观镜 WEB 应用安全防护系统

用户使用手册

2020 年 2 月

Bubble Web Application Security System

上海观安信息技术股份有限公司 电话：021- 62090100
技术支持邮件：websec@idss-cn.com 产品服务电话：400-728-0510
地址：上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

目录

第1章系统概述

1.1. 背景

观镜 Web 应用安全防护系统系统的设计理念源于团队成员十余年安全服务经验，并且结合当前大数据技术、流量分析技术等领先技术，将 Web 安全防御系统置于客户系统之前，在不影响客户机原有业务的情况下，将客户系统的 web 数据进行混淆和加密，将攻击阻挡在网站之前。同时，该系统可以拦截网络上常见自动化工具的恶意请求，有效的保护企业网站安全。它具有功能强大、部署简单、多引擎、易扩展等特点。

1.2. 目的

观镜 Web 应用安全防护系统支持通过 WEB 管理界面进行配置站点以及管理。本手册主要介绍如何使用观镜 Web 应用安全防护系统进行对站点的防护和管理、策略配置以及常见场景防御配置等操作。

第2章前置知识

2.1. 操作系统

2.1.1. LINUX 操作系统

需要具备基本的 Linux 系统操作能力，针对常见的操作命令等等需要熟练掌握：

2.1.2. Windows 操作系统

需要掌握日常的办公操作、软件安装卸载，掌握在 Windows 上搭建与部署网站，熟练使用 Vmare Workstation 和 VirtualBox 等虚拟化平台操作，熟练使用 MySQL 等数据库管理系统。

2.2. HTTP 协议基础

HTTP 协议是 Hyper Text Transfer Protocol（超文本传输协议）的缩写，是用于从万维网服务器传输超文本到本地浏览器的传送协议。HTTP 协议工作于客户端-服务端架构上，浏览器作为 HTTP 客户端通过 URL 向 HTTP 服务端即 WEB 服务器发送所有请求，WEB 服务器根据接收到的请求后，向客户端发送响应信息，其默认端口号为 80。

2.2.1. HTTP 请求方法

序号	方法	中文描述
1	GET	请求指定的页面信息，并返回实体主体。
2	HEAD	类似于 GET 请求，但返回的响应中没有具体的内容，用于获取报头。
3	POST	向指定资源提交数据进行处理请求（例如提交表单或者上传文件）。数据被包含在请求体中。POST 请求可能会导致新的资源的建立和/或已有资源的修改。
4	PUT	从客户端向服务器传送的数据取代指定的文档的内容。
5	DELETE	请求服务器删除指定的页面。
6	CONNECT	HTTP/1.1 协议中预留给能够将连接改为管道方式的代理服务器。
7	OPTIONS	允许客户端查看服务器的性能。
8	TRACE	回显服务器收到的请求，主要用于测试或诊断。
9	PATCH	是对 PUT 方法的补充，用来对已知资源进行局部更新 。

2.2.2. HTTP 状态码

当浏览者访问一个网页时，浏览者的浏览器会向网页所在服务器发出请求。当浏览器接收并显示网页前，此网页所在的服务器会返回一个包含 HTTP 状态码的信息头用以响应浏览器请求。下面是常见的 HTTP 状态码：

状态码	英文名称	中文描述
100	Continue	继续。客户端应继续其请求。

200	OK	请求成功。一般用于 GET 与 POST 请求。
201	Created	已创建。成功请求并创建了新的资源。
301	Moved Permanently	永久移动。请求的资源已被永久的移动到新 URL ,返回信息会包括新的 URL，浏览器会自动定向到新 URL。今后任何新的请求都应使用新的 URL 代替。
302	Found	临时移动。与 301 类似。但资源只是临时被移动。客户端应继续使用原有 URL。
400	Bad Request	客户端请求的语法错误，服务器无法理解。
403	Forbidden	服务器理解请求客户端的请求，但是拒绝执行此请求。
404	Not Found	服务器无法根据客户端的请求找到资源（网页）。通过此代码，网站设计人员可设置"您所请求的资源无法找到"的个性页面。
405	Method Not Allowed	客户端请求中的方法被禁止。
500	Internal Server Error	服务器内部错误，无法完成请求。
501	Not Implemented	服务器不支持请求的功能，无法完成请求。
502	Bad Gateway	作为网关或者代理工作的服务器尝试执行请求时 ,从远程服务器接收到了一个无效的响应。
505	HTTP Version not supported	服务器不支持请求的 HTTP 协议的版本，无法完成处理。

2.3. MYSQL 基础知识

需要会使用基础的 MYSQL 语句进行相应的数据库操作，包括创建数据库、创建表、创建用户、给用户赋予权限、修改数据库密码、导入文件等等不同基本情况。

2.4. WEB 安全基础知识

2.4.1. SQL 注入攻击测试

SQL 注入就是通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。具体来说，它是利用现有应用程序，将（恶意）SQL 命令注入到后台数据库引擎执行的能力，它可以通过在 Web 表单中输入（恶意）SQL 语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行 SQL 语句。总结产生 SQL 注入的位置，一是站点使用输入内容构造动态的 SQL 语句访问数据库，二是站点代码使用存储过程，存储过程作为包含未筛选的用户输入的字符串来传递，这两种情况都会发生 SQL 注入。但总的来说，只要存在数据库交互的点就有可能存在 SQL 注入漏洞。

需要掌握常见的 SQL 注入攻击的测试语句，这里作简单基本介绍：

序号	SQL 注入攻击测试语句说明	
	语句内容	验证判断
1	?id=1 and 1=1	判断是否为数字型注入
2	and 1=(select @@version)	查询数据库版本
3	and exists (select * from user_tables)	查询是否存在 user_tables 表
4	' and '1'='2	判断是否为字符型注入
5	and '%'='%/%'	判断是否为字符型注入
6	and user>0	获取当前数据库用户名
7	order by 10	判断当前查询语句的字段数

2.4.2. XSS 跨站攻击测试

XSS 跨站脚本攻击是一种常见的 Web 安全漏洞，它主要是指攻击者可以在页面中插入恶意脚本代码，当受害者访问这些页面时，浏览器会解析并执行这些恶意代码，从而达到窃取用户身份/钓鱼/传播恶意代码等行为。

需要掌握常见的测试 XSS 跨站攻击的测试语句，这里作简单基本介绍：

序号	XSS 跨站攻击测试语句说明

	语句内容	验证判断
1	<script>alert(1)</script>	触发弹框
2	<iframe/src \/\/onload = prompt(1)	触发弹框
3	<svg/onload=alert(1)	触发弹框
4	`-alert(1)">'onload="`<svg/1='	触发弹框
5	'><script>alert(123);</script x='	触发弹框
6	\";alert('XSS');//	触发弹框
7	c="javascript:";	触发弹框

2.4.3. 自动化扫描工具

需要掌握相关常见不同类型的自动化扫描工具，以方便对防护站点进行功能测试：

序号	工具名称	实现功能
1	AWVS	Web 安全扫描
2	Nmap	端口扫描
3	APPSCAN	Web 安全扫描
4	ZAP	Web 安全扫描
5	Burp Suite	Web 安全扫描

第3章系统操作

3.1. 登录系统

观镜 Web 应用安全防护系统 2.1 采用 B/S 架构，可直接在浏览器输入部署服务前地址，打开登录界面，首次登录需

要先进行注册，然后才可以正常登录，首次注册的用户权限默认为管理员“admin”，登录成功之后可在管理界面对用户进行增加或删除等管理。登录界面不提供“密码找回”功能，如您不慎遗忘密码，可由管理员登录进入用户管理界面进行重置密码，如只有当前一个用户，请联系厂商进行密码找回或重置。

根据配置好的 IP 地址访问管理端后会有以下提示：

图 3-1

点击高级显示出详情：

图 3-2

点击“继续前往 X.Y.Z.W（不安全）”即可正常访问，随后进入以下界面：

图 3-3

输入密码完成注册，然后即可正常登陆。

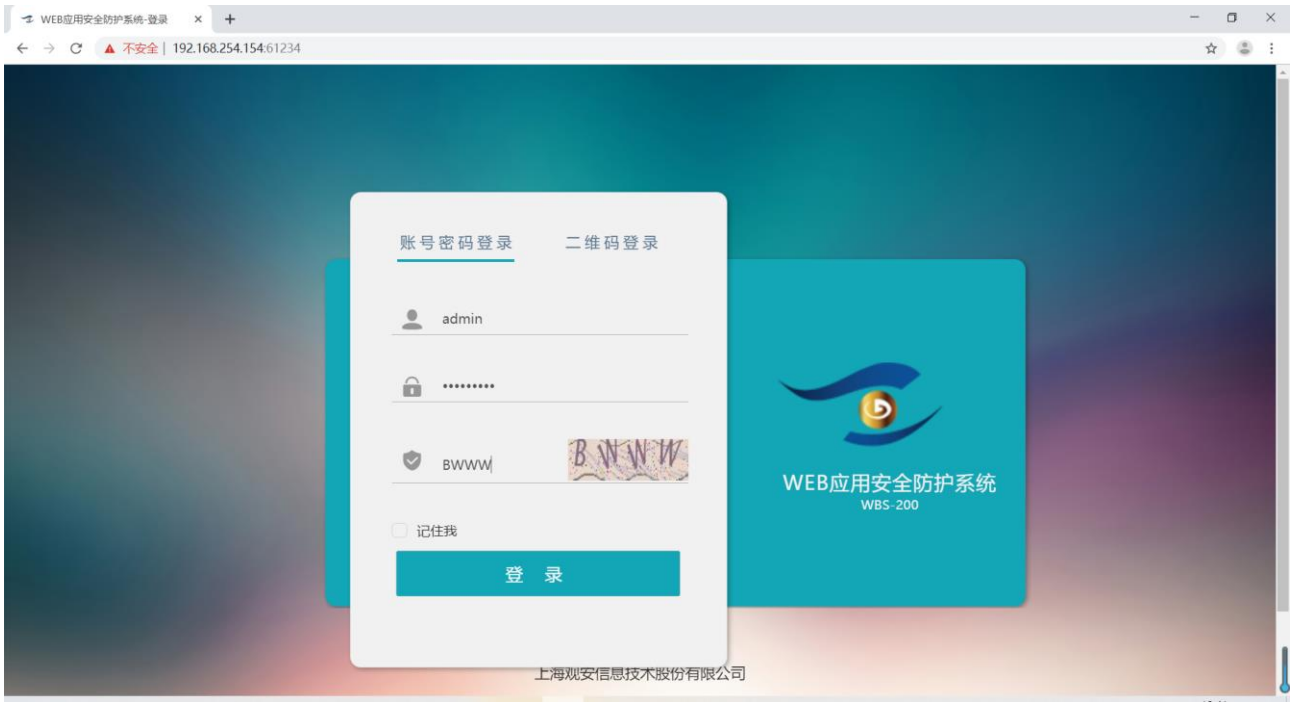


图 3-4

3.2. 忘记密码

如果用户忘记密码，请及时联系厂家进行密码找回。

第4章系统功能

4.1. 首页

4.1.1. 攻击画像

观镜 Web 应用安全防护系统系统可根据对网站防护的数据生成攻击画像，通过攻击画像可直观查看网站的访问状况，被攻击业务 TOP10、访问 IP TOP10、攻击类型 TOP 10 以及被攻击 URL 等信息。

模块说明：

模块名称	模块说明	备注

处理请求	统计对防护站点的所有请求数量 ,不包括透传模式下请求数据	
保护请求	统计对防护站点在拦截模式下的所有请求	
异常请求	统计对防护站点在拦截模式下检测到的异常请求总数	
正常请求	统计对防护站点在拦截模式下的所有正常请求	

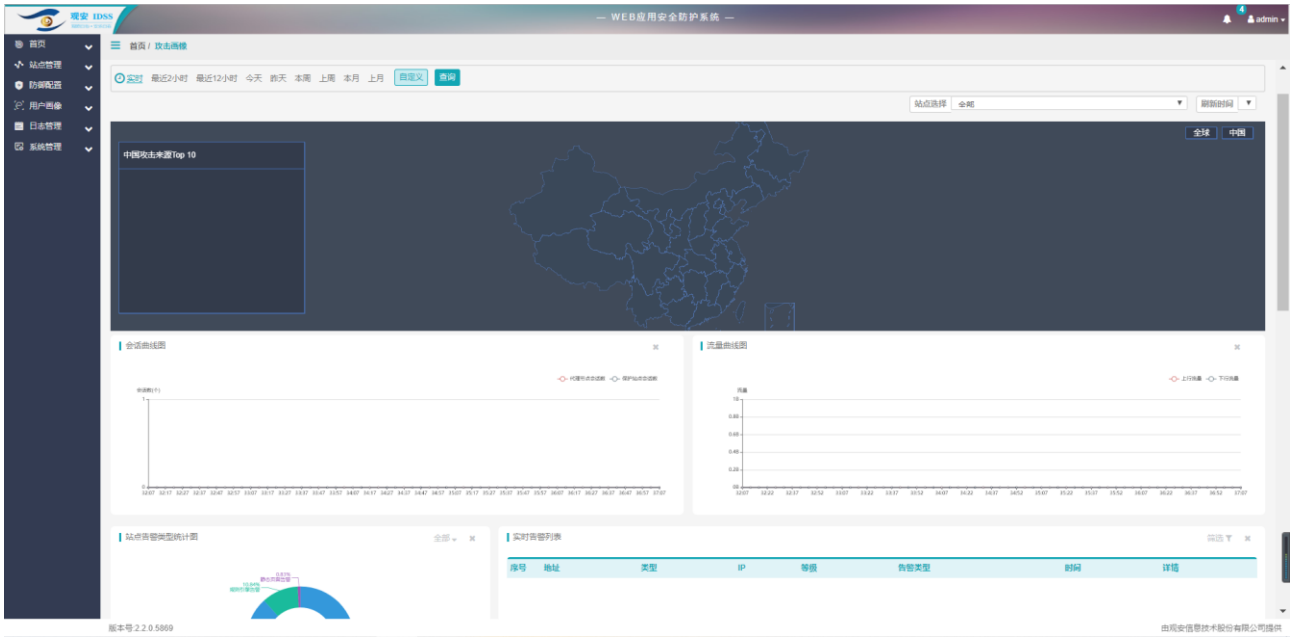


图 4-1

4.1.2. 被攻击业务统计列表

图 4-2

4.1.3. 被攻击地址统计列表

图 4-3

4.1.4. 自动化工具统计列表

图 4-4

4.1.5. 来源 IP 访问统计列表

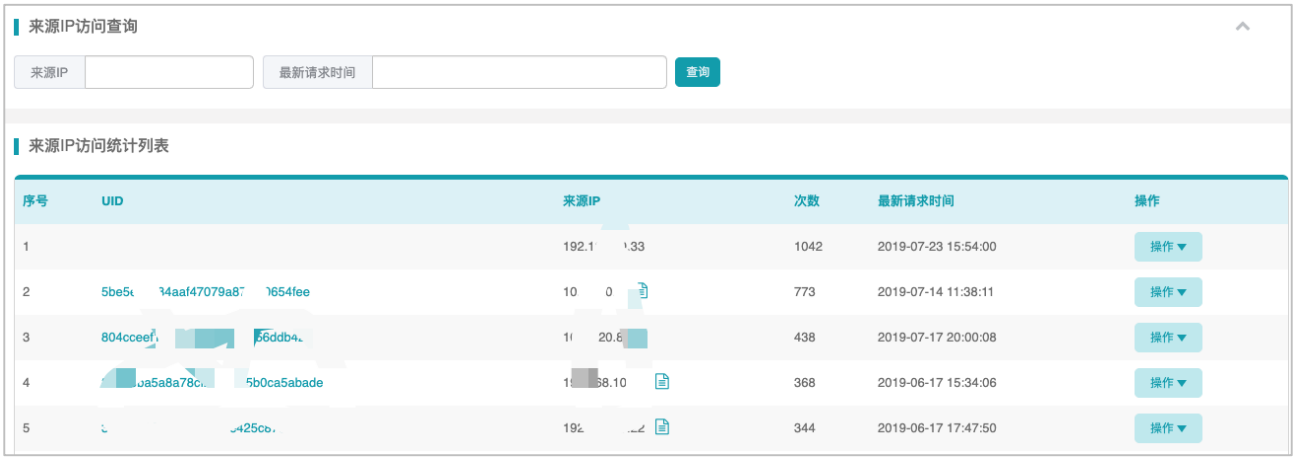


图 4-5

4.1.6. 来源浏览器统计列表

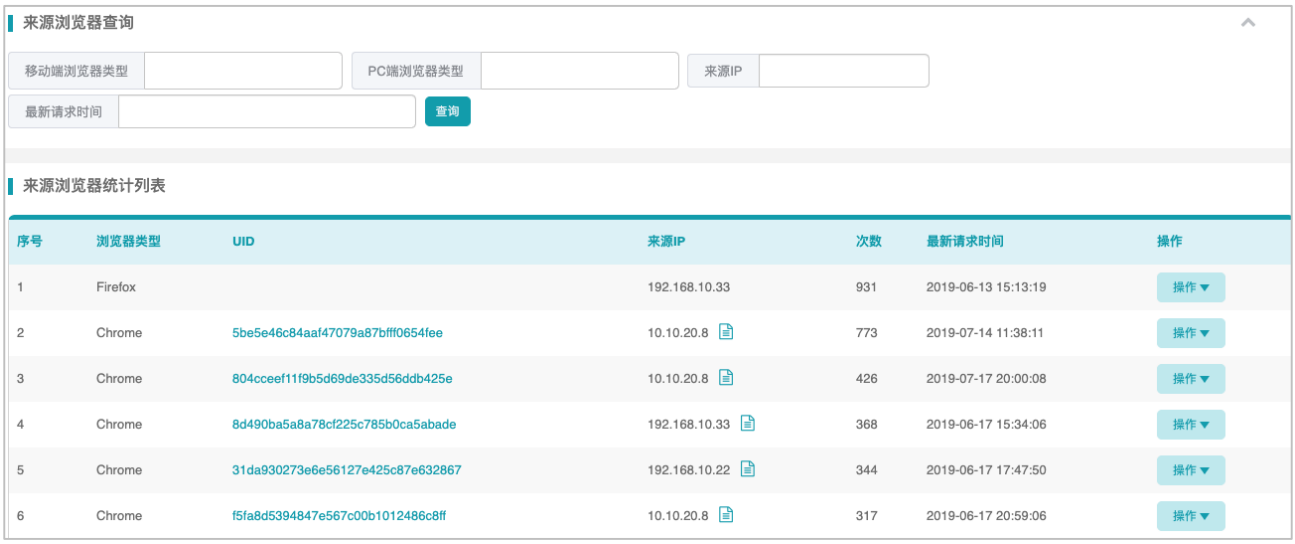


图 4-6

4.2. 站点管理

系统配置可通过管理界面先配置站点以及策略，然后关联节点即可完成保护，站点保护支持普通模式保护，即一个节点

防护一个服务器，一个节点防护多个不同类型的服务器，还支持负载均衡模式，即一个节点防护一个站点的多个服务器。

4.2.1. 站点配置

新增站点即增加需要保护的网站，站点名称可自定义名称，访问地址即保护后用户访问的地址，保护站点地址输入真实服务器的 IP 地址或域名信息，当前支持 HTTP、HTTPS 和 WebSocket 协议，当选择 HTTPS 协议时需要上传证书以保障正常访问。

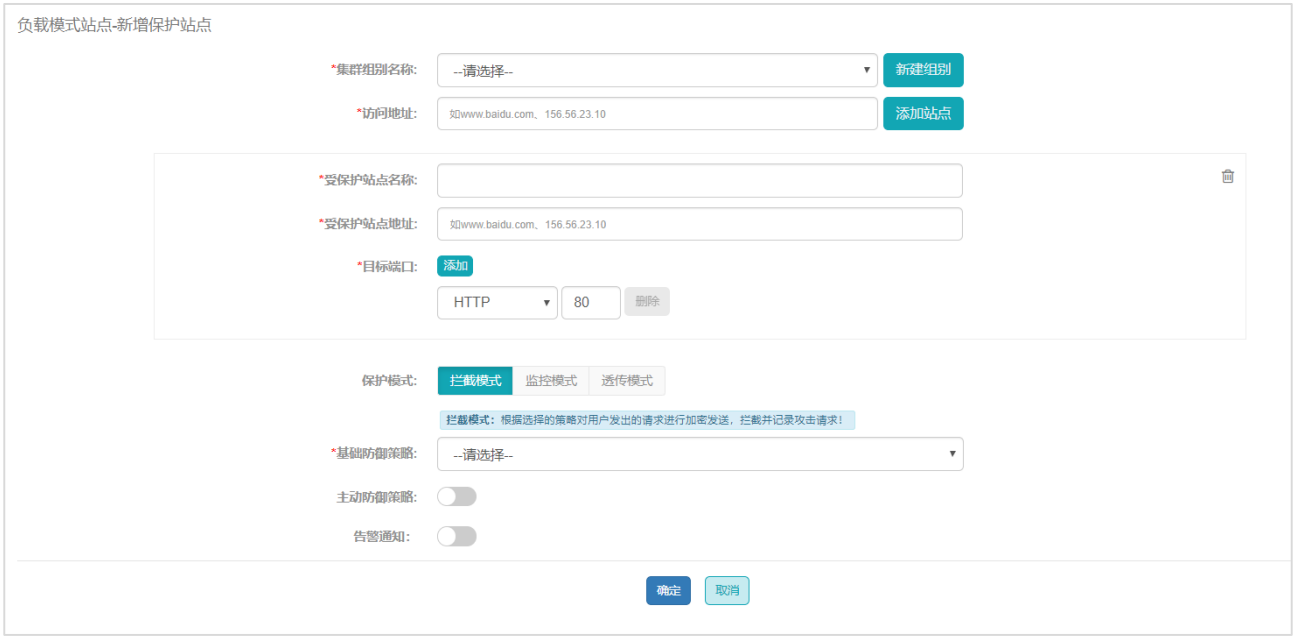
添加站点时可选三种保护模式（拦截模式、监控模式和透传模式），系统默认为拦截模式，具体拦截内容根据所选策略进行，监控模式只对请求进行记录不做拦截操作，透传模式将所有请求放行不进行任何操作，在新增站点后可根据实际业务需求选择保护模式，以免影响网站的业务正常运行。

站点配置支持普通模式和负载均衡模式，负载均衡模式可以通过配置一个节点服务器来保护一个站点多个不同的服务器。

普通模式添加如下：

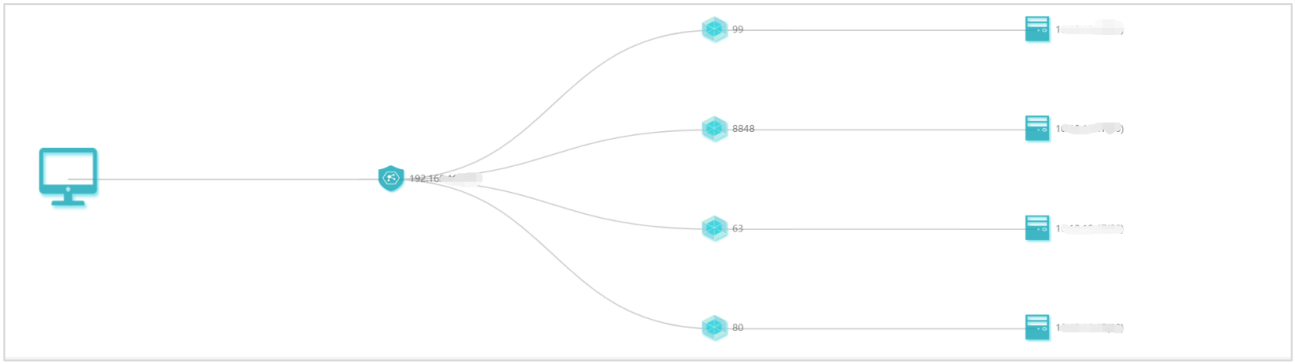
新增普通站点-图 4-7

负载均衡模式添加如下：



新增负载均衡站点-图 4-18

站点管理提供拓扑结构图，可直观查看当前节点防护站点情况：



拓扑结构图-图 4-19

4.2.1.1. HTTP 类型站点配置

步骤 1 当观镜完全部署后，以测试站点“www.testfire.net”为例。选择“站点管理>站点管理>新增站点>普通模式”，按提示对应输入“站点名称”、"访问地址”、"受保护站点地址”、"目标端口”、"保护模式”、"基础防御策略”、"主动防御策略”、"告警通知”等相关信息，点击【保存】，如图 4-20 所示，添加完成之后，列表更新，当前保护状态显示为“未配置”，如图 4-21 所示。

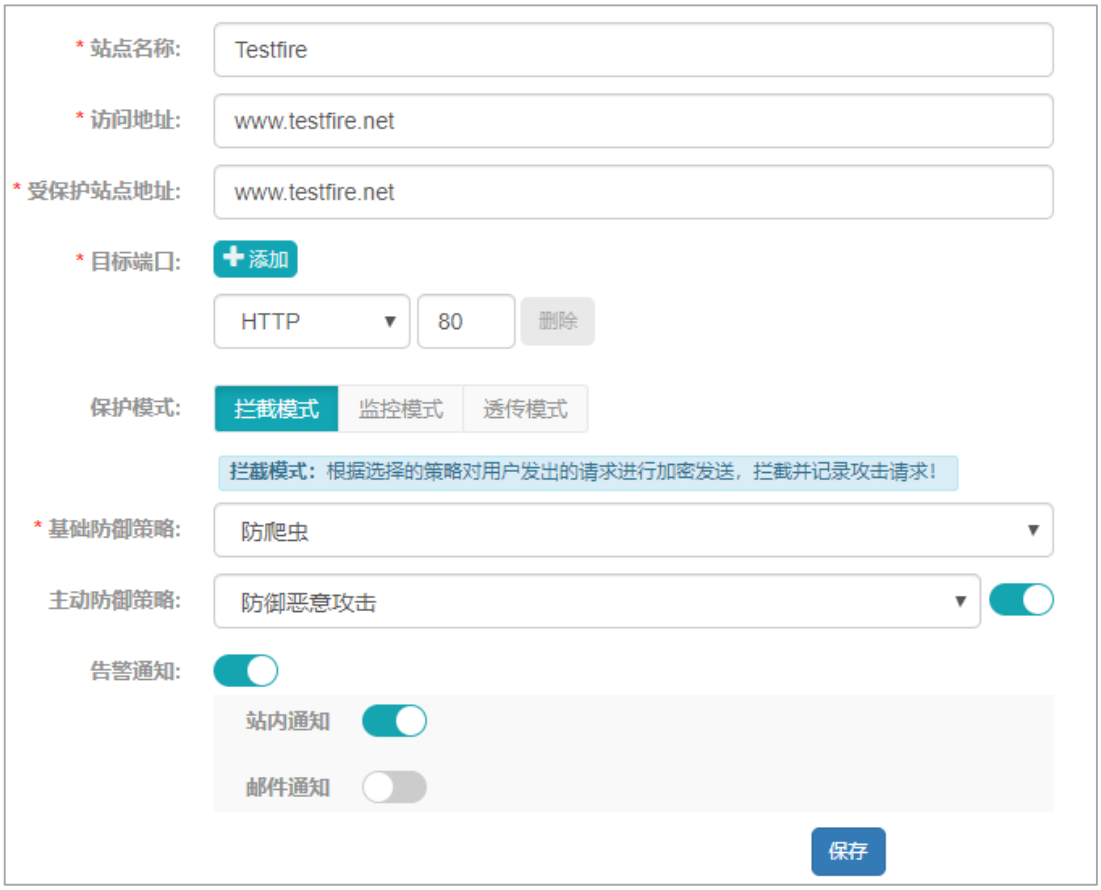


图 4-20 新增 HTTP 类型防护站点

图 4-21 站点列表初始更新

步骤 2 点击“操作”栏  按钮进行关联节点服务器，根据提示选择需要关联的“动态防御节点 IP 地址”以及“动态

防御节点端口”，随后选择对应的“保护模式”以及“基础防御策略”和“主动防御策略”，点击【保存】，如图 4-22 所示；站点列表二次更新状态，当前保护状态显示为“已停止 “，如图 4-23 所示。

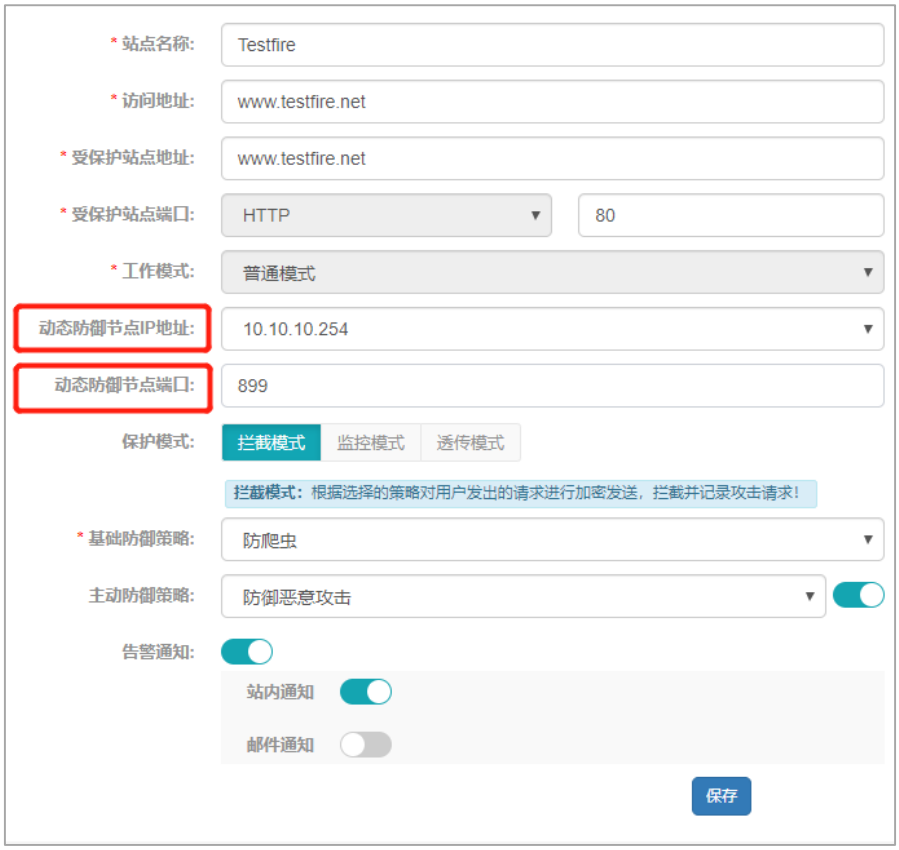


图 4-22 节点服务器关联

图 4-23 站点列表二次更新

步骤 3 选择”站点管理>节点管理>节点列表” ，找到节点服务器运行开关，如图 4-24 所示，关闭节点服务器开关，停止

状态如图 4-25 所示。

图 4-24 节点服务器运行开关

图 4-25 关闭节点服务器运行开关

步骤 4 重新启节点服务器开关，节点服务器状态为 “ ”（开启）时查看普通模式站点列表，“保护状态“更新为“运行中”，如图 4-26 所示。

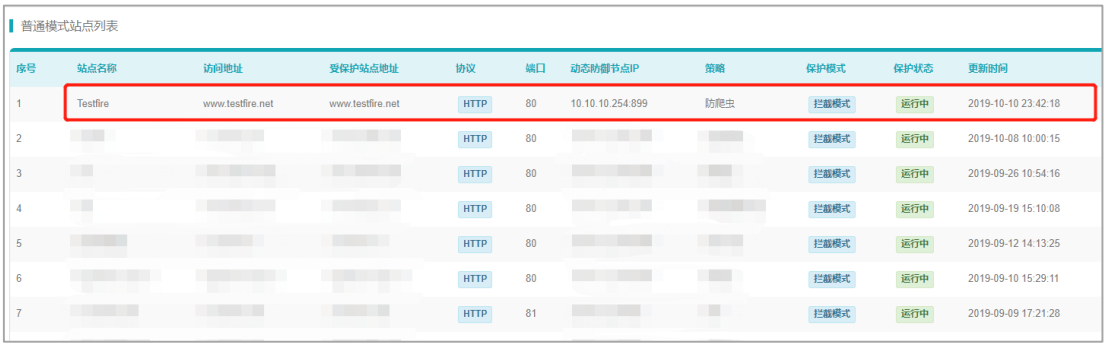


图 4-26 站点防御配置完成

步骤 5 站点防护测试配置，若为本地测试，因未绑定域名，所以通过域名访问时需先在 Windows 下配置 hosts，如图 4-27 所示；需要注意的是，这里仅作为本地测试的方式，但对于客户业务来说，需要用户通过 DNS 域名解析服务将访问流量重定向至观镜防御节点的 IP 地址。

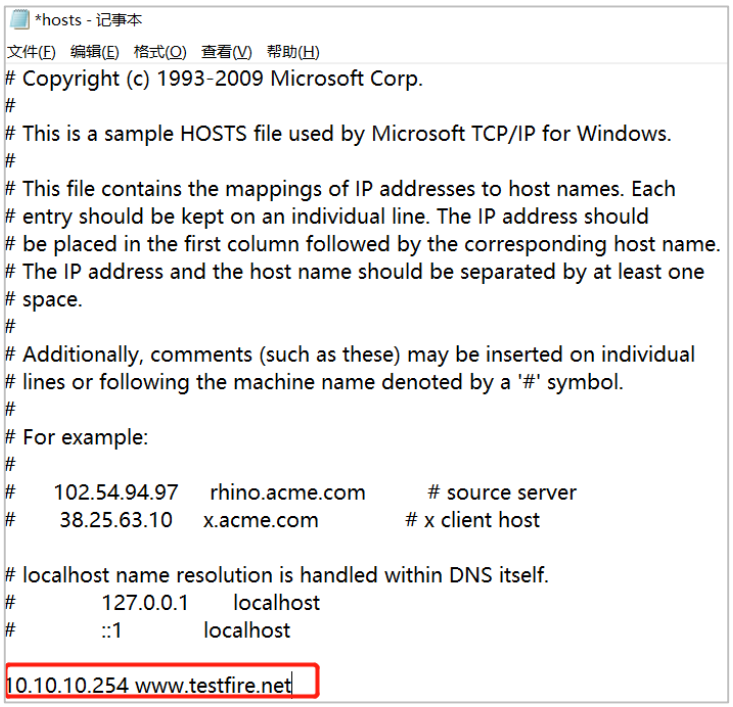


图 4-27 本地 host 修改配置

步骤 8 浏览器端访问测试站点，地址不再是原先的访问地址，而是“http(s)://动态防御节点 IP 地址 :动态防御节点端口”，查看是否和原先访问地址展示的 Web 界面一致，如图 4-28 所示。

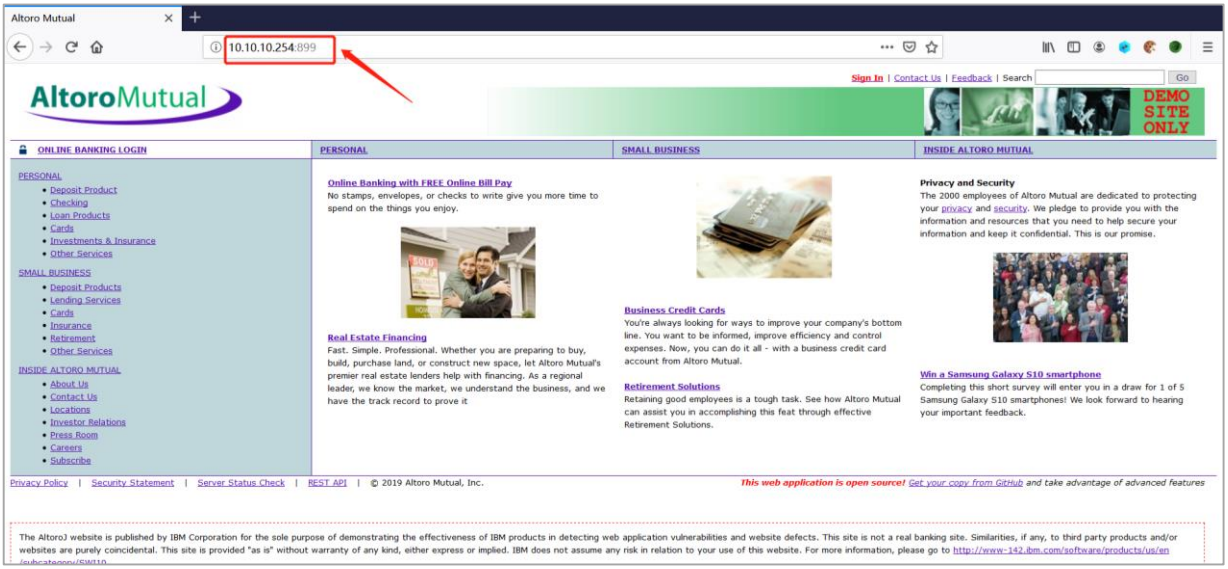


图 4-28 动态防御效果展示界面

4.2.1.2. HTTPS 类型站点配置

HTTPS 类型的站点进行防护配置时 ,在“站点管理>站点管理>新增站点”时 ,遵循的协议由“HTTP”变更为“HTTPS”，此时注意需要证书的上传，如图 4-29 所示，其余的配置顺序和 HTTP 类型的站点基本一致，可参照前文。

图 4-29 配置 HTTPS 类型防护站点

4.2.1.3. 注意事项

- 在当前已有站点处于保护状态中且节点运行的情况下，如果需要新增站点进行防护，需要在站点配置完毕、节点关联完成显示当前站点运行保护状态为“已停止”时，重新启动相关节点服务器，以便新增的防护站点配置正常生效。
- 在配置一个节点一个端口保护多个不同站点时，如果使用“节点 IP+端口”形式访问站点，则只会访问最先添加的站点，如要正常访问则根据站点配置中的访问地址进行访问即可。

4.2.2. 节点管理

节点配置中不需要在管理端进行添加，在部署系统的时候，通过配置数据库文件上报节点信息即可。

节点管理界面可对已上报的节点进行快捷关联站点、启动、停止和删除的操作。节点管理界面有节点信息统计，包含内存状态、CPU 状态、磁盘状态等。

图 4-30

4.2.3. 证书管理

证书管理主要针对 HTTPS 站点的证书更新和删除操作。

图 4-31

图 4-32 更新证书

4.2.4. 业务匹配

业务匹配功能主要将防护站点中的特定 URL 地址与业务相匹配用于识别被攻击业务的信息，支持通过普通模式、正常模式和字典模式进行匹配，支持设置全局业务字典以及单个站点业务匹配。

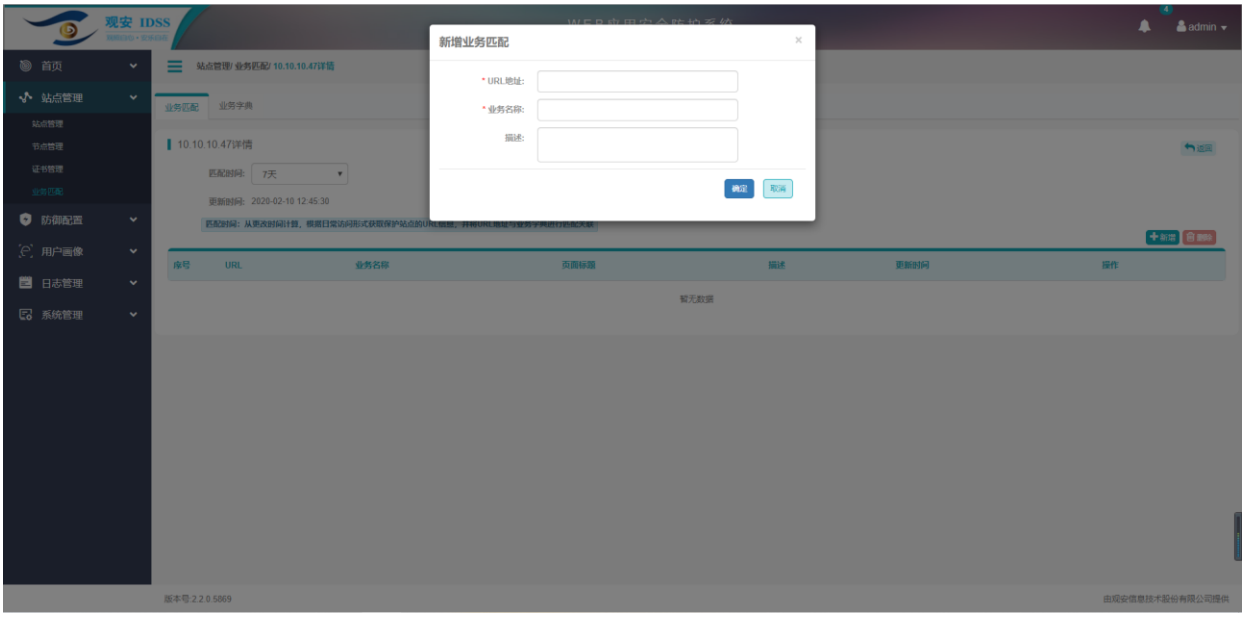


图 4-33 业务关联

4.3. 防御配置

防御配置包括主动防御配置、基础防御配置、数据脱敏配置、规则引擎配置、虚拟验证码、规则字典管理、威胁情报管理和页面监控配置。

4.3.1. 主动防御配置

主动防御配置提供系统默认三种策略模板以及自定义编辑策略，支持节点加密对象控制、敏感请求信息防护、反爬虫配置。

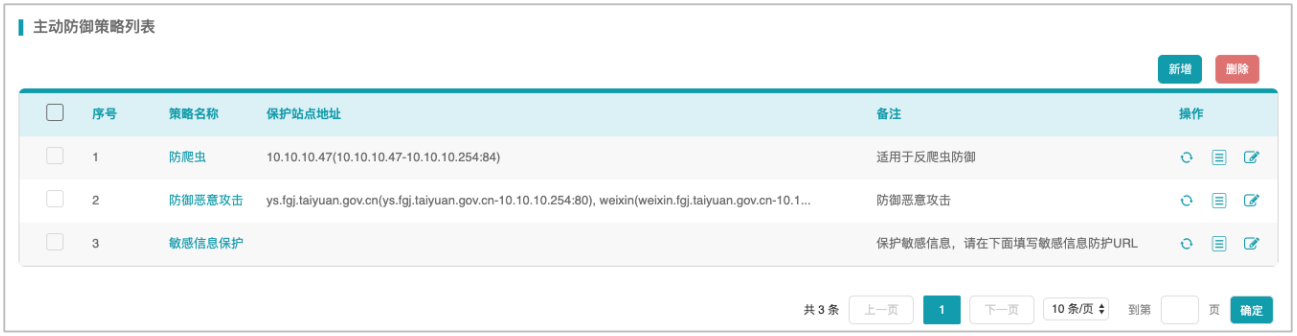


图 4-34 策略列表

4.3.2. 基础防御配置

基础防御配置提供系统默认三种策略模板以及自定义编辑策略，支持 HTTP 协议控制，异常页面重定向、文件上传限制及静态页面加速，支持设置站点白名单控制，添加在白名单内的路径不受策略限制，可有效提高兼容性，确保业务正常运行。

图 4-35 策略列表

策略中配置请求头部消息保护、敏感信息请求保护、敏感信息响应保护时支持使用普通匹配、正则匹配和字典匹配，其中字典匹配可根据提示进行配置。

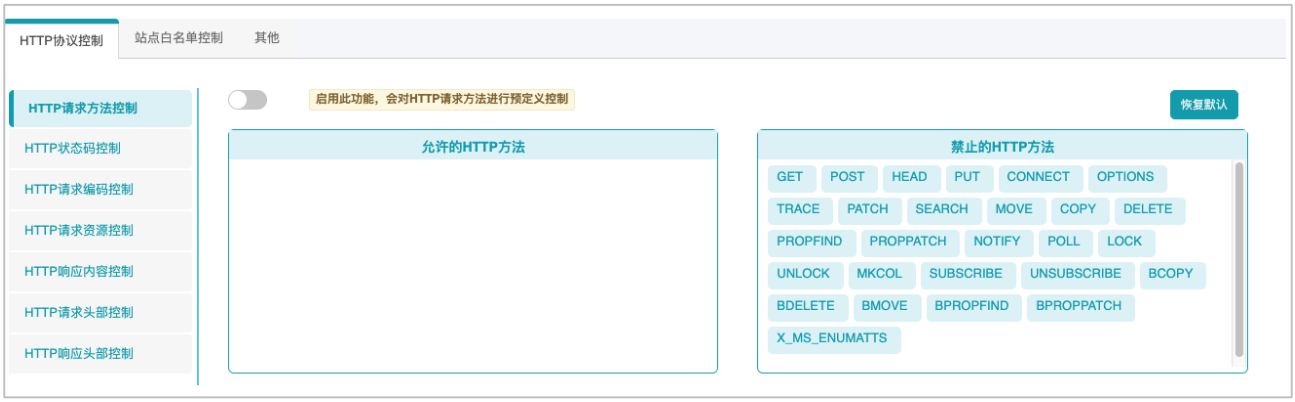


图 4-36 策略配置

4.3.2.1. HTTP 协议控制——请求方法

策略配置

步骤 1 当观镜完全部署后，以测试站点“www.testfire.net”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-37 所示。

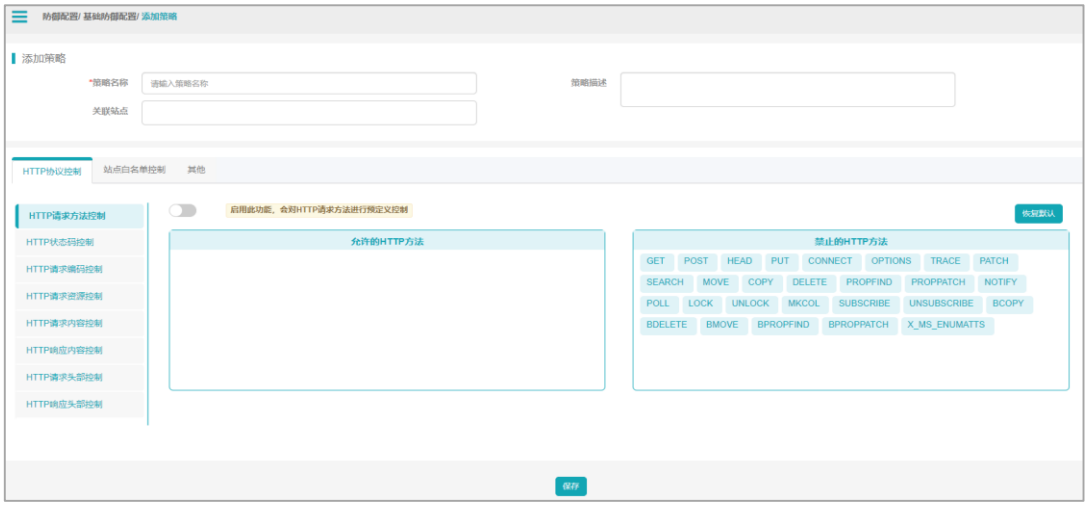


图 4-37 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如：新建策略名称为“test”，关联站点为“www.testfire.net”（观镜对此站点的防护地址为“10.10.10.254:88”），选择“HTTP 协议控制>HTTP 请求方法控制”，开启功能开关“ ”选中允许的 HTTP 请求方式为“GET”“POST”“ HEAD”,其余项默认保持禁止，点击【保存】，如图 4-38 所示。

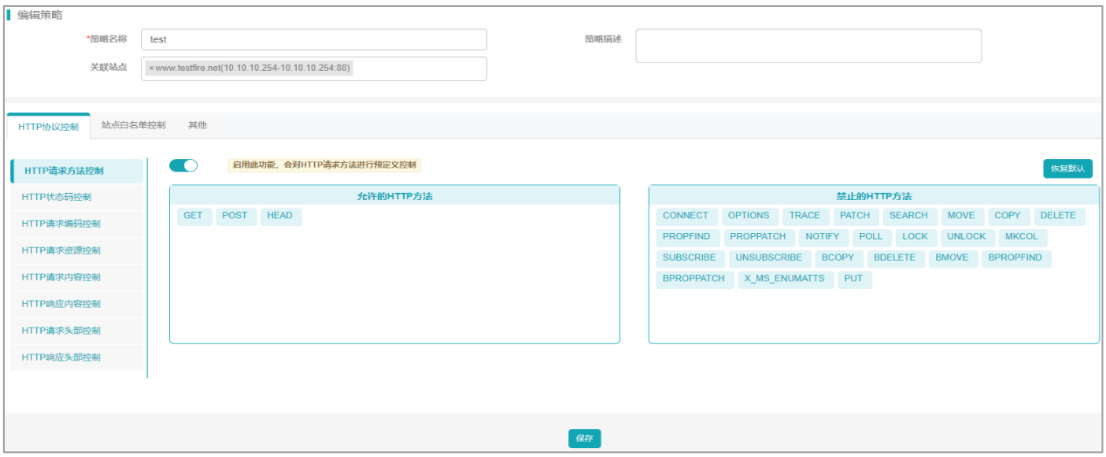


图 4-38 HTTP 请求方法控制策略配置

策略验证

以上配置完成后，针对服务器被禁止的 HTTP 请求方式时，就会被观镜阻拦，并且生成告警日志。使用 Burp Suite 抓包改包构造如上的请求方式，修改情况如图 4-39、图 4-40 所示，选择“日志管理>安全防御日志”查看告警日志，结果如图 4-41 所示。

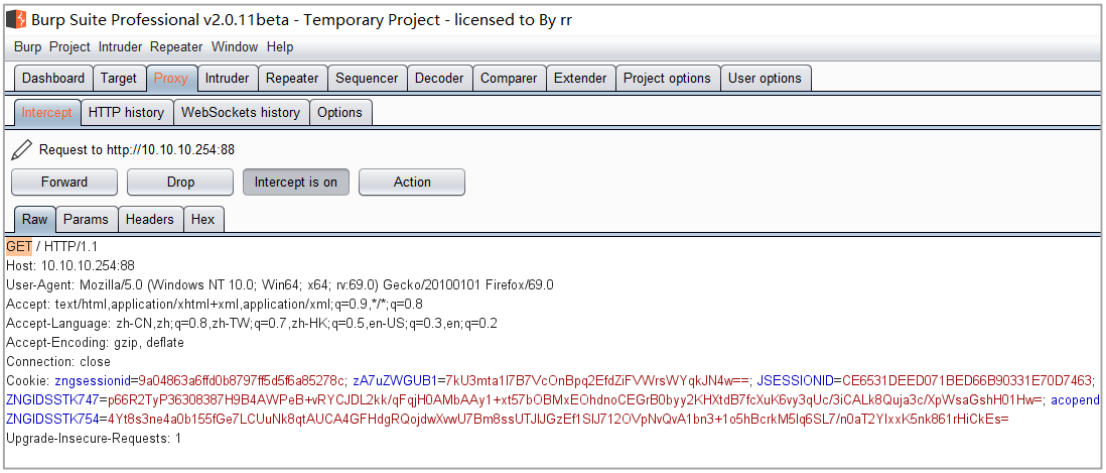


图 4-39 Burp Suite GET 请求抓包结果

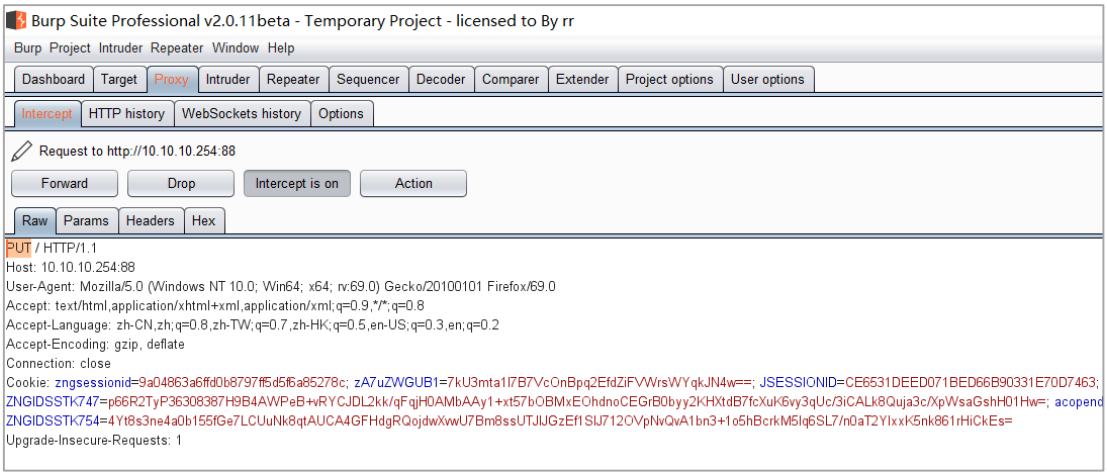


图 4-40 Burp Suite GET 请求改包（PUT 请求）结果

图 4-41 HTTP 请求方法控制告警日志

4.3.2.2. HTTP 协议控制——状态码

策略配置

步骤 1 当观镜完全部署后，以测试站点“www.testfire.net”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-42 所示。

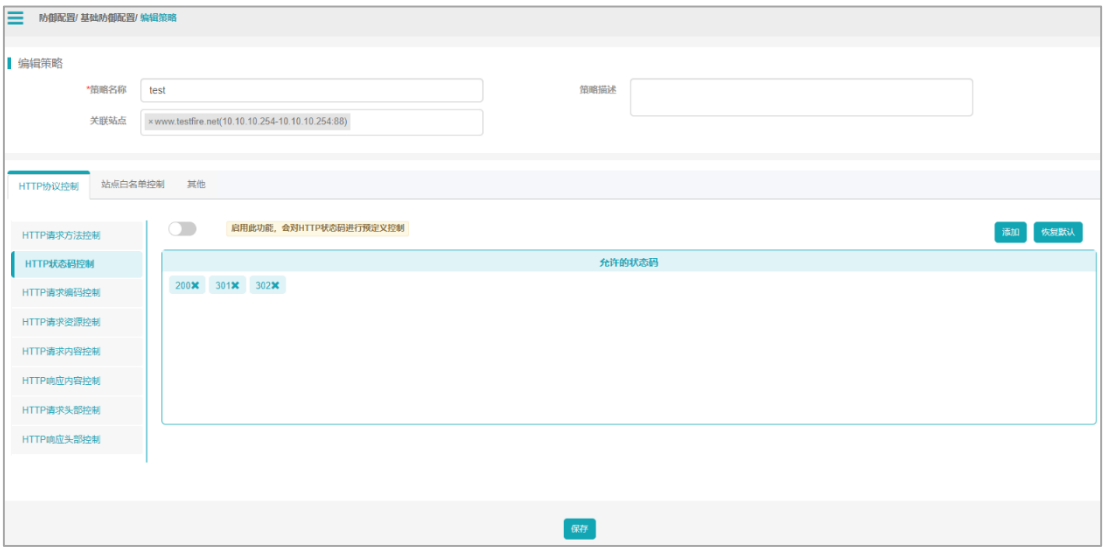


图 4-42 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如：新建策略名称为“test”，关联站点为“www.testfire.net”（观镜对此站点的防护地址为“10.10.10.254:88”），选择“HTTP 协议控制>HTTP 状态码控制”，开启功能开关“ ”选中允许的 HTTP 响应状态码为“200”“301”“302”（也可点击【添加】按钮编辑新的状态码），点击【保存】，如图 4-43 所示。

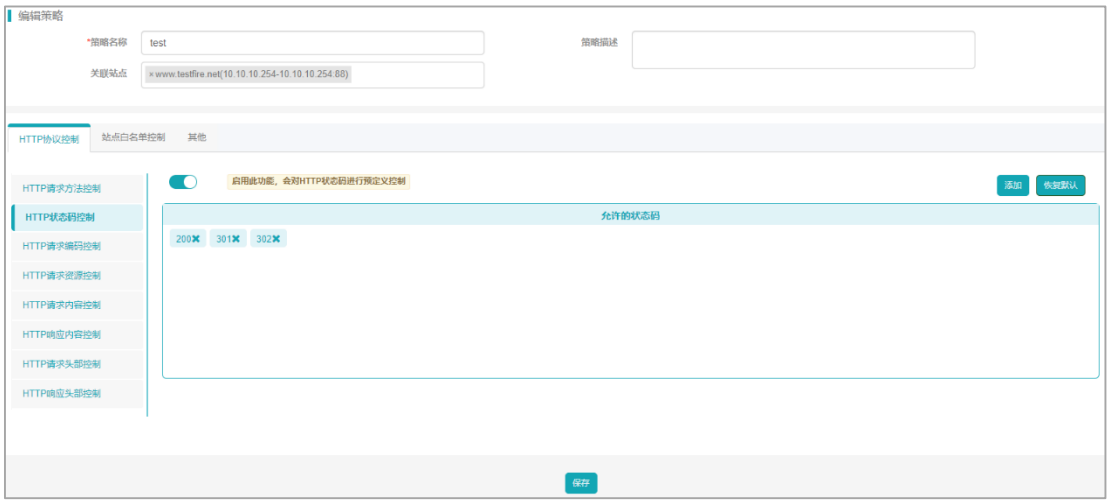


图 4-43 HTTP 状态码控制策略配置

策略验证

以上配置完成后，针对服务器触发被禁止返回的 HTTP 状态码例如“304”时，就会被观镜阻拦，并且生成告警日志，

选择“日志管理>安全防御日志”查看告警日志，结果如图 4-44 所示。

图 4-44 HTTP 状态码控制告警日志

4.3.2.3. HTTP 协议控制——请求编码

策略配置

步骤 1 当观镜完全部署后，以测试站点“10.10.10.47”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-45 所示。

图 4-45 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如 新建策略名称为“test”，关联站点为“10.10.10.47”（观镜对此站点的防护地址为“10.10.10.254:90”）选择“HTTP 协议控制>HTTP 请求编码控制”，开启功能开关“ ”

选中允许的 HTTP 请求编码为“HEX”“BASE64”，禁止的 HTTP 请求编码为“URL”、“UNICODE”，点击【保存】，如图 4-46 所示。

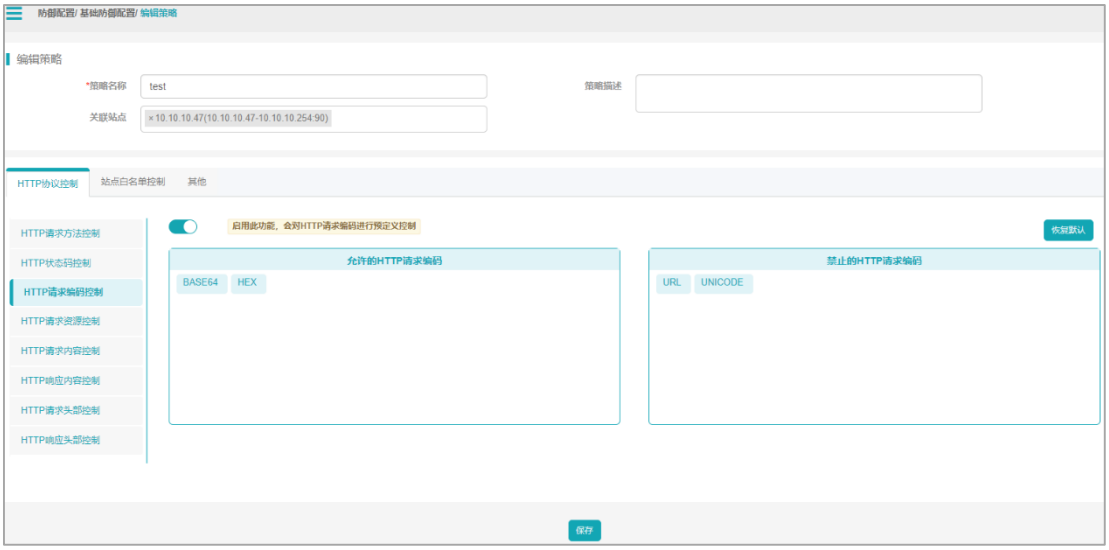


图 4-46 HTTP 请求编码控制策略配置

策略验证

以上配置完成后，针对服务器触发被禁止 HTTP 请求编码例如“URL”时，就会被观镜阻拦，并且生成告警日志，选择“日志管理>安全防御日志”查看告警日志，结果如图 4-47 所示。

图 4-47 HTTP 请求编码控制告警日志

4.3.2.4. HTTP 协议控制——请求资源

策略配置

步骤 1 当观镜完全部署后，以测试站点“www.testfire.net”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-48 所示。

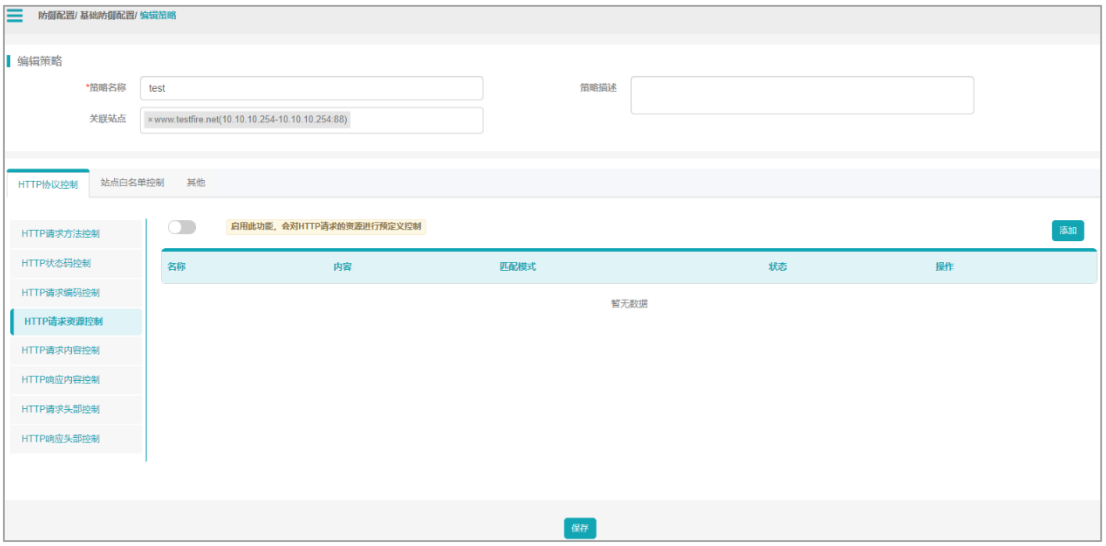


图 4-48 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如：新建策略名称为“test”，关联站点为“www.testfire.net”（观镜对此站点的防护地址为“10.10.10.254:88”），选择“HTTP 协议控制”>“HTTP 请求资源控制”，开启功能开关“ ”，点击【添加】，新增 HTTP 请求资源控制，对应填入“名称”、“匹配模式”、“内容”、“动作”，这里以禁止请求访问 htm 资源为例，点击【保存】，如图 4-49 所示。

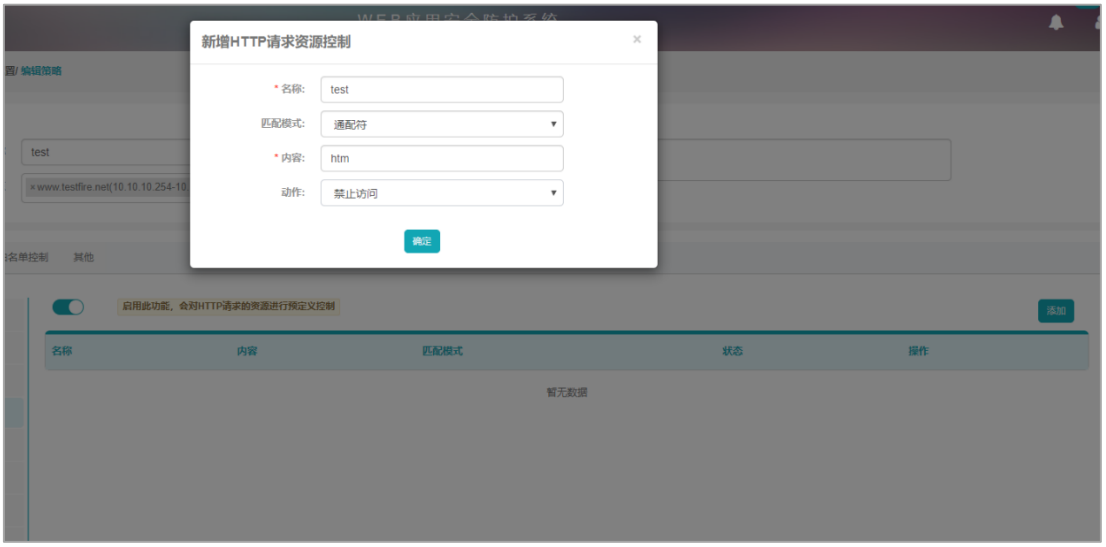


图 4-49 HTTP 请求资源控制策略配置

策略验证

以上配置完成后，针对服务器请求访问被禁止的 htm 资源时，就会被观镜阻拦，并且生成告警日志，选择“日志管理>安全防御日志”查看告警日志，结果如图 4-50 所示。

图 4-50HTTP 请求资源控制告警日志

4.3.2.5. HTTP 协议控制——请求内容

策略配置

步骤 1 当观镜完全部署后，以测试站点“www.testfire.net”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-51 所示。

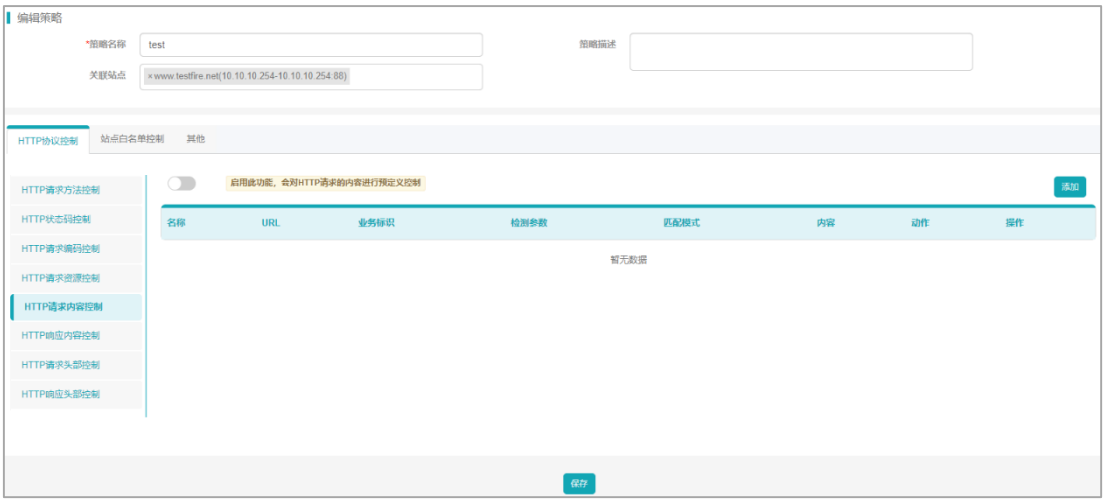


图 4-51 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如 新建策略名称为“test”，关联站点为“10.10.10.47”（观镜对此站点的防护地址为“10.10.10.254:90”）选择“HTTP 协议控制>HTTP 请求内容控制”，开启功能开关“ ”，点击【添加】，新增 HTTP 请求内容控制，对应填入“名称”、“URL”、“检测参数”、“匹配模式”、“内容”、“动作”，这里以禁止请求 URL 路径为“/awstats/awstats.pl”下当参数 “config”内容为“owaspba”为例，点击【保存】，如图 4-52 所示。

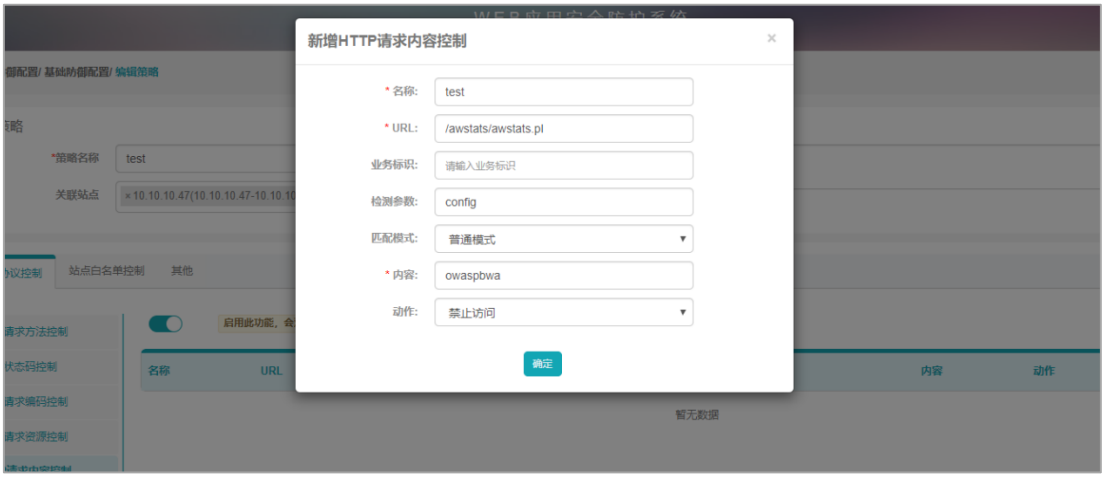


图 4-52 HTTP 请求内容控制策略配置

策略验证

以上配置完成后，针对服务器触发被禁止返回的 HTTP 请求内容时，就会被观镜阻拦，并且生成告警日志，选择“日志管理>安全防御日志”查看告警日志，如图 4-53 所示。

图 4-53 请求内容控制验证

4.3.2.6. HTTP 协议控制——响应内容

策略配置

步骤 1 当观镜完全部署后，以测试站点”10.10.10.47”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-54 所示。

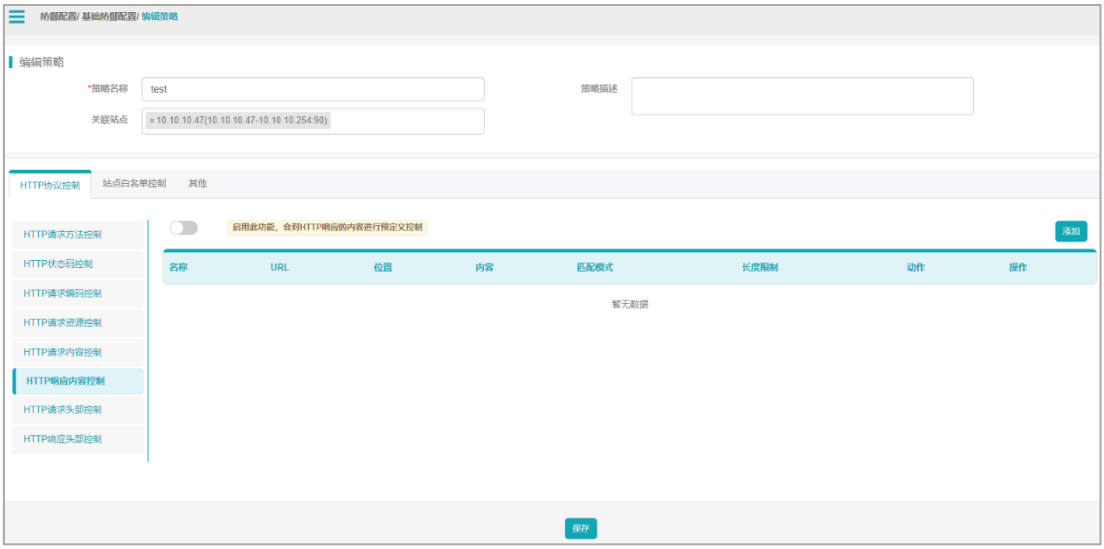


图 4-54 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如 新建策略名称为“test”，关联站点为“10.10.10.47”（观镜对此站点的防护地址为“10.10.10.254:90”）选择“HTTP 协议控制>HTTP 响应内容控制”，开启功能开关“ ”点击【添加】，新增 HTTP 响应内容控制，对应填入“名称”、“URL”、“内容”、“动作”，这里以禁止请求 URL 路径为“/wordpress/”下的“New Plug-ins”内容为例，如图 4-55 所示。

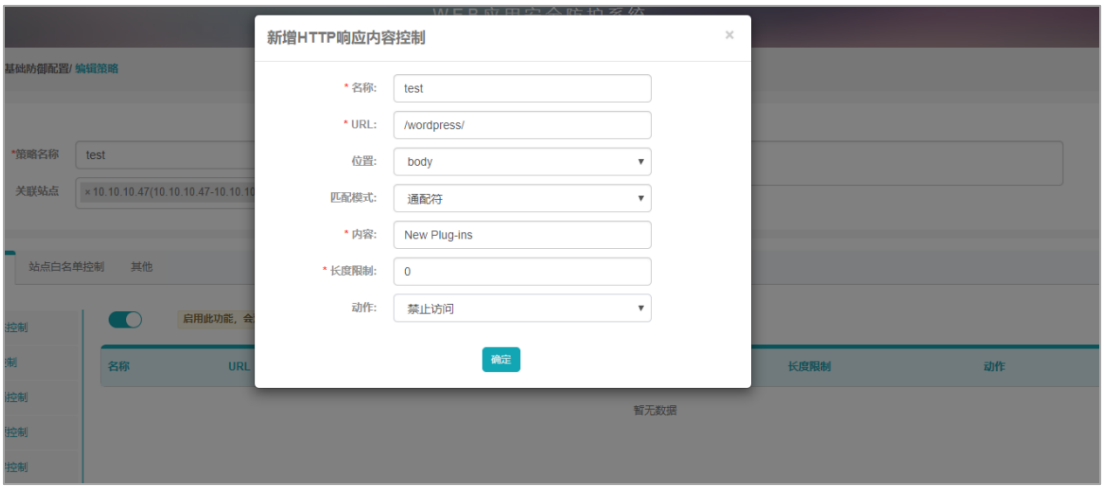


图 4-55 HTTP 响应内容控制策略配置

策略验证

以上配置完成后，针对服务器触发被禁止的 HTTP 响应内容时，就会被观镜阻拦，并且生成告警日志，选择“日志管理>安全防御日志”查看告警日志，结果如图 4-56 所示。

图 4-56HTTP 响应内容控制告警日志

4.3.2.7. HTTP 协议控制——请求头部

策略配置

步骤 1 当观镜完全部署后，以测试站点”10.10.10.47”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-57 所示。

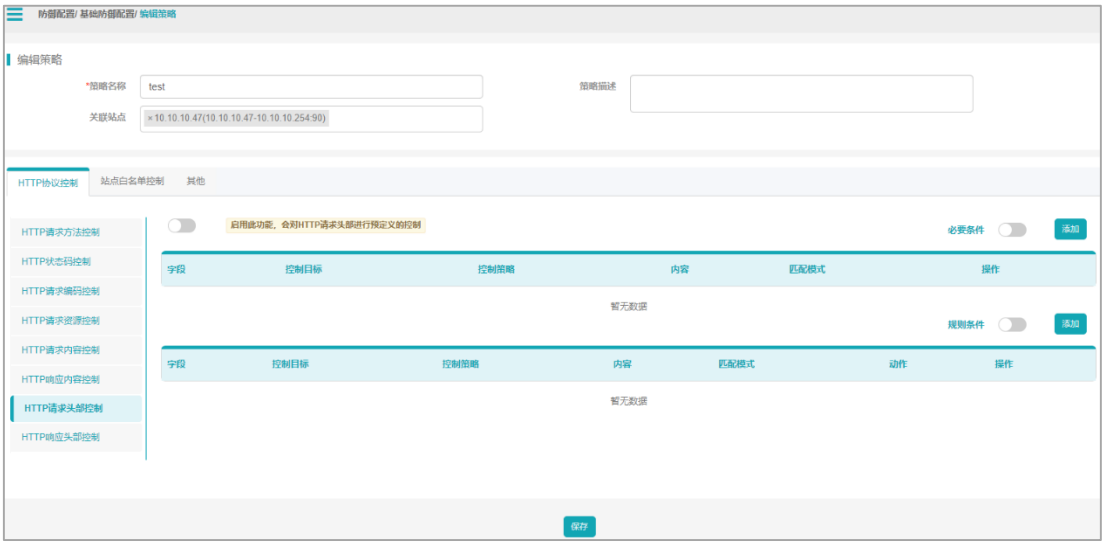


图 4-57 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如 新建策略名称为“test”，关联站点为“10.10.10.47”（观镜对此站点的防护地址为“10.10.10.254:90”），选择“HTTP 协议控制”>“HTTP 请求头部控制”，开启功能开关以及规则条件开关“ ”，点击【添加】，对应填入“字段”、“控制目标”、“控制策略”、“匹配模式”、“字典类型”、“动作”，这里以禁止访问当字段“User-Agent”下的内容为“Mozilla”为例，点击【保存】，如图 4-58 所示。

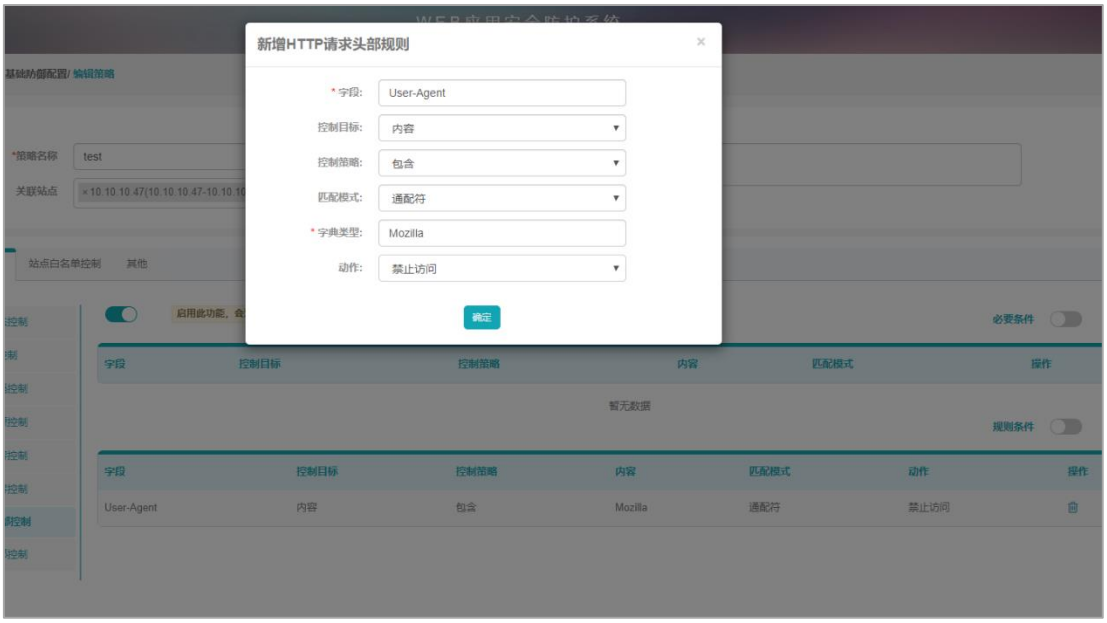


图 4-58 HTTP 请求头部控制策略配置

策略验证

以上配置完成后，针对服务器触发被禁止返回的 HTTP 请求头部信息时，就会被观镜阻拦，并且生成告警日志，选择“日志管理>安全防御日志”查看告警日志，结果如图 4-59 所示。

图 4-59 HTTP 状态码控制告警日志

4.3.2.8. HTTP 协议控制——响应头部

策略配置

步骤 1 当观镜完全部署后，以测试站点”10.10.10.47”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-60 所示。

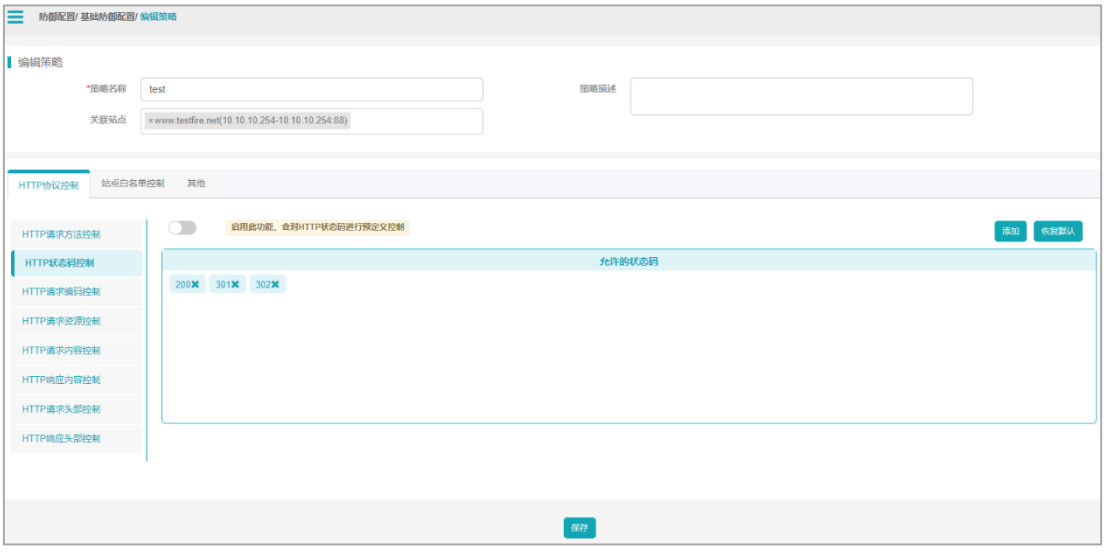


图 4-60 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如 新建策略名称为“test”，关联站点为“10.10.10.47”（观镜对此站点的防护地址为“10.10.10.254:90”），选择“HTTP 协议控制>HTTP 响应头部控制”，开启功能开关以及规则条件开关“ ”，点击【添加】，对应填入“字段”、“控制目标”、“控制策略”、“匹配模式”、“字典类型”、“动作”，这里以禁止访问当字段“Set-Cookie”下的内容为“zngsessionid”为例，点击【保存】，如图 4-61 所示。

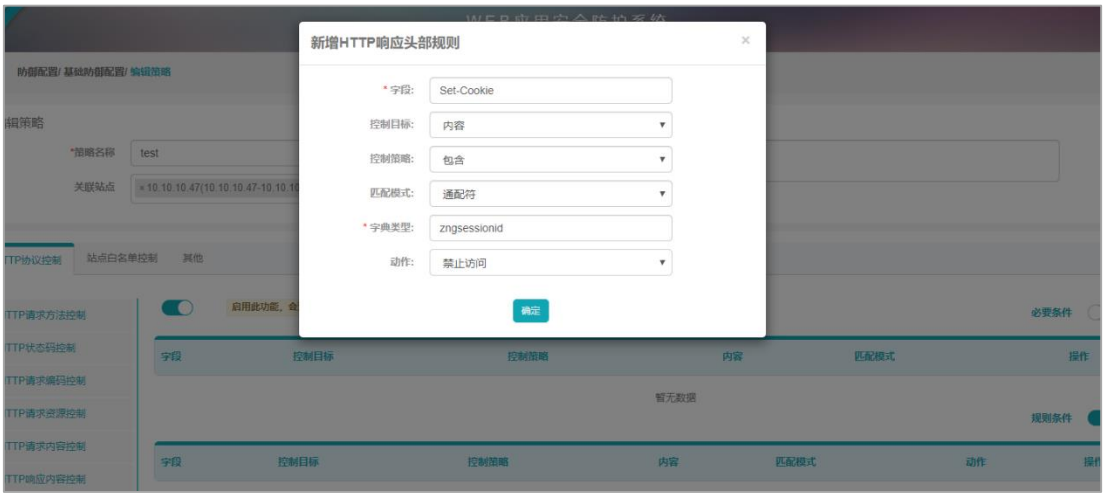


图 4-61 HTTP 响应头部控制策略配置

策略验证

以上配置完成后，针对服务器触发被禁止返回的 HTTP 响应头部信息时，就会被观镜阻拦，并且生成告警日志，选择“日志管理>安全防御日志”查看告警日志，结果如图 4-62 所示。

图 4-62 HTTP 响应头部控制告警日志

4.3.2.9. 异常页面重定向

策略配置

步骤 1 当观镜完全部署后，以测试站点“10.10.10.47”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下“ ”按钮直接编辑即可，新增策略如图 4-63 所示。

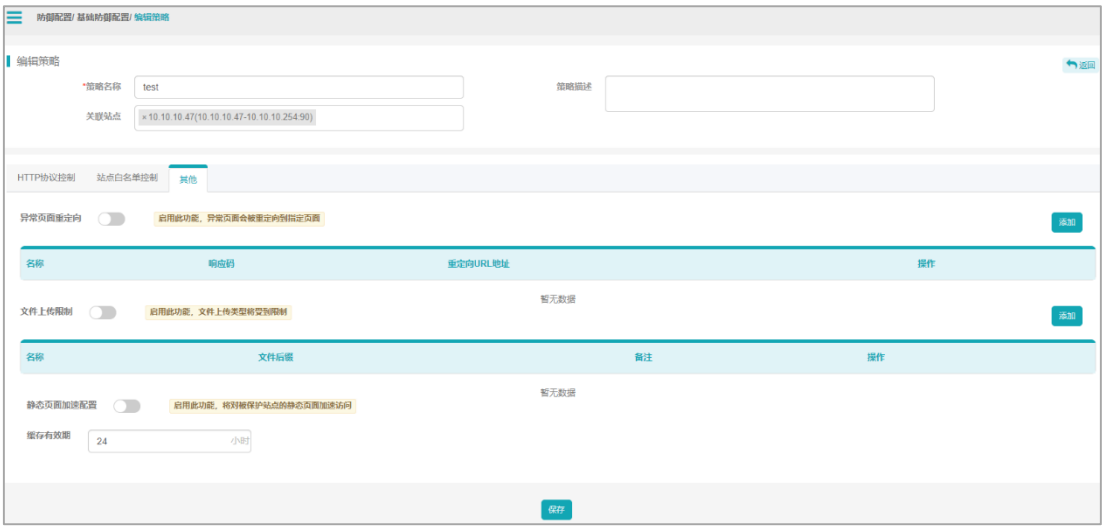


图 4-63 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如 新建策略名称为“test”，关联站点为“10.10.10.47”（观镜对此站点的防护地址为“10.10.10.254:90”），选择“其他>异常页面重定向”，开启功能开关“ ”，点击【添加】，新增异常页面重定向配置，输入“名称”、“响应码”、“重定向 url 地址”，这里以当响应码为“403”时，重定向页面至“http://www.baidu.com”为例，点击【保存】，如图 4-64 所示。

图 4-64 异常页面重定向策略配置

策略验证

以上配置完成后，针对服务器触发被状态码“403”时，就会被观镜阻拦，并重定向至百度首页，结果如图 4-65 所示。

图 4-65 异常页面重定向结果

4.3.2.10. 文件上传限制

策略配置

步骤 1 当观镜完全部署后，以测试站点“10.10.10.47”为例。选择“防御配置>基础防御配置>基础防御策略列表”，点击【新增】添加策略，或者点击序号 1~3 系统默认自带的三种策略下的“ ”按钮直接编辑即可，新增策略如图 4-66 所示。

图 4-66 基础防御配置编辑策略

步骤 2 按提示对应输入“策略名称”、“策略描述”以及“关联站点”，例如 新建策略名称为“test”，关联站点为“10.10.10.47”（观镜对此站点的防护地址为“10.10.10.254:90”），选择“其他>文件上传限制”，开启功能开关“ ”，点击【添加】，新增文件上传限制配置，输入“名称”、“备注”、“文件后缀”，这里文件后缀为“php”限制上传为例，点击【保存】，如图 4-67 所示。

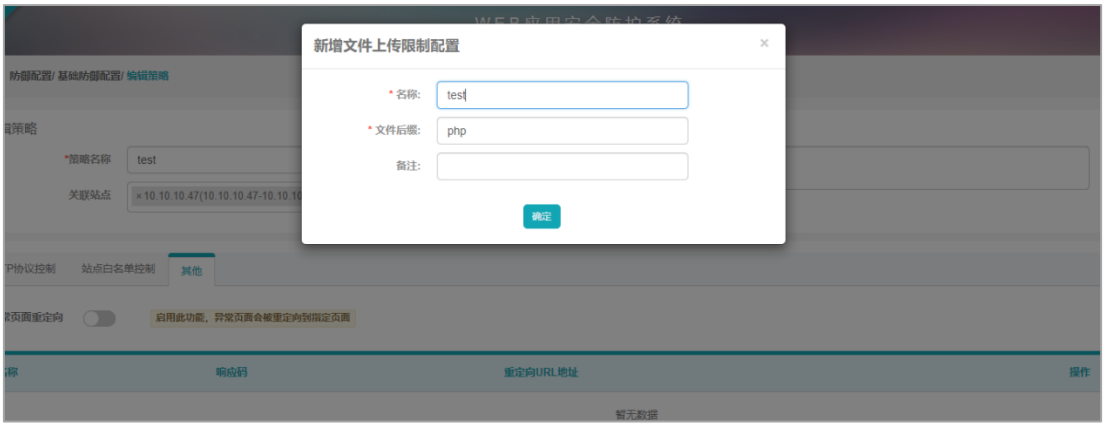


图 4-67 文件上传限制策略配置

策略验证

以上配置完成后，针对服务器上传 php 文件时时，就会被观镜阻拦，并且生成告警日志，选择“日志管理>安全防御日志”查看告警日志，结果如图 4-68 所示。

图 4-68 文件上传限制告警日志

4.3.3. 数据脱敏配置

通过配置指定的位置，选择响应的加密算法对数据进行脱敏配置。

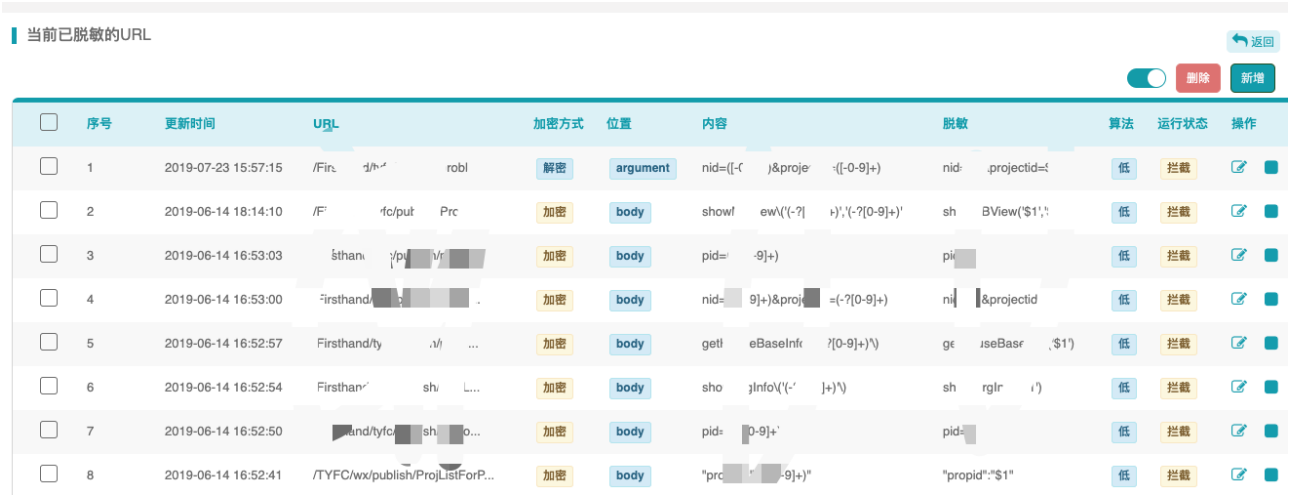


图 4-69 数据脱敏配置列表

策略配置

步骤 1 当观镜完全部署后，以测试站点“www.testfire.net”为例。选择“防御配置>数据脱敏配置>基础防御策略列表”，找到目标站点后，开启功能开关“ ”，点击【新增】，添加目标站点下需要脱敏的 URL，填入“加密方式”、“URL”、“内容”、“脱敏”、“算法”、“加密方式”、“运行状态”、“是否启动”相关信息后，点击【确定】，这里以 URL 路径为“/index.jsp”下的“Phone”内容中的“1.800.555.0002”脱敏为“xxxx”为例，配置结果如图 4-70，图 4-71 所示。

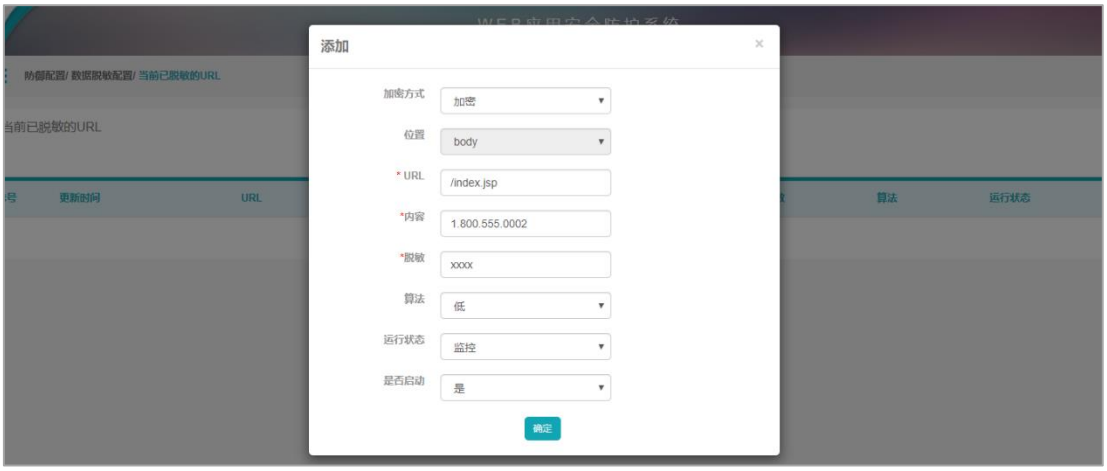


图 4-70 数据脱敏配置编辑策略

图 4-71 数据脱敏配置编辑策略完成

策略验证

以上配置完成后，针对服务器目标站点刷新页面后，会发现“Phone”内容中“1.800.55.002”成功脱敏为“xxxx”，对比结果如图 4-72、图 4-73 所示。

图 4-72 数据脱敏前后目标站点内容

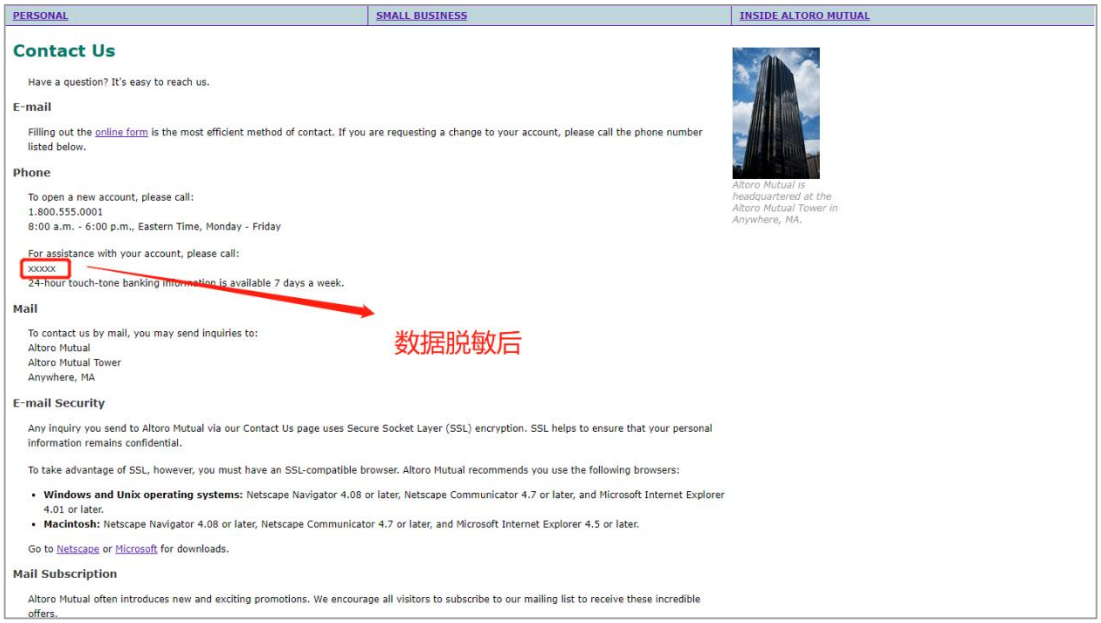


图 4-73 数据脱敏后后目标站点内容

4.3.4. 规则引擎配置

规则引擎为用户提供了自定义规则的功能，为了更完善的适应站点的业务，根据站点日常访问量来精准的配置更适合站点的策略，通过 UID 来精准识别访问源，可以更精准的防范恶意访问而不误杀，支持配置访问触发规则时的处理方式，如界面通知或邮件通知，以及拉入恶意 IP 库等。

图 4-74 规则引擎配置列表

策略配置

步骤 1 当观镜完全部署后，以测试站点“10.10.10.47”为例。选择“防御配置>规则引擎配置>规则引擎列表”，点击【新建规则】添加规则，对应输入“规则名称”、“地址”、“规则”、“动作”，点击【确定】，新建规则如图 4-75、图 4-76 所示。

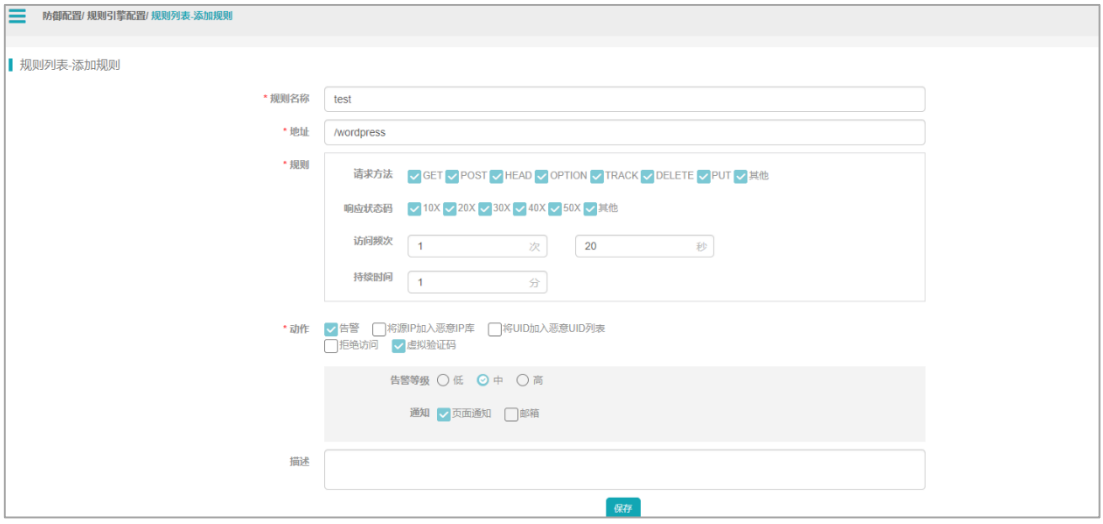


图 4-75 规则引擎配置编辑策略

图 4-76 规则引擎配置编辑策略完成

步骤 2 择“防御配置>虚拟验证码”，开启功能开关“ ”，选择“验证复杂程度”、“验证码长度”、“默认验证配置”、“失败验证配置”，点击【确定】，配置结果如图 4-77 所示。

图 4-77 虚拟验证码配置

策略验证

以上配置完成后，针对服务器目标站点按规则频次访问后，就会被观镜阻拦，提示验证码信息，结果如图 4-78 所示。

图 4-78 规则引擎触发告警

4.3.5. 虚拟验证码

虚拟验证码用于在出发规则引擎后的处置动作，支持配置复杂度及验证次数等。

图 4-79 虚拟验证码

4.3.6. 规则字典管理

字典管理用来对策略配置中选择的字典进行管理，对站点的业务关联提供全局字典等。字典类型包括业务关联、头部保护、敏感信息和敏感响应四类，支持普通模式和正则模式两种。

图 4-80 字典配置

4.3.7. 威胁情报管理

威胁情报管理当前版本主要用于对恶意 IP、恶意用户以及 IP 安全组的管理，系统内置数十万条全球范围内的恶意 IP 数据，支持人工添加 IP，支持从日志中快捷添加至恶意 IP 库中以阻止访问，并且可以对恶意 IP 进行导出操作。

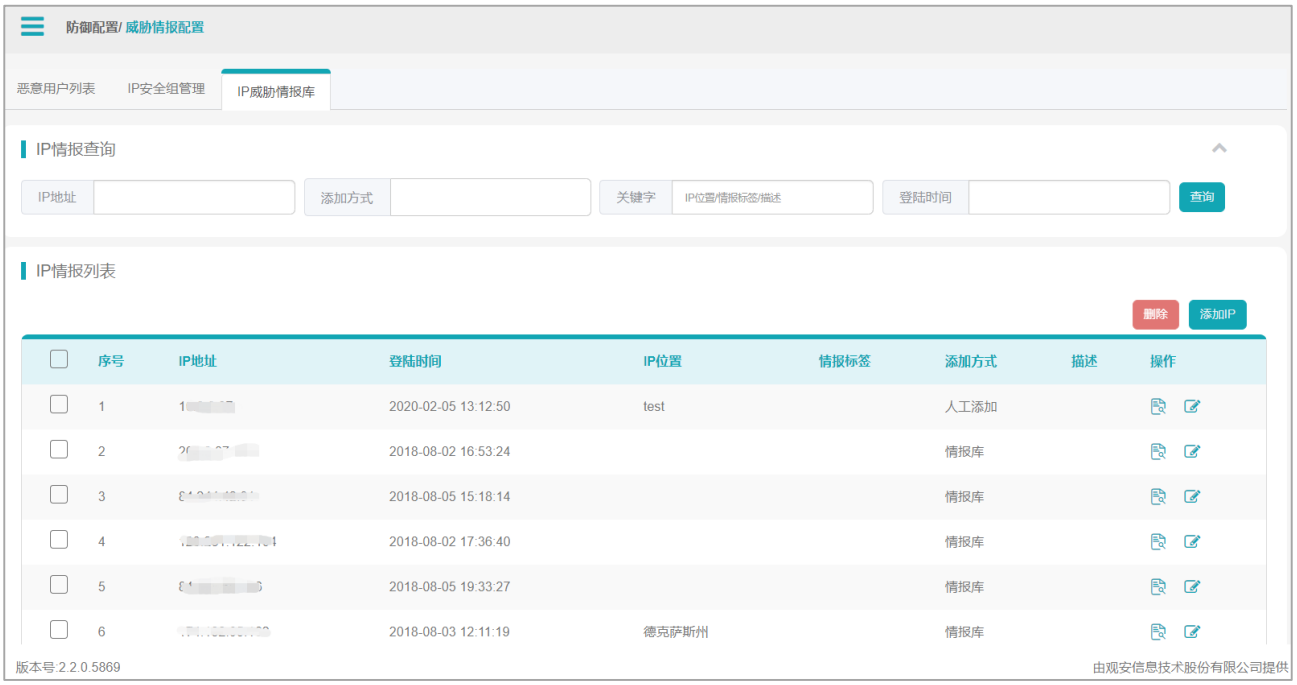


图 4-81 恶意 IP

安全组管理支持用户自定义访问规则，设置指定 IP 或 IP 段允许访问、透传访问或禁止访问，并更具规则优先级进行执行，方便用户在特殊环境下对网站进行安全操作。

图 4-82 用户自定义安全组

4.3.8. 页面监控配置

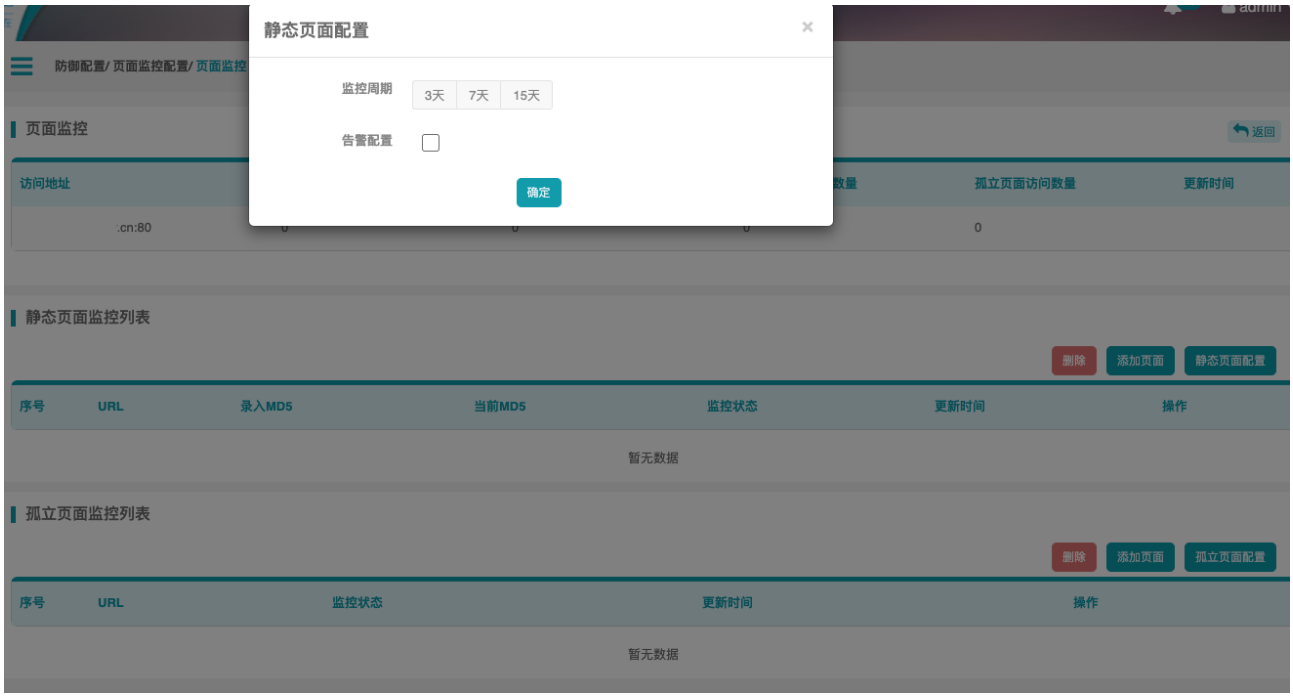


图 4-83 页面监控配置

4.4. 用户画像

通过各种指纹将来访用户标记为唯一用户，并统计该用户的访问信息。

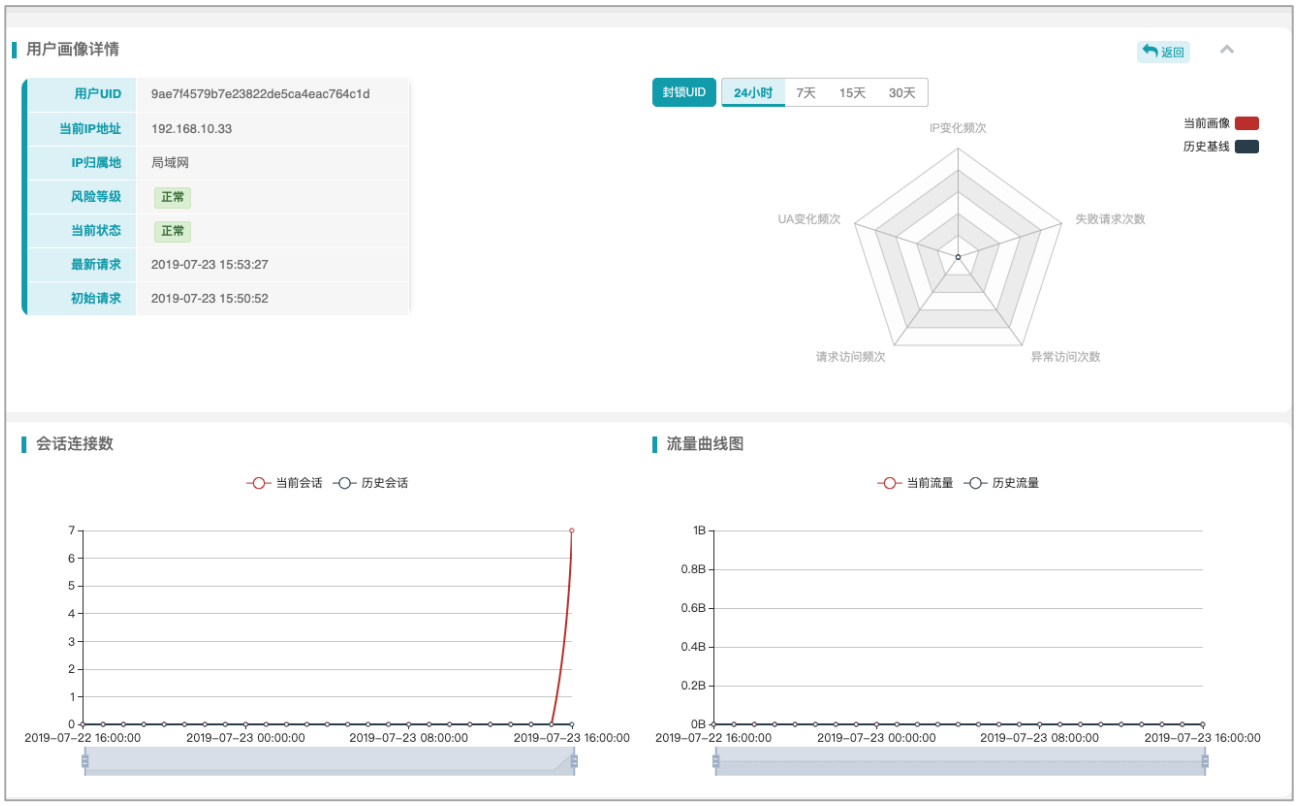


图 4-84 用户画像

4.5. 日志管理

4.5.1. 安全防御日志

防御日志中可查看所有保护站点记录的请求记录，支持通过多种条件进行组合查询，方便用户对攻击进行溯源。支持通过快捷操作将访问日志中的 IP 地址添加至安全组规则或恶意 IP 库，支持将访问日志中的被访问 URL 地址添加至策略中的站点白名单，以免一项正常业务的运行。

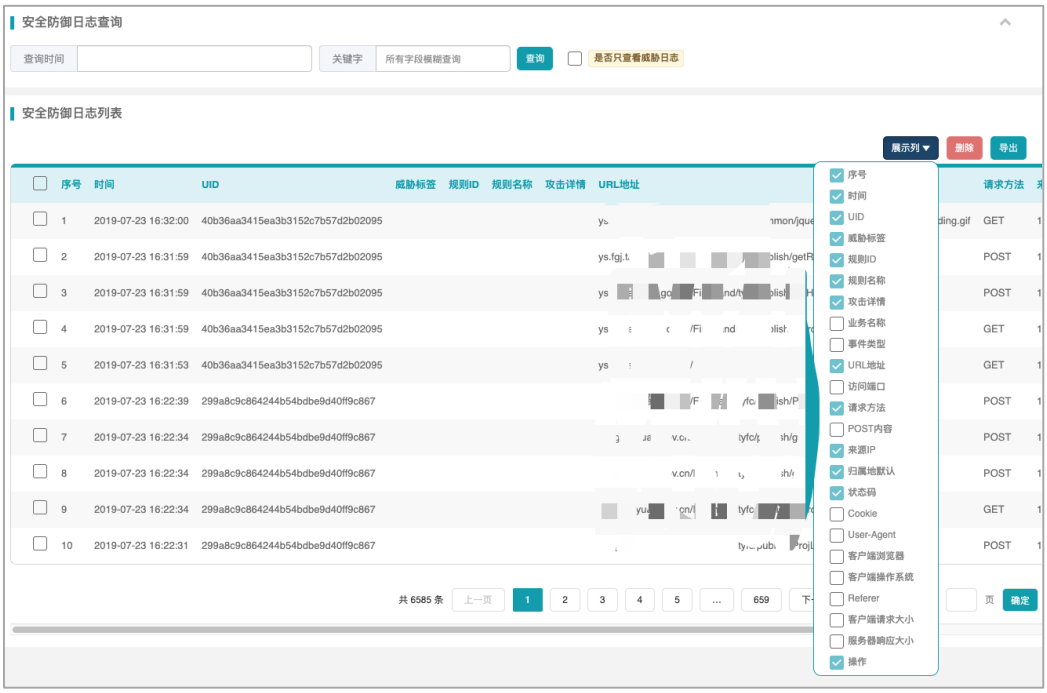


图 4-85 防御日志

图 4-86 快捷发送至恶意 IP 库

图 4-87 快捷发送至安全组规则

图 4-88 快捷发送至策略白名单

4.5.2. 系统操作日志

系统操作日志提供当前系统登录登出以及功能操作等信息记录，方便用户查看系统操作信息。

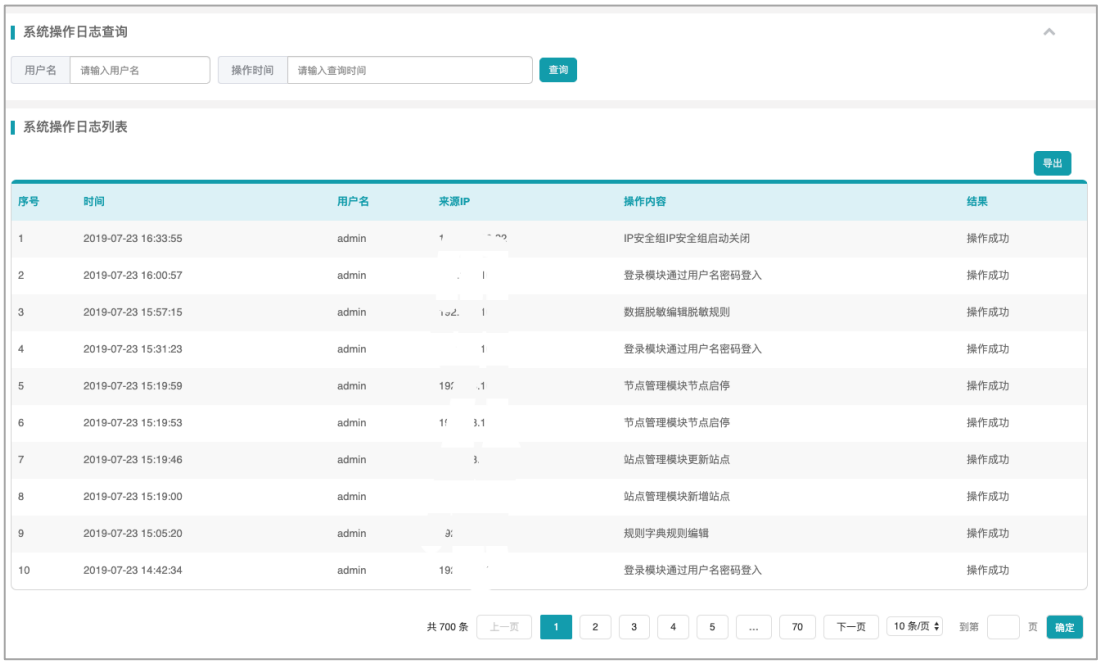


图 4-89 系统操作日志

4.5.3. 告警通知日志

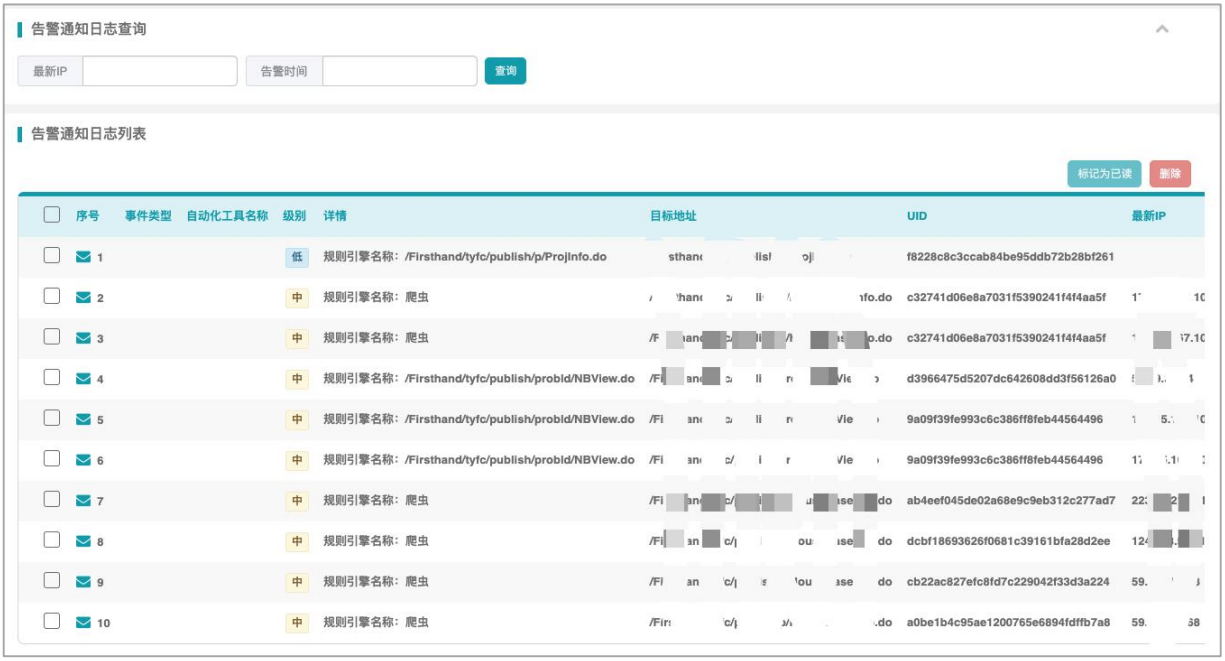


图 4-90

4.6. 系统管理

4.6.1. 用户管理

用户管理界面支持增加和更新用户信息，支持创建普通用户和管理员两种角色用户，其中管理员角色拥有系统所有操作权限，普通角色用户只有查看权限，还可以通过用户管理对用户进行锁定和解锁操作，支持配置登入策略，当连续失败 N 次时锁定设定时间。

图 4-91

图 4-92

图 4-93

4.6.2. 存储配置

日志配置提供通过 Syslog 和 FTP 来管理日志服务器，可通过配置输出指定类型的日志，为避免持续访问造成的日志

量过大，提供日志磁盘归档管理，当日志容量达到设定阈值时则对旧日志进行归档操作。

图 4-94 日志配置

4.6.3. 告警配置

通过告警配置对系统告警进行统一管理。

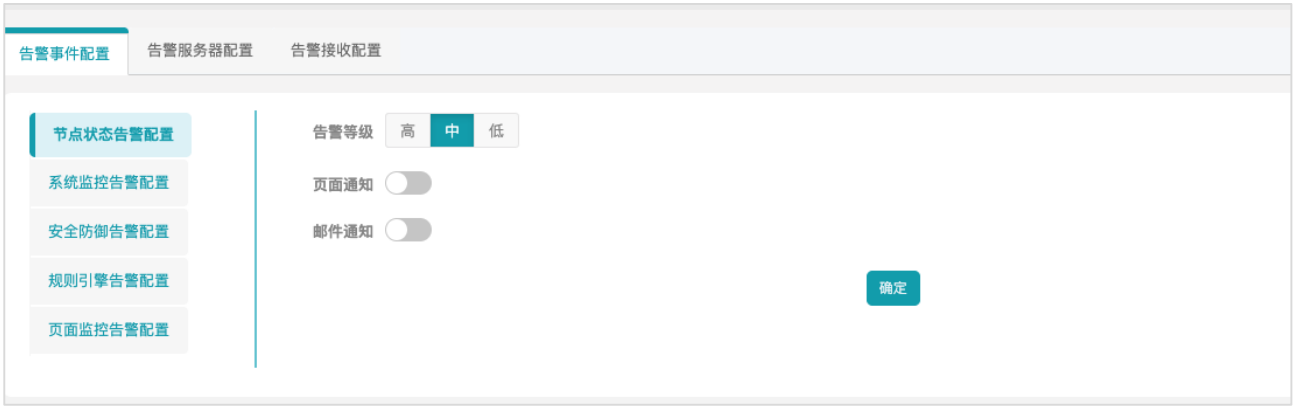


图 4-95 告警配置

配置邮箱服务器作为发送端，如未正确配置则无法发送邮箱告警功能。

图 4-96 日志配置

4.6.4. 系统信息

通过版本信息可以直接查看观镜 Web 应用安全防护系统 2.1 的当前版本以及授权信息，可以通过上传更新包离线升级系统以及更新授权文件，如下图所示：

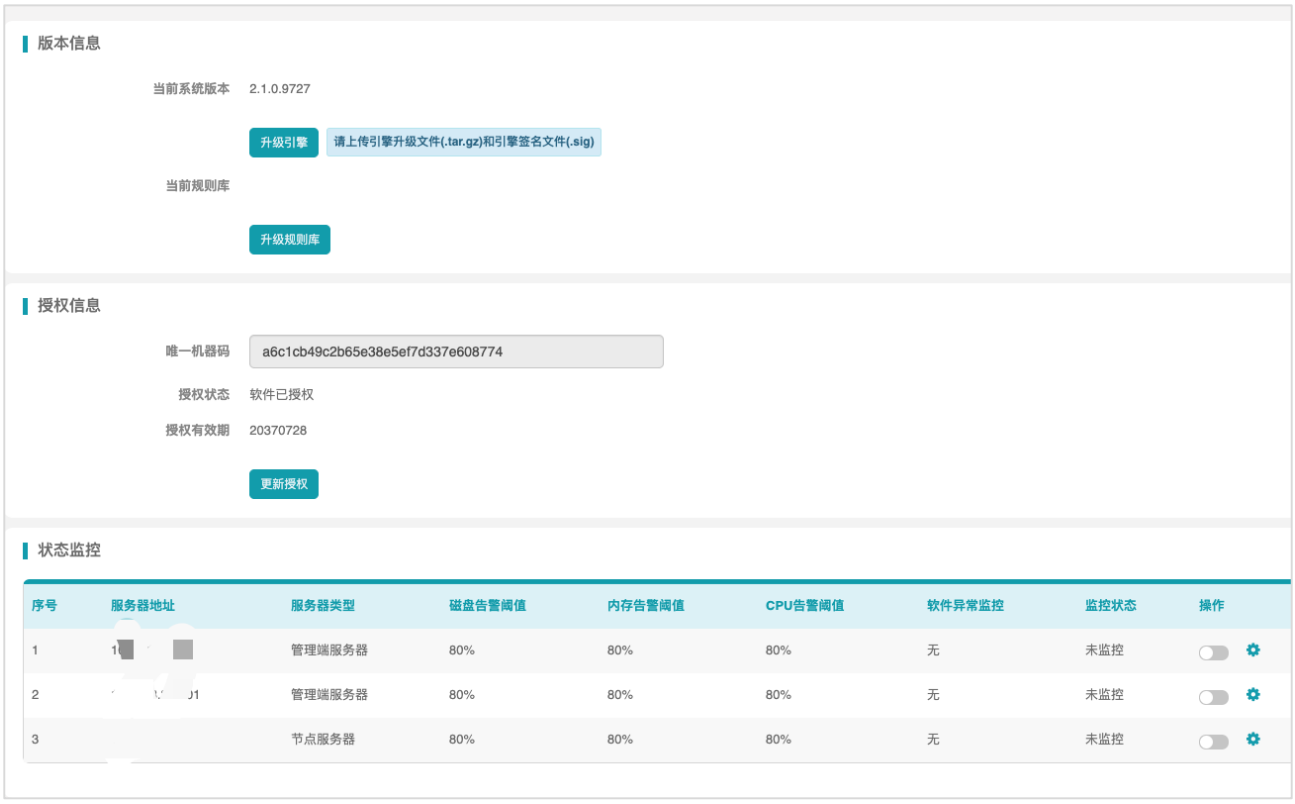


图 4-97 系统信息