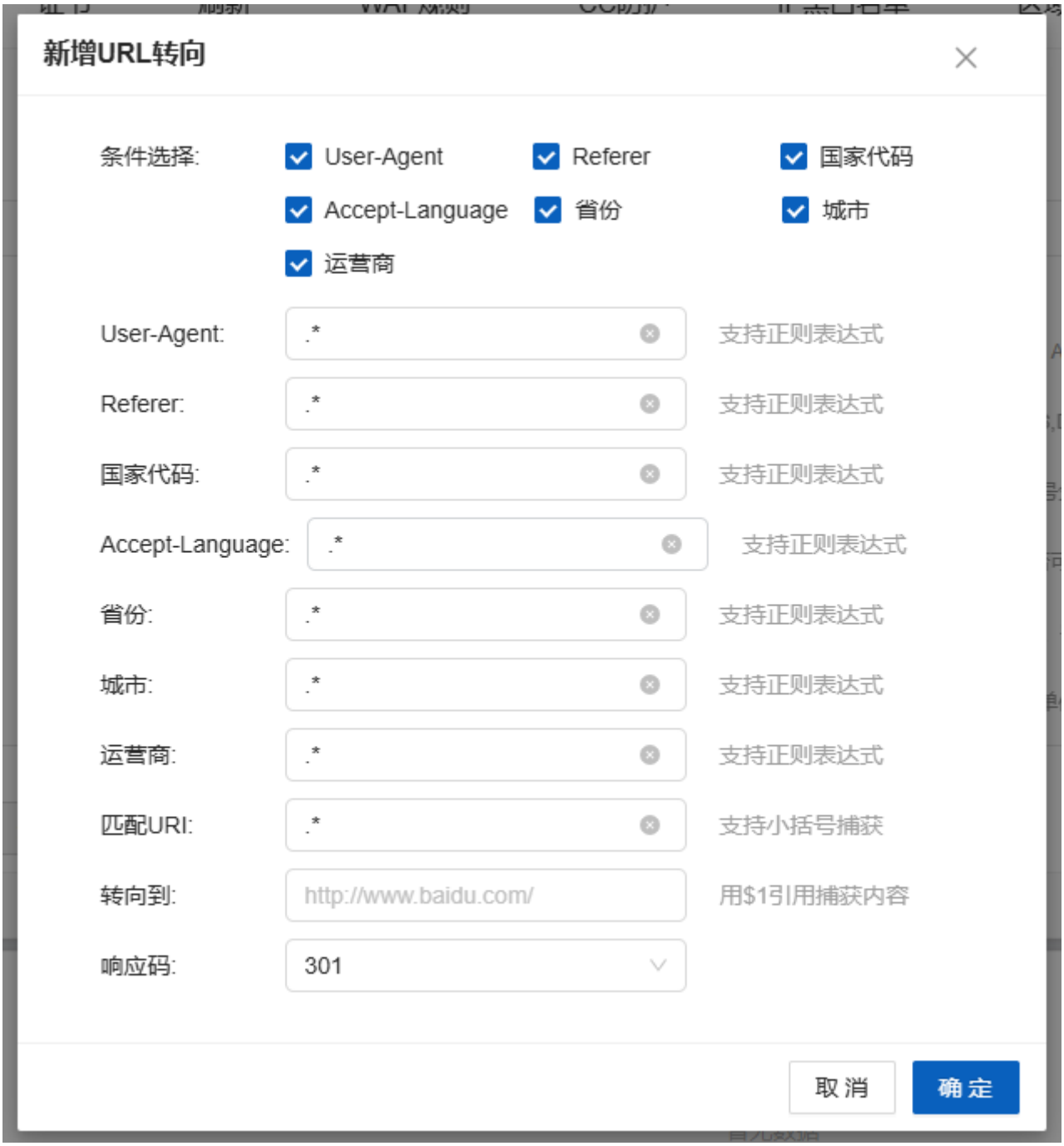
4.1.3.9.3 是否启用跨域访问：

开启之后如下图：

- allow_origin：填*或者http://domain.com，如果 AllowCredentials 为 true，则不能为 *
- allow_methods：有效值为GET,POST,OPTIONS,DELETE,PUT,PATCH,HEAD，*表示任意方式
- allow_headers：允许添加哪些自定义的头，逗号分隔多个，* 表示任意头
- expose_headers：针对本站的HTTP响应头，是否可读取，否则浏览器的XMLHttpRequest对象不读自定义头，* 表示所有头都可读
- allow_credentials：是否允许附带本站的【Cookie、客户端证书或自定义Http头】
- max_age：下次预检的间隔时间是多久，单位为秒

4.1.3.9.4 URL转向

点击新增，可以看到如下界面：



可以根据条件来判断所有的访问是否跳转到指定的URL。

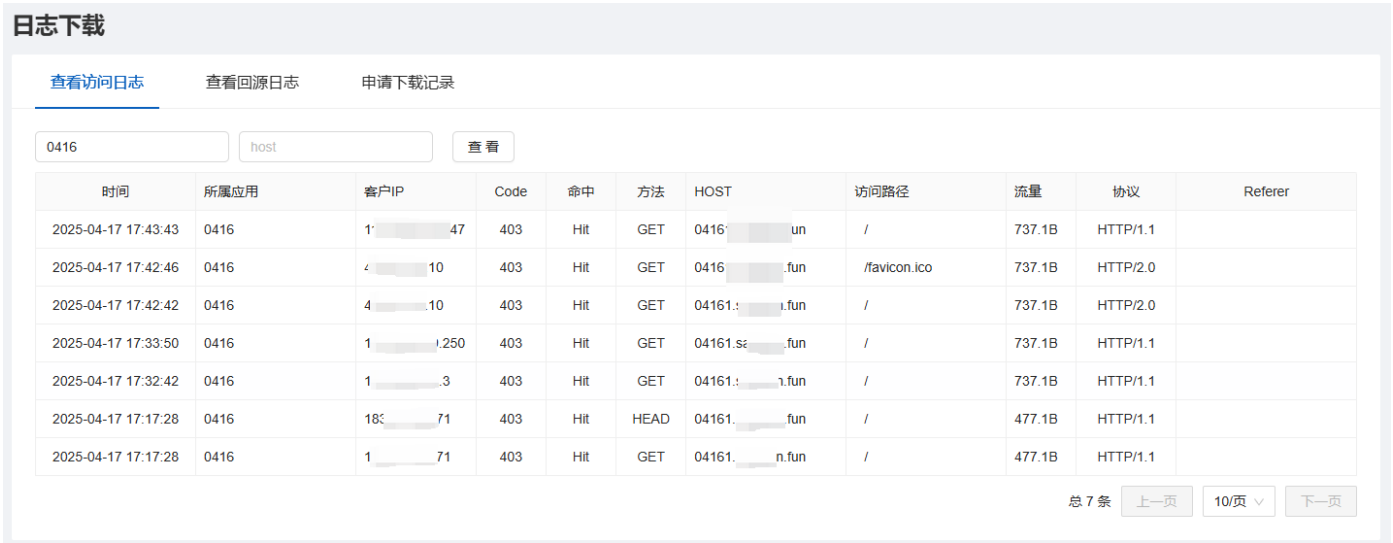
4.2 证书管理

可以新增单个证书，也可以批量添加证书，如果证书已签发可以下载该证书。

4.3 日志下载

日志下载包含三个模块：

4.3.1 查看访问日志

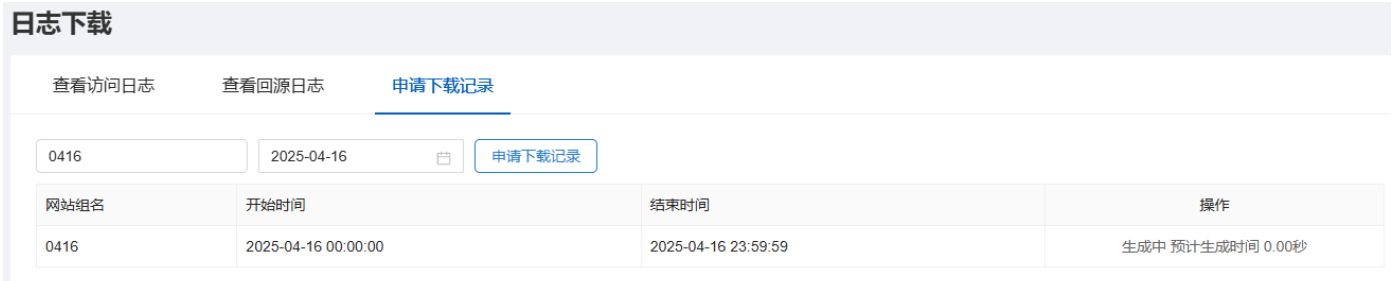


选择网站组后点击查看按钮，系统会显示最新的访问日志。

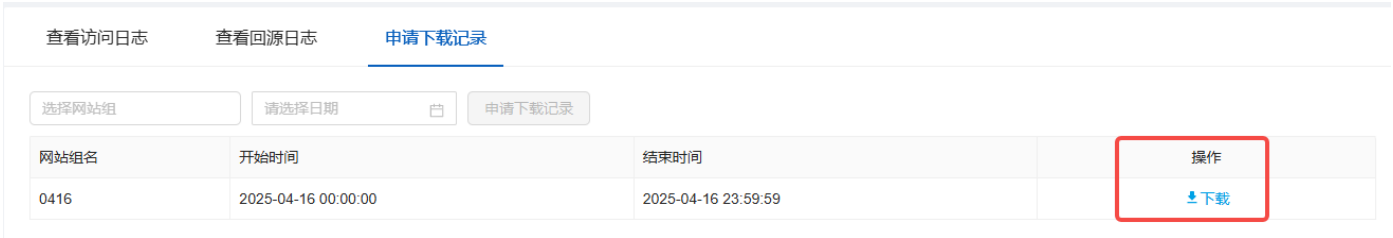
4.3.2 查看回源日志

可以查看全部或者某个网站组某一天的回源日志。

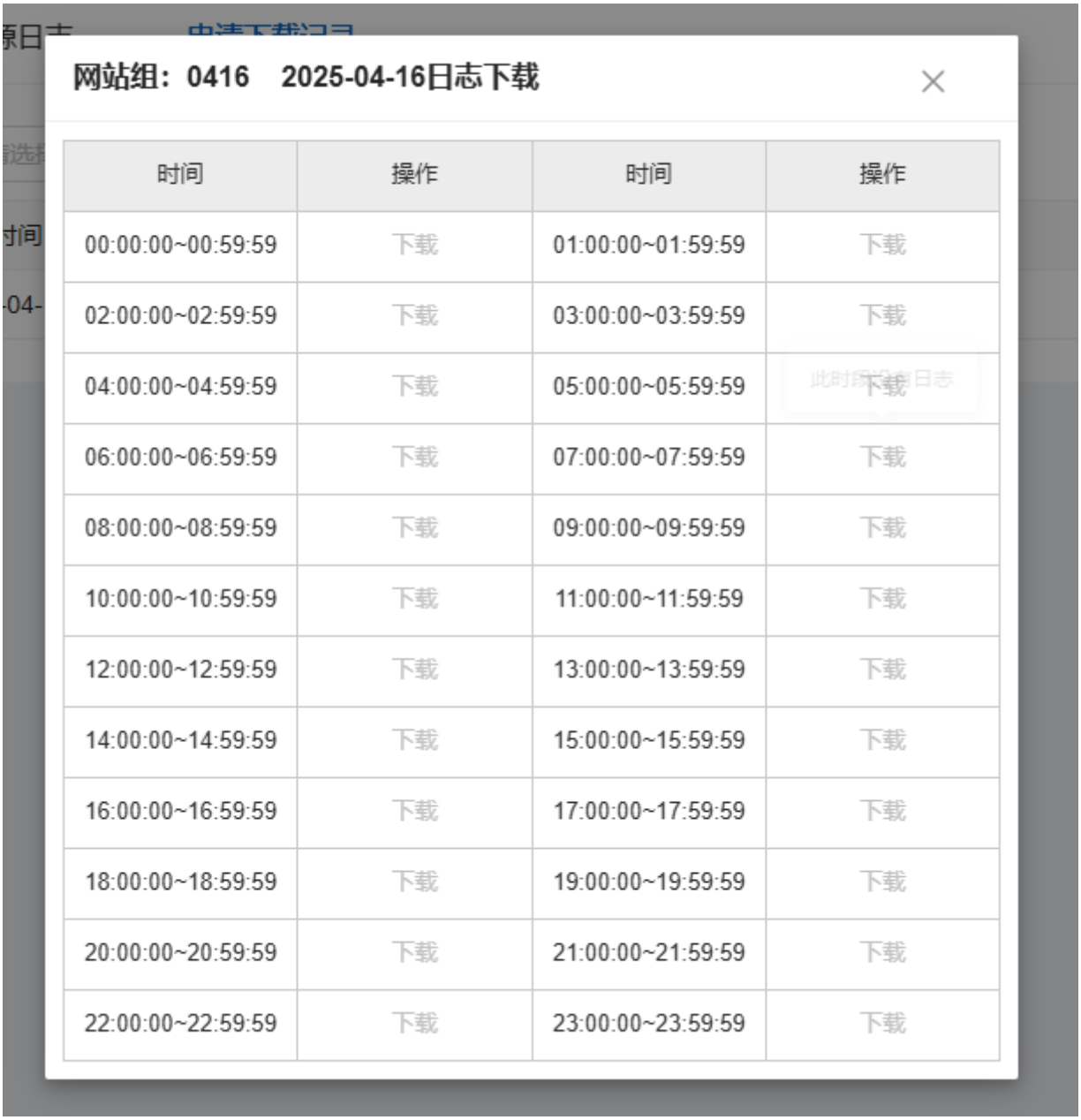
4.3.3 申请下载记录



日志下载采用申请下载模式，用户选择一个网站组，然后指定日期，点击申请下载按钮。如果该网站组有访问日志，系统就会直接以每小时为基准生成24个日志文件的压缩包，用户可以按需下载。



点击下载按钮，弹出如下对话框：



如果改天的对应时间区间有访问日志，下载按钮就可以点击，否则下载按钮置灰，不可点击。

4.4 WAF管理

WAF管理就是设置所有防护规则和记录所有防护日志的地方，包含如下七个模块。

4.4.1 WAF规则

WAF，Web应用防火墙（Web Application Firewall，简称WAF）您可以自定义访问控制规则和频率控制规则，防御符合规则的请求。也可以设置CC防御规则，用于防止恶意高频请求。

4.4.1.1 自定义WAF规则

用户可以按照自身需求设置WAF规则，点击添加自定义WAF规则按钮，弹出如下窗口：

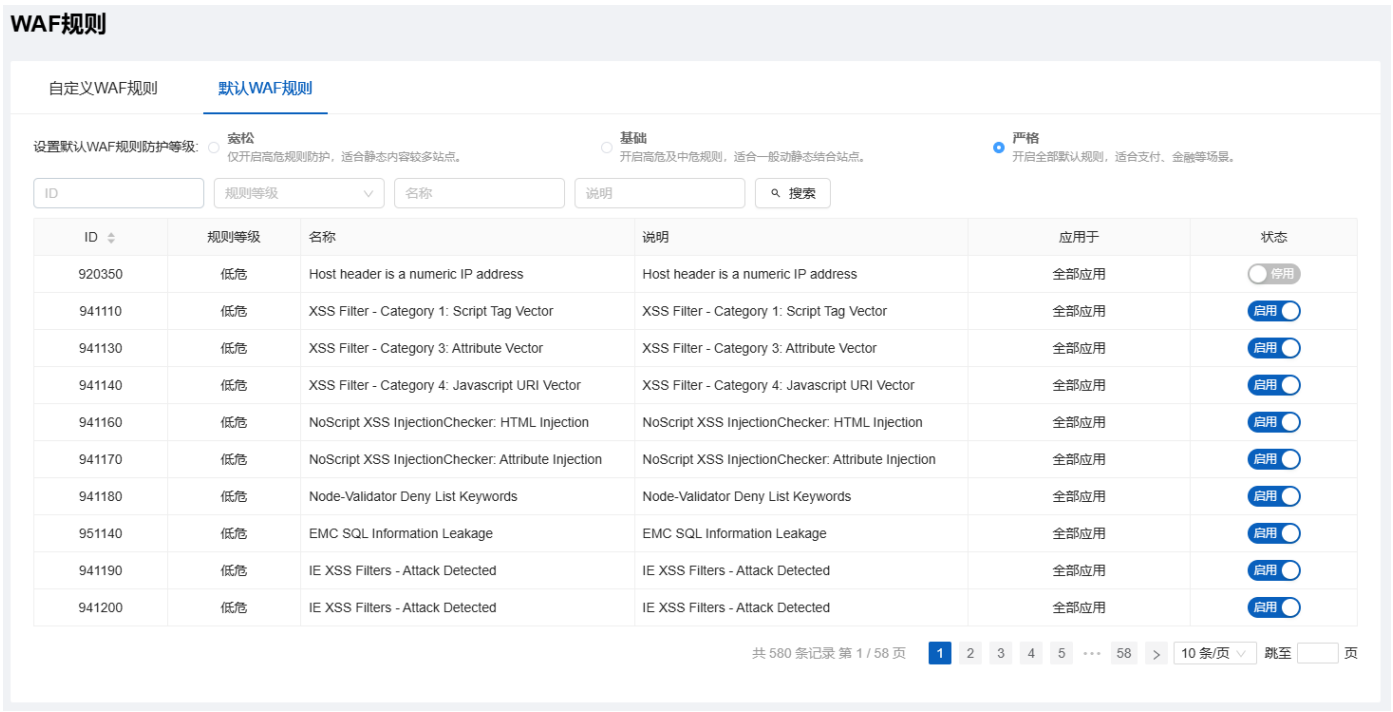
- 规则名称：用户设置的规则名称，可以设置中英文数字及符号
- 应用于：可以选择全部应用（即全部网站组，包括以后添加的网站组也应用该规则），也可以单独选择某一个或某几个网站组。
- 匹配字段：用户的请求中匹配的字段，具体点击后面的问号可以查看帮助。
- 逻辑符号：匹配字段时运用哪个逻辑符号来计算，具体点击后面的问号可以查看帮助。
- 匹配内容：在确定的匹配字段中根据逻辑符号匹配此处设置的内容。
- 动作：包含如下动作，

- 拦截：阻止本次访问请求
- 通过并记录：允许本次访问，将本次访问记录到WAF日志中
- 验证码：弹出验证码，用户需输入正确的验证码才允许访问
- 放行：直接放行，不做任何处理
- 5秒盾：页面出现5秒倒计时，5秒倒计时结束后才可以访问
- 点击验证：在弹出页面上点击之后才可以访问
- 滑动验证：页面出现滑块，将滑块滑动到正确位置后才可以访问
- 旋转图片验证：需要将图片旋转到正确的位置才可以访问
- 302验证：页面会自动进行302跳转，如果非浏览器访问且不跟随302跳转将不能访问
- 浏览器验证：验证请求是否是通过浏览器发起，非浏览器发起的请求将不可访问

◦ 是否启用：本条WAF规则是否启用。

4.4.1.2 默认WAF规则

除了自定义WAF规则，系统也提供一套默认的WAF规则，这套规则提供三个模式：宽松、基础、严格。如下图：



规则中包含了大量常见的攻击防护，您可以根据您自身的需要设置对应规则的开启和关闭。

注意：默认规则都是针对您的全部网站组的。

4.4.2 CC规则

单条CC规则由三部分组成：匹配器，过滤器，动作。多条CC规则组合成规则组。

4.4.2.1 匹配器:

匹配器由匹配项，操作符，匹配值组成。比如匹配项是IP，操作符是=，匹配值是192.168.0.1，表示客户端IP是192.168.0.1才算匹配。

说明: 一个匹配器可以有多个匹配项，添加多个匹配项时， **此匹配器所有的匹配项都满足时，这个匹配器才为真。**

在匹配器通过之后，就使用过滤器来对请求进行验证。

4.4.2.2 过滤器:

用来对客户请求进行验证，比如统计请求数是否超限，验证码是否输入正确，是否跳转到正确的URL等。

如果验证次数超过指定次数，那么就执行下面指定的动作来拦截或记录。

4.4.2.3 动作:

当请求无法通过过滤器时，执行该动作。

4.4.2.4 匹配器中的匹配项

用来匹配用户的请求，可以匹配的项目有：

- 请求URI(不带参数)：去除参数的url，如原始/123.php?a=1，经处理变成/123.php再去匹配
- IP地址：客户端IP地址
- 域名：客户请求的域名
- 请求URI：请求的url，如/123.php?a=1，保留参数匹配。
- 请求方法：如GET, POST等
- 浏览器UA：浏览器名称，如Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
- 请求来源：如 http://demo.abc.com/console/index.html

- 国家代码：由两位字母表示某个国家的IP地址，比如CN表示在中国网络下请求网站的客户，完整的国家代码列表 https://www.iban.com/country-codes
- 省份 (中文)：支持中文字符，如：河北省，上海市，新疆维吾尔自治区。注：需要写完整名称。
- 城市 (中文)：支持中文字符，如：广州市，苏州市。注：需要写完整名称。
- 运营商 (中文)：支持中文字符，如：中国电信
- 请求头accept_language：浏览器可以接受的语言种类。例如，en或en-us代表英语，zh或zh-cn代表中文。

4.4.2.5 匹配器中的操作符：

- 等于：即与匹配值完全匹配条件才成立
- 不等于：参考等于
- 包含：要匹配的值包含有匹配值条件就成立，如请求URI为/index.php，匹配值为php的话，条件成立
- 不包含：参考包含
- 前缀匹配：匹配所有以指定字符串开头的URI。即从前面开始匹配，如请求URI为/api/index，当匹配值为/api时，条件成立，值为index或api时，条件不成立。
- 后缀匹配：匹配所有以指定字符串结尾的URI。即从尾部开始匹配，如请求URI为/api/index，当匹配值为index或ex时，条件成立，匹配值为/api时，条件不成立。
- 正则匹配：如^/[0-9]+，即匹配以/开头，后面接数字的URI

4.4.2.6 过滤器中的项目类型

- **请求速率：** 固定时间周期内，最大请求数不超过某个值，或单个URL访问次数不超过某个值。
- **5秒盾：** 当触发条件时，CDN会将访问用户引导到一个倒计时为5秒的页面，等5秒倒计时结束之后，跳回用户需要访问的页面
- **302跳转：** 当客户请求CDN节点时，CDN会以302跳转的形式返回一个URL，客户跟随访问这个URL才算验证通过，否则算失败。用户无感。
- **浏览器识别：** 客户请求CDN节点时，CDN返回一段带跳转功能的js代码，客户跟随访问这个URL才算验证通过，否则算失败。用户无感。
- **滑动验证：** 当触发条件时，用户的访问会跳转到一个需要拖动滑块验证的页面，在用户验证成功后会返回用户需要访问的页面。
- **验证码：** 当触发条件时，用户的访问会跳转到一个需要输入或者点击验证码的页面，在用户验证成功后会返回用户需要访问的页面。
- **旋转图片：** 当触发条件时，用户的访问会跳转到一个需要将图片旋转到正确位置的页面，在用户验证成功后会返回用户需要访问的页面。

4.4.2.7 动作选项

- 封禁（英文：IPset）：使用iptables的ipset模块拦黑ip。选择该选项时可以设置IP的封禁时间，在封禁时间内，该IP将无法访问加速网站。
- 跳出（英文：Exit）：中断本次连接。
- 记日志（英文：Log）：记录该条访问的日志。

4.4.2.8 规则

- 规则由匹配器，过滤器，动作组成。
- 一条规则可以指定一个或两个过滤器。
- 当指定一个过滤器时，当这个过滤器验证失败时，直接执行动作;
- 当指定两个过滤器时，即指定过滤器1和过滤器2，那么当过滤器1验证失败，这时还不会执行动作，而是继续使用过滤器2验证， **只有当两个过滤器都验证失败时，才执行动作。**
- 这样可以有效减少误封，比如过滤器1使用请求频率，过滤器2使用滑动验证，这样可以防止误封请求量比较大的客户。

4.4.2.9 规则组

- 多条规则组合就形成规则组。网站绑定的为规则组。
- 同一个规则组中有多条规则时，依次匹配。

4.4.3 IP黑白名单

可以设置针对全部网站组或单个网站组的IP白名单或黑名单。

说明：IP白名单优先，如果一个IP在白名单中，所有WAF和CC规则以及区域封禁都将对该IP不生效。

点击添加 IP白名单 或 IP黑名单 即可弹出如下编辑IP名单的窗口：

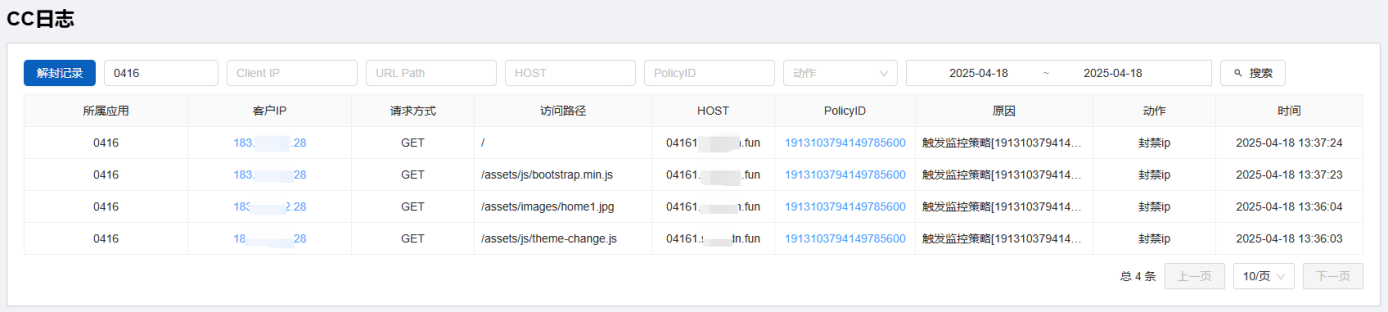
4.4.4 区域封禁

该功能类似网站组管理中的区域封禁。可以设置全部网站组的封禁区域，也可以单独设置某一个网站组的封禁区域。

4.4.5 WAF日志

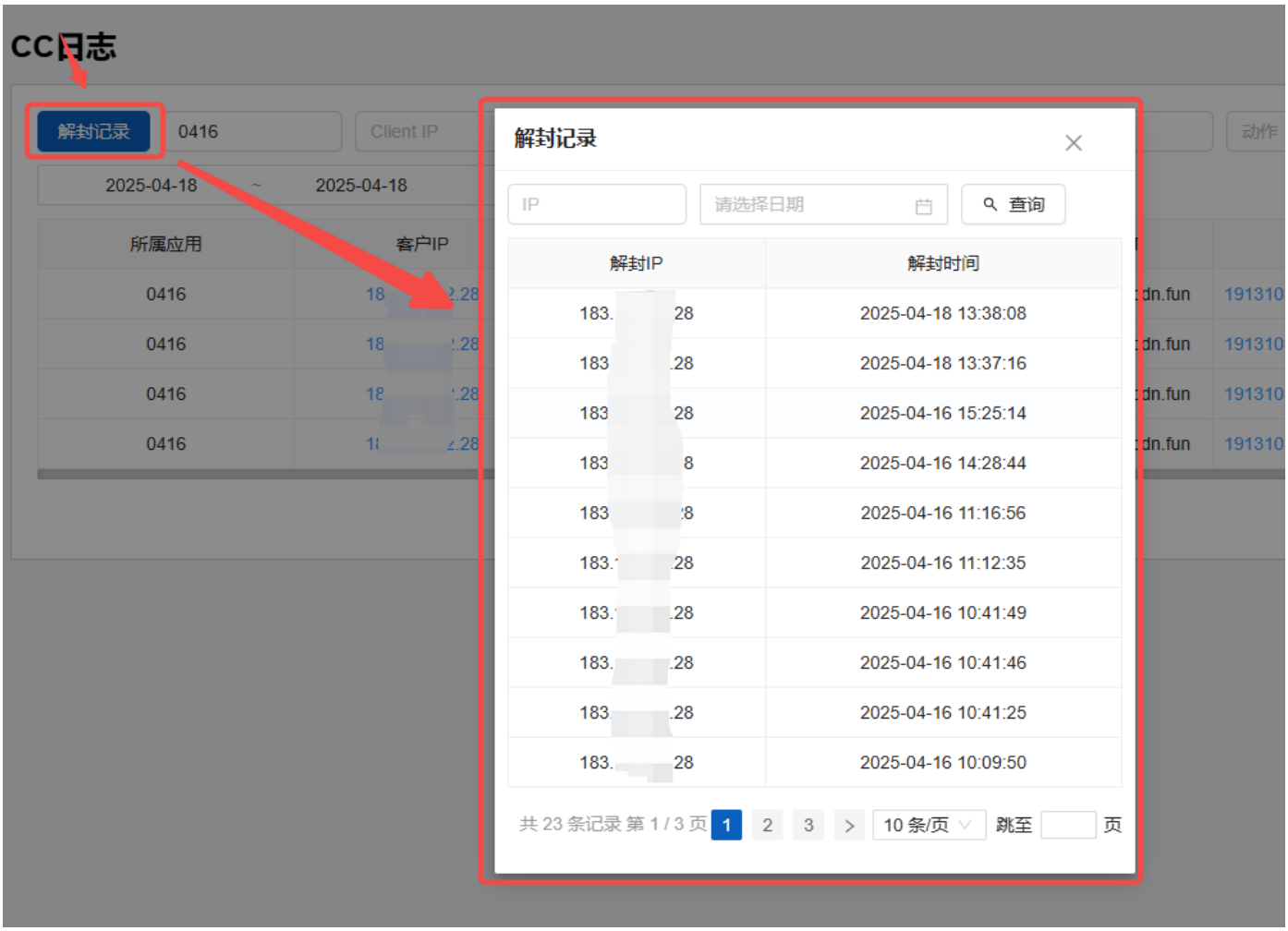
这里可以产看全部产生的WAF日志。你可以看到具体是哪一个IP访问了哪一个URL因为触发了哪条WAF规则而被记录下来。

4.4.6 CC日志



这里可以看到全部触发了CC规则产生的日志。点击policyID可以看到是触发了什么规则产生的封禁。如下图：

点击页面左上角的 解封记录 IP，可以看到IP的解封记录。如下图：



如果一个IP触发CC规则被封禁，需要解禁，可以在防护分析页面看到封禁IP列表。如下图：

点击数字，可以看到封禁IP列表，如下图：

可以对当前封禁的IP进行 解封、 拉黑（拉入黑名单）、加白（加入白名单）等操作。

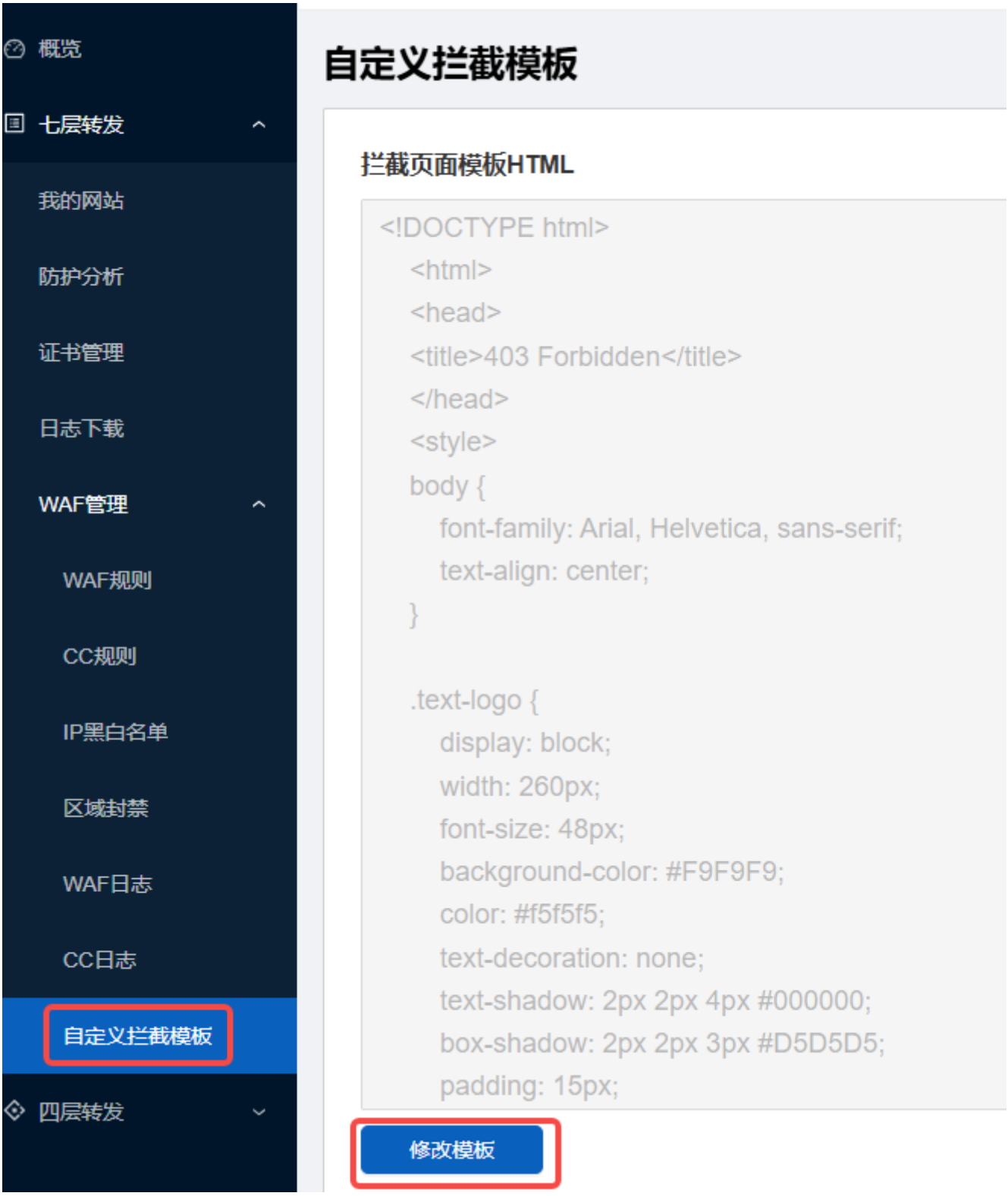
4.4.7 自定义拦截模板

当触发WAF规则时，系统会返回一个提示页面，效果如下：

MCDN

Reason: None, Policy ID: 1912792060935536640, by MCDN.io

您可以修改这个页面的显示效果，



点击修改模板，可以看到下图：

拦截页面模板HTML

```
    box-shadow: 2px 2px 3px #D5D5D5;
    padding: 15px;
    margin: auto;
}

.block_div {
    padding: 10px;
    width: 70%;
    margin: auto;
}

</style>
<body>
<div class="block_div">
<h1 class="text-logo">Gateway</h1>
<hr>
Reason: {{.VulnName}}, Policy ID: {{.PolicyID}}, by Application Gateway
</div>
</body>
</html>
```

取消　保存　参数说明: .PolicyID: 触发拦截的规则ID; .VulnName: 触发拦截的漏洞名称

其中：PolicyID: 触发拦截的规则ID; .VulnName: 触发拦截的漏洞名称。您编辑模板时可以将这些参数放入，方便调试及分析。

注意：仅请求被拦截时才适用拦截模板。

5. 四层转发

MCDN不仅支持7层的转发，还支持4层转发。

5.1 我的转发

如果您没有购买过包含四层转发的套餐，请已移步套餐管理中购买对应套餐。

如果您已经购买了包含四层转发功能的套餐，就可以点击添加转发进入添加转发的操作。

点击 添加转发 按钮，弹出如下窗口：

- 转发名称：新建的转发名称，支持中英文数字及符号。
- 选择套餐：选择您购买的包含四层转发功能的套餐。
- 源站：添加源站地址，第一个框为IP地址，第二个框为端口号，第三个框为权重。支持添加多个。
- 监听端口：第一个框为四层转发的监听端口，第二个框为选择协议，支持TCP和UDP。监听端口支持添加多个。

5.2 四层转发管理

点击编辑可以进入四层管理界面。如下图：

- 基础信息
  - 转发名称：该转发的名称
  - CNAME：系统签发的CNAME，分为共享和独享，根据套餐不同而不同
  - 当前套餐：用户添加转发时所选的套餐，支持更换套餐
- 监听端口
  - 监听端口：第一个框为监听端口，第二个为选择协议类型，支持TCP和UDP，支持添加多个。
- 源站配置
  - 点击添加可以添加新源站
  - 也可以通过操作中的编辑和删除来对源站进行操作
- ACL
  - 默认行为：放行，默认所有用户都放行；阻止，默认所有用户都组织。
  - 规则：可以设置某个IP是放行还是阻止。

- 区域封禁
  - 设置该转发在某个区域内不可访问，中国大陆支持设置某省不能访问，非中国大陆支持设置某个国家或大洲不能访问。

5.3 四层转发日志

四层转发日志中包含访问日志和防护日志两个模块。

5.3.1 访问日志

访问日志中可以看到客户端IP，转发开始时间、结束时间。

注意：结束时间并不是该连接真实结束的时间，而是建立连接就会每隔一分钟记录一条日志。

5.3.2 防护日志

如果用户转发中设置了阻止IP或者区域封禁等规则，一旦这些规则被触发，系统就会记录一条防护日志。如上图。

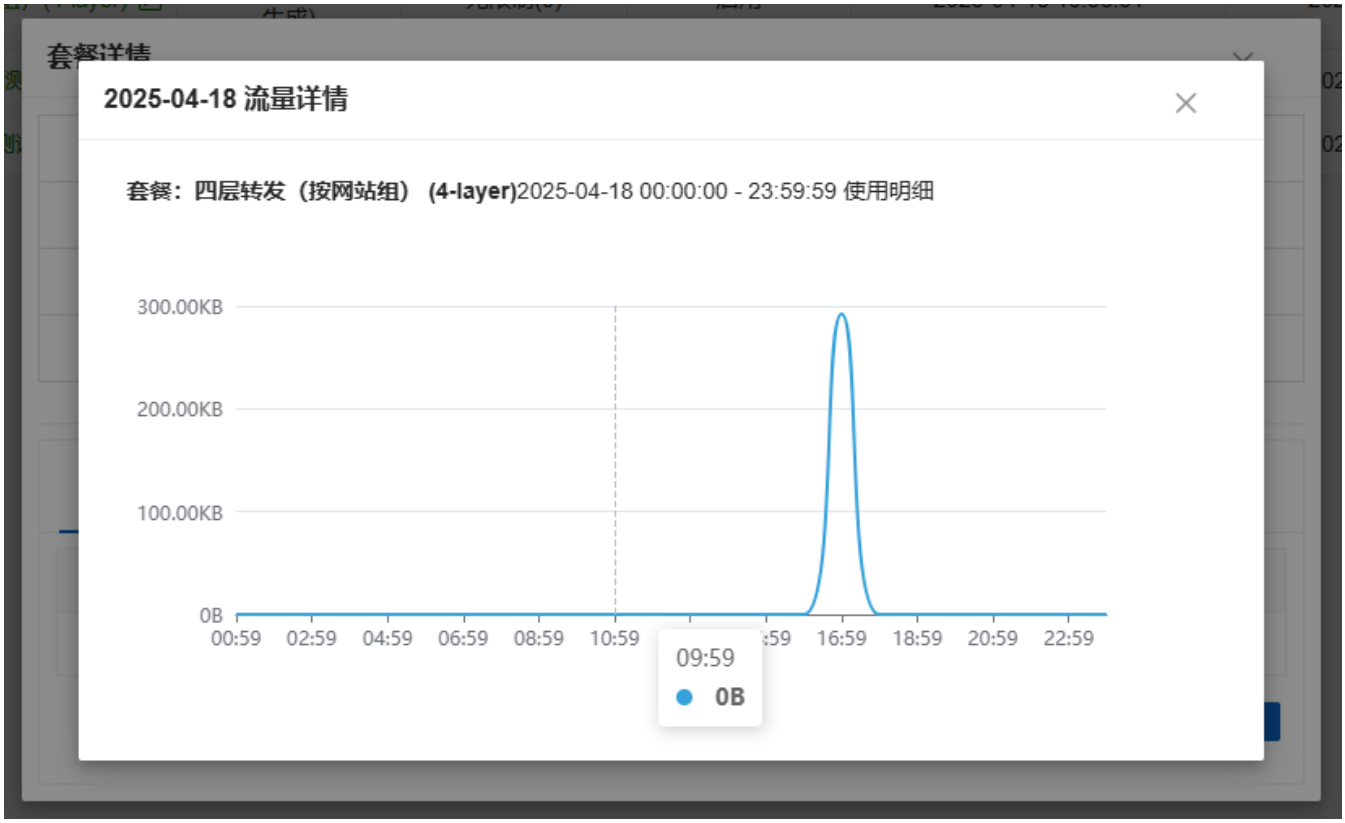
6. 套餐管理

6.1 我的套餐

该页面可以展示用户购买的全部套餐，支持修改套餐名称。点击 详情 按钮，可以查看该套餐的每日流量消耗情况。如下图：

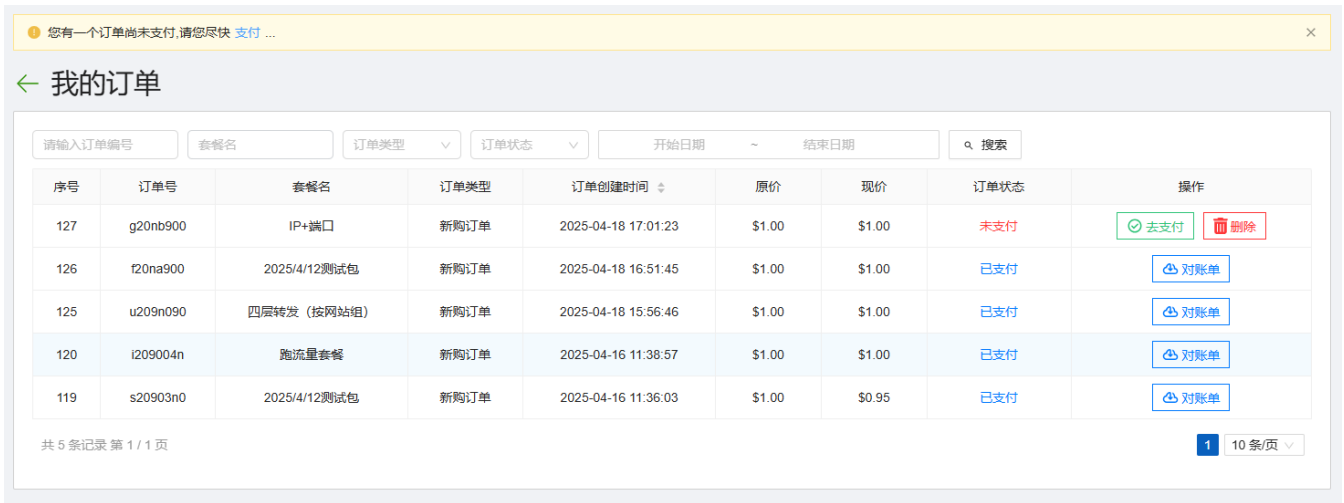
点击 套餐操作记录 可以看到该套餐的购买及续费情况。如下图：

点击当日适用下面的流量数字，可以查看当天流量消耗的图表。如下图：



系统还支持按照最近30天、按月、按期统计流量消耗情况。

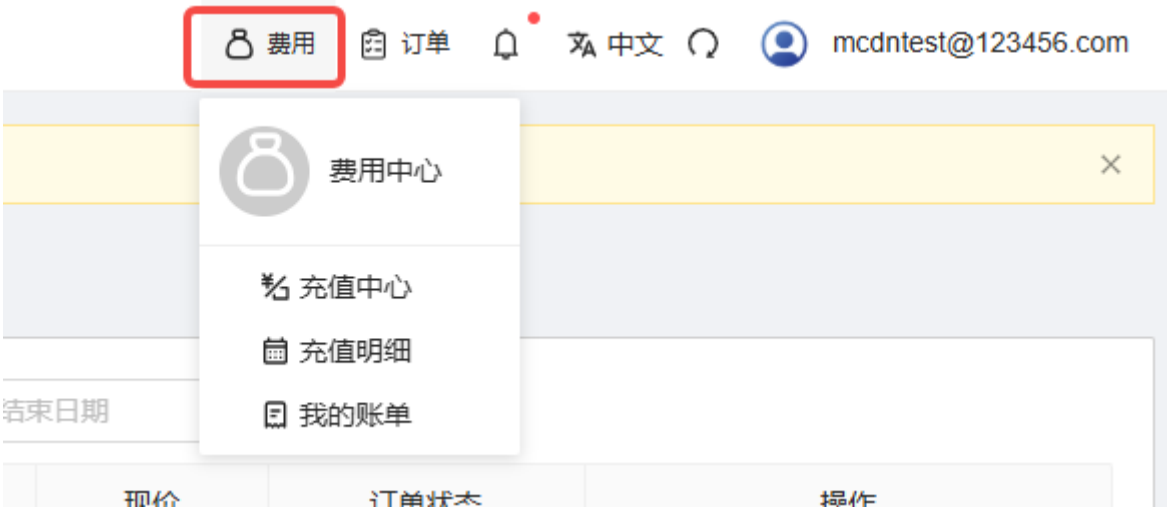
6.2 我的订单



我的订单页面可以查看用户过往的全部订单，也可以申请对账单。如果有订单还未支付，可以点击顶部的支付提醒，也可以进入订单页面点击 去支付 按钮查看。

点击 对账单 按钮，系统会弹出一个公司信息收集窗口，填完公司信息后系统就会生成一个PDF格式的对账单。

7. 费用管理



点击右上角的 费用 图标，可以进行充值、查看充值明细、下载账单操作。

7.1 充值中心

系统支持多种充值方式，您可以选择对应的方式按照系统提示完成充值操作。

7.2 充值明细

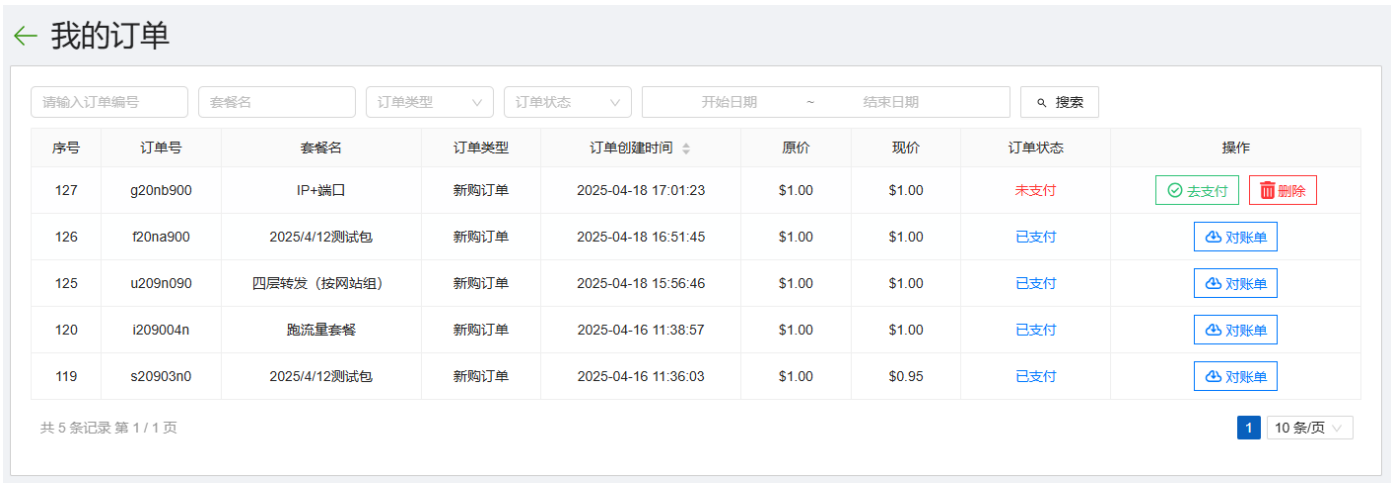
点击充值明细按钮，弹出上图界面，可以查看过往的每一笔充值记录。

7.3 我的账单

这里可以下载过往每一笔支付的对账单。

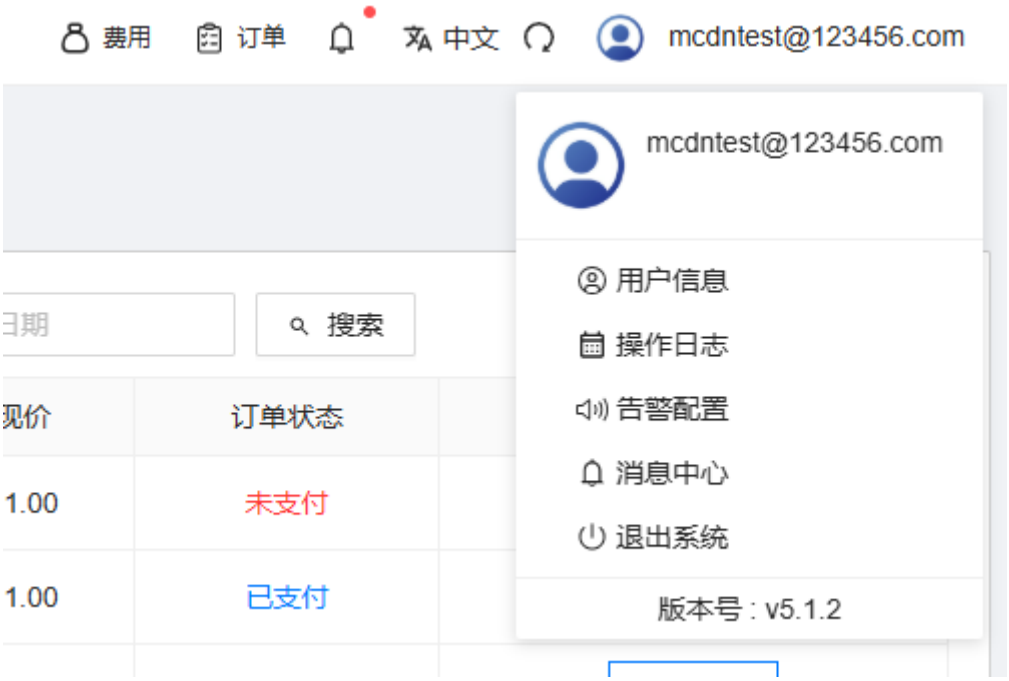
8. 订单管理

点击右上角订单图标，可以进入订单管理页面。



9. 用户信息

9.1 用户信息



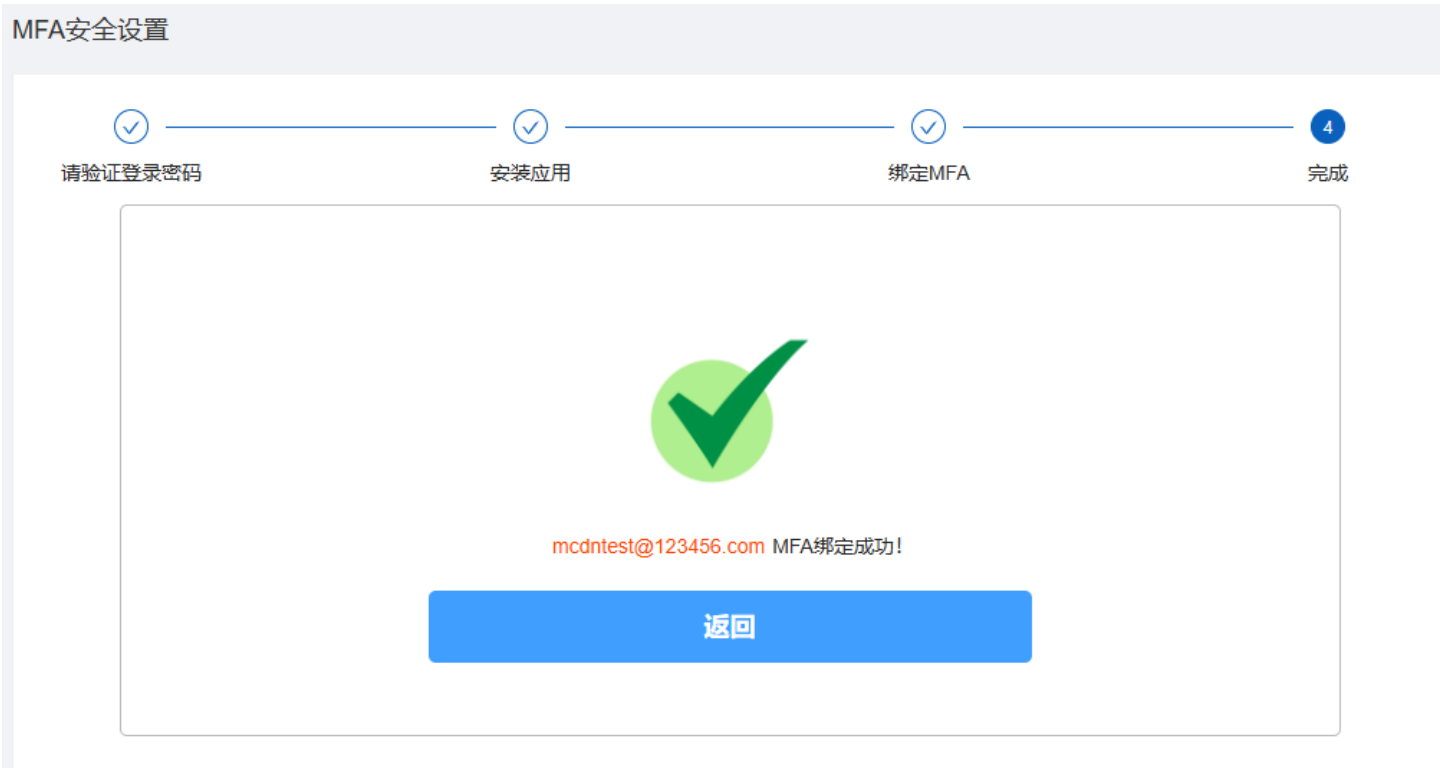
点击 用户信息 可以进入用户信息页面，如下图：

您可以重设密码、充值、查看账单、查看充值明细。还可以绑定两部验证（MFA），如下图：

MFA安全设置

MFA安全设置

系统会生成一个二维码，用Google的身份验证器扫码，输入对应的6位数字校验码，即可完成绑定。



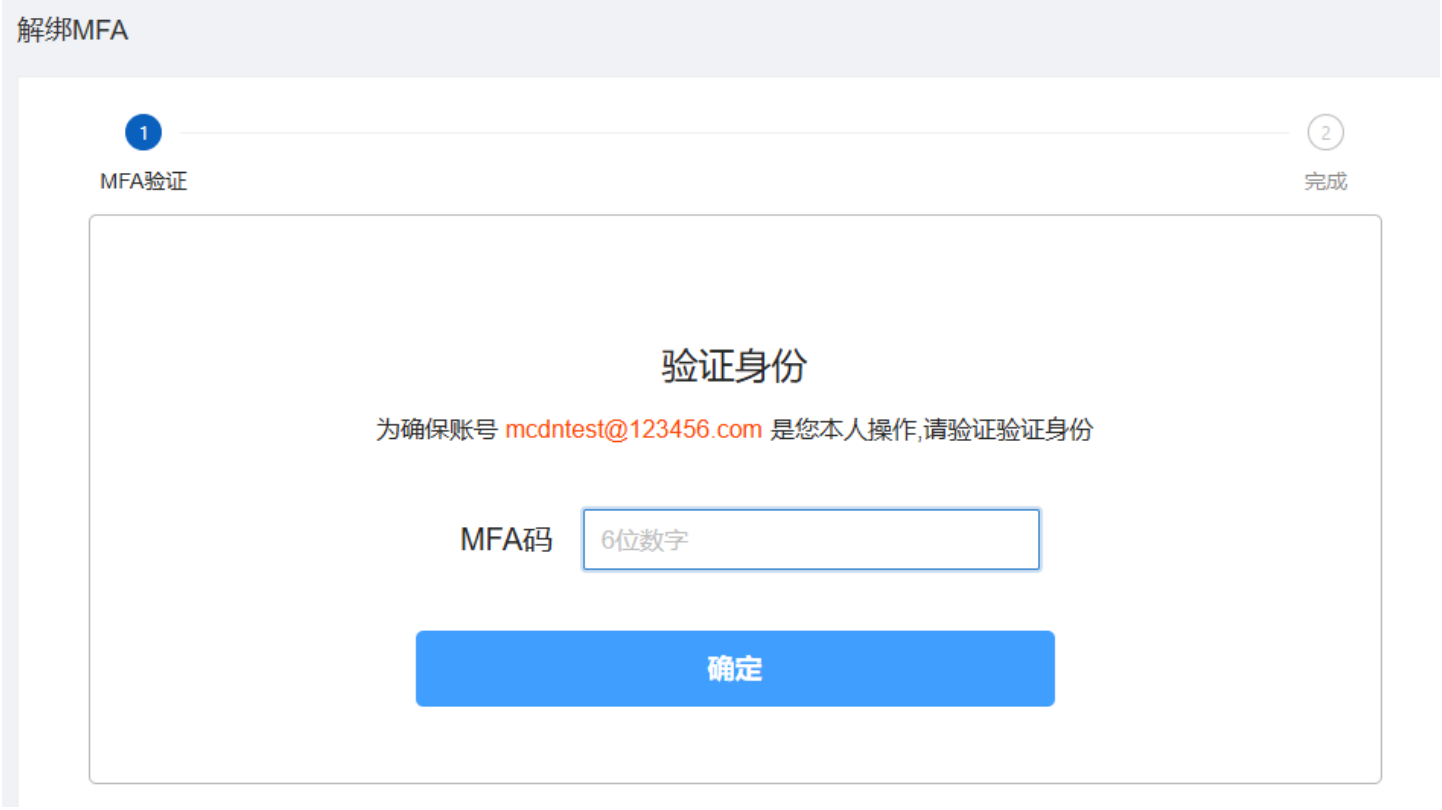
绑定之后登录时需要校验，如下图：

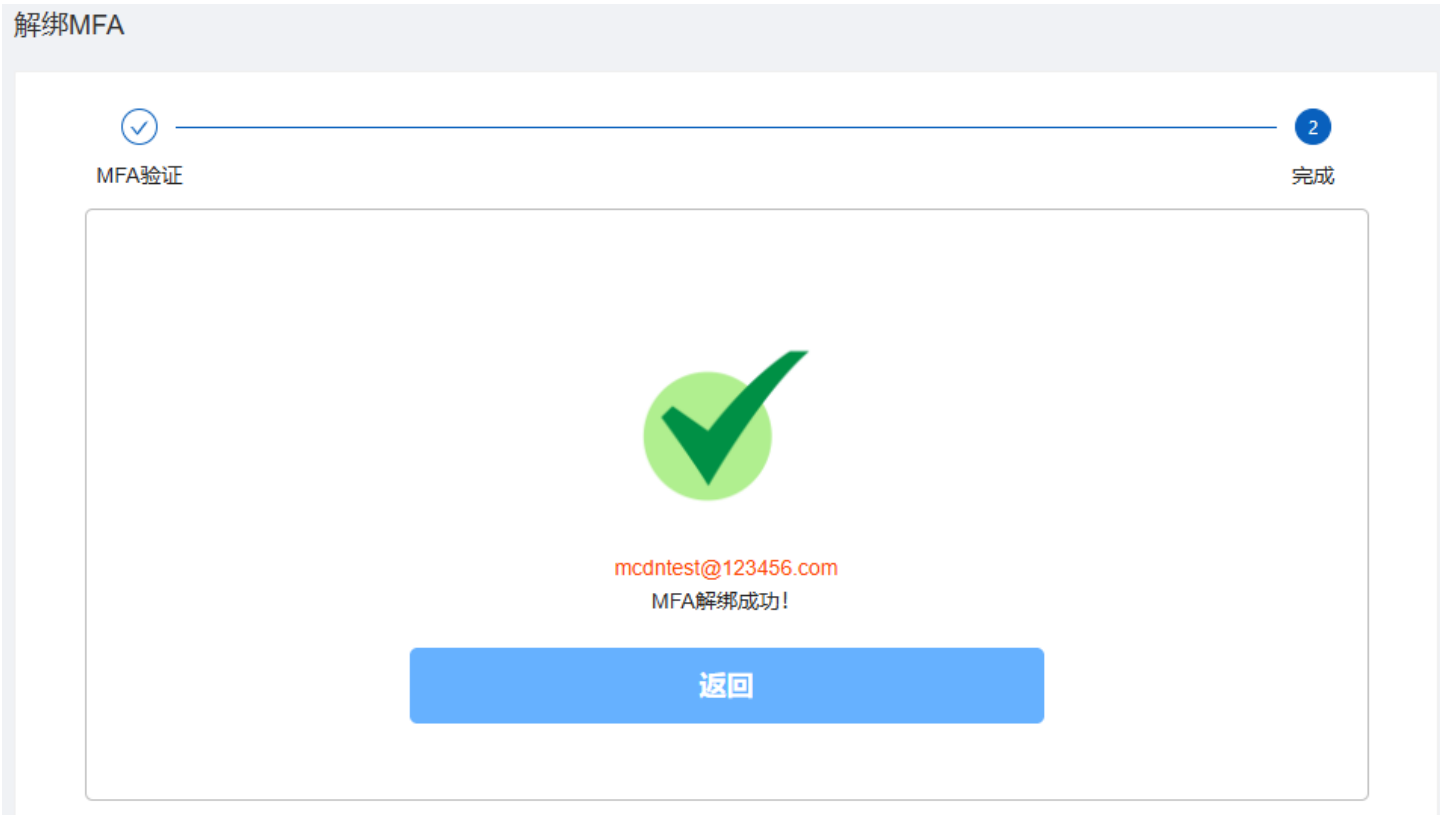
点击登录，进入MFA校验环节：

输入校验码后点击校验，方可登录系统。

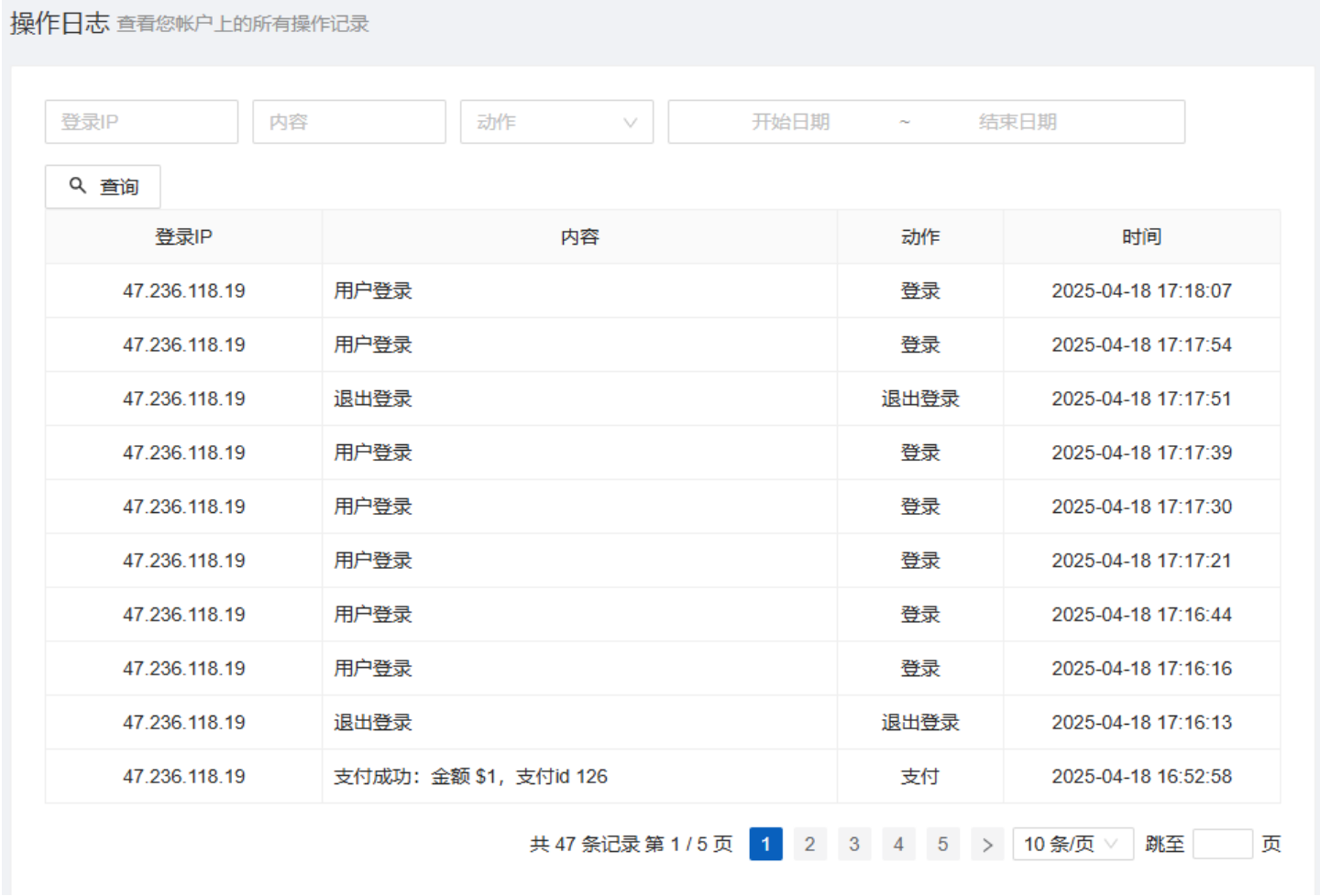
如果您不需要再绑定MFA，也可以点击 解绑 按钮进行解绑。如下图：

输入MFA校验码，即可完成解绑。如下图：


解绑MFA
1
MFA验证
2
完成
验证身份
为确保账号 mcdntest@123456.com 是您本人操作,请验证验证身份
MFA码
6位数字
确定


解绑MFA
MFA验证
2
完成
mcdntest@123456.com
MFA解绑成功!
返回

9.2 操作日志

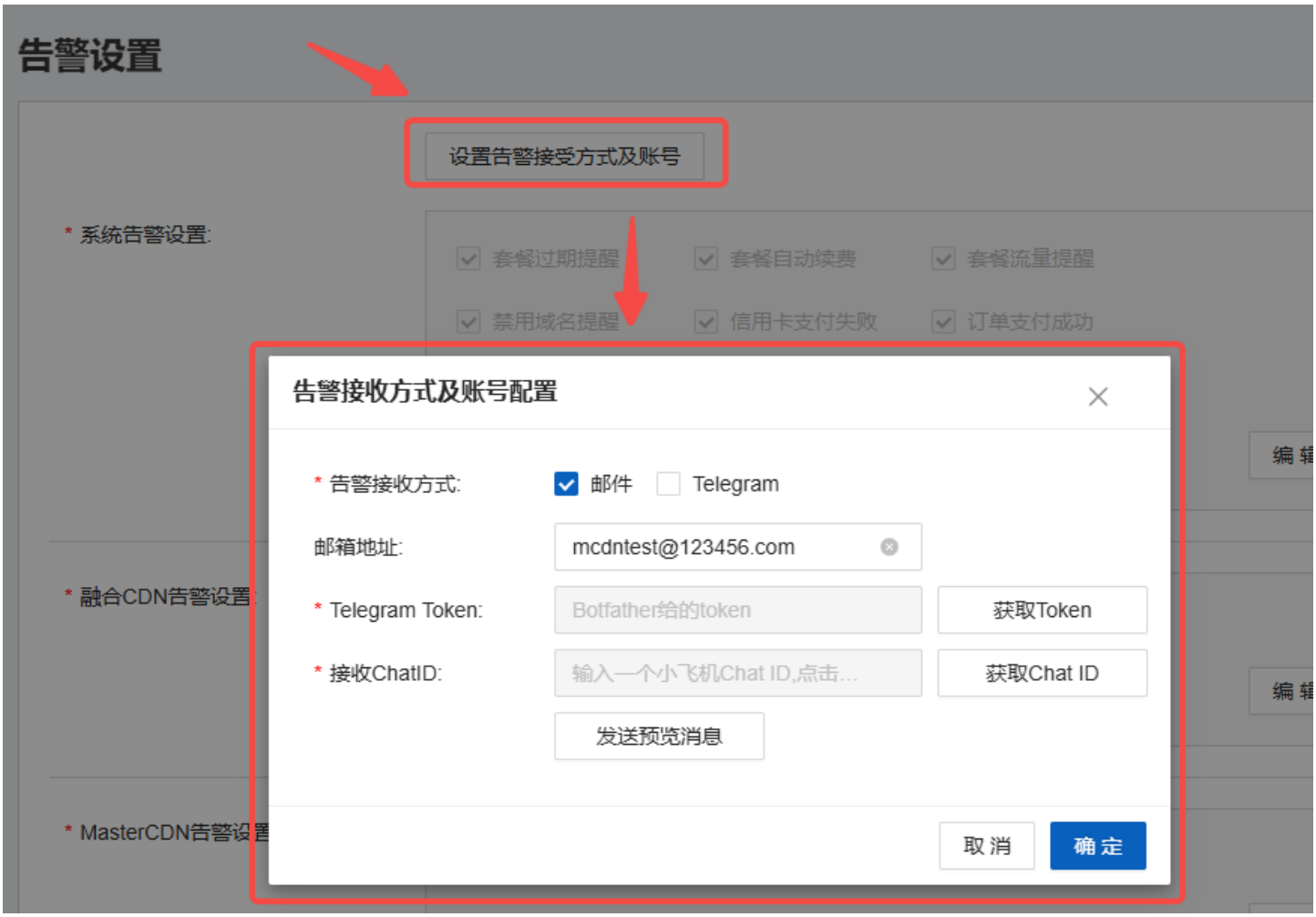


可以查看用户的登录及操作情况。

9.3 告警配置

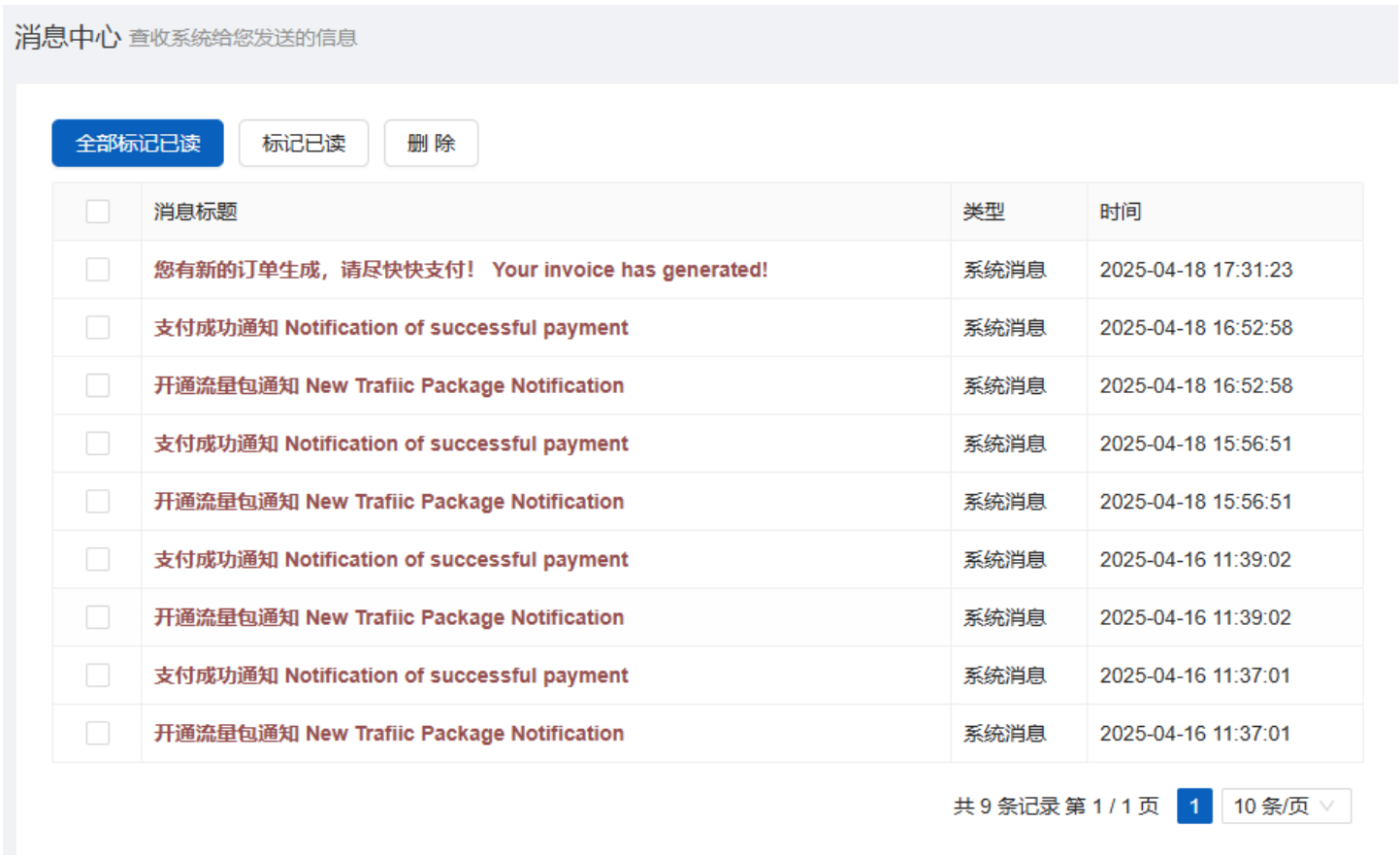
当套餐过期、域名被禁用、CDN开通成功时，系统会发送邮件或telegram消息，您可以通过这个页面配置哪些消息需要告知。

设置告警接收方式及账号：



点击可以根据提示添加对应的告警消息的接收账号。

9.4 消息中心



系统通知、公告及预警消息都会在这个页面显示。

9.5 退出系统

系统弹出确认框，确认之后退出系统。