通付盾®
Pay Egis

通付盾动态 WAF 使用手册

V3.2.11.12

仅相关人员观看

目 录

系统概况

统计分析

以图表或列表方式展现摘要信息，可了解当前系统最重要的一些运行参数、运行状态和授权信息。

安全监控

用于安全事件的监控，可选择性的选取事件特征进行查询。

配置中心

通过添加站点并对站点对象制定相对应的防护引擎等方式对相应站点进行防护。

系统管理

可对日志信息集中采集以及动态 WAF 运行状态等的监测。

用户指南

通付盾动态 WAF 系统为新一代业务应用安全防护产品，搭载通付盾动态防护引擎、爬虫防护引擎和智能决策引擎，整合站点加固、动态验证、人机识别、风险过滤、自动化攻击拦截等技术对所有访问的流量进行安全检测、过滤和智能阻断。

术语解释

事件

每一笔经过防火墙的访问请求，叫做“事件”，包含访问的信息，如 IP、referer、User-Agent 等；

安全类型

动态 WAF 可监测出的攻击或进行的防护，安全类型分为正常流量、SQL 注入攻击防护、HTTP Flood 攻击防护、Web 应用扫描防护、XSS 攻击、CSRF 防护、命令注入防护等。

站点

站点就是我们平时所做的网站 Web 服务（Web Service）是基于 XML 和 HTTP、HTTPS 的一种服务。

引擎

引擎为攻击防护和动态加固的核心，包括爬虫防护引擎、智能决策引擎及动态防护引擎，需防护的站点可选择使用所需防护的引擎。

API 接口

API（Application Programming Interface，应用程序接口）是一些预先定义的接口或指软件系统不同组成部分衔接的约定。

用户权限管理

动态 WAF 设备的用户使用三权分立的原则对设备进行管理和配置，所谓“三权分立”是指的将用户管理，配置管理和审计管理三种不同的操作分派给三种管理员用户员分别为：用户管理员、配置管理员和审计管理员来进行，实现管理员用户之间的各司其职。

1、用户管理员是系统固有的一个用户，默认用户名为“**admin**”，不可更改，初始密码“**tfd123456**”，用户管理员可以通过工具栏上的“修改密码”功能或者在用户管理界面，修改自身密码。

用户管理员登录后，可见用户管理界面，可以添加、删除、修改、锁定配置管理员、设置密码连续错误上限的次数导致系统自动锁定和账户锁定时间，设定用户密码强度。用户管理员不能对审计管理员进行编辑、修改密码、锁定等操作。

2、审计管理员是系统固有的一个用户，默认用户名为“**audit**”，不可更改，初始密码“**tfd123456**”，审计管理员可以通过工具栏上的“修改密码”功能，修改自身密码。

审计员登录后，可见审计日志界面，审计日志中记录了所有用户进入系统后的各种操作日志，审计员可以查询、删除、导入、导出这些操作日志。

3、配置管理员是系统固有的一个用户，默认用户名为“**useradmin**”，不可更改，初始密码“**tfd123456**”，登录后可以通过工具栏上的“修改密码”功能自行修改密码。

配置管理员是执行系统主要业务的角色，系统中的业务除用户管理和审计日志其它的所有业务均由配置管理员完成。

通过在登录页面输入不同的用户名，即可进入不同的管理员页面。

用户管理员

系统中有且唯一的用户管理员。用户管理员可以配置用户的新增、编辑、修改密码、锁定、删除各类操作（审计管理员除外）。

用户管理员“**admin**”是系统中唯一的一个用户管理员，系统中不可以创建其他的用户管理员，也不可以删除用户管理员，唯一可以对用户管理员进行的操作就是修改密码。操作如下：

旧密码：指的是用户当前密码，用于对用户进行验证

新密码：需要修改的新密码并且满足密码强度

再次输入新密码：再次输入新设置的密码

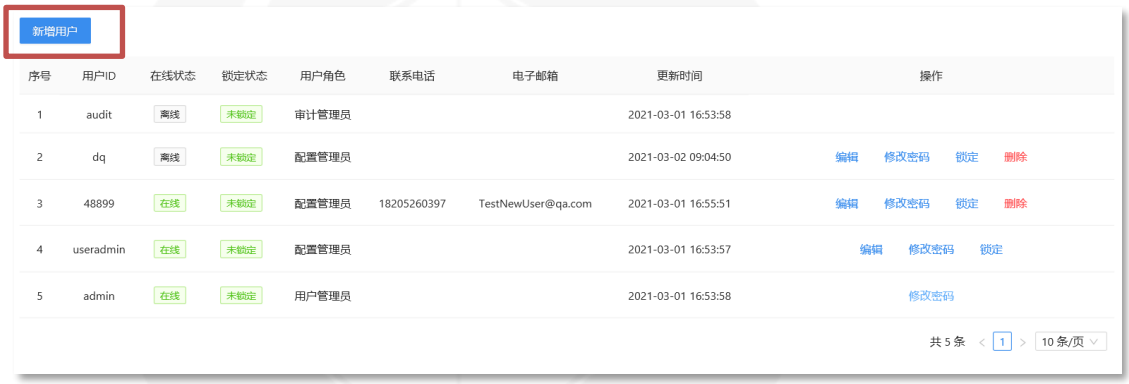
系统中可以有多个配置管理员，每一个配置管理员都有自己相应的配置权限：读写或者只读。配置管理员可以根据自己的权限进行相应的配置管理操作。系统中默认有一个配置管理员“**useradmin**”，具有最高的策略配置权限。

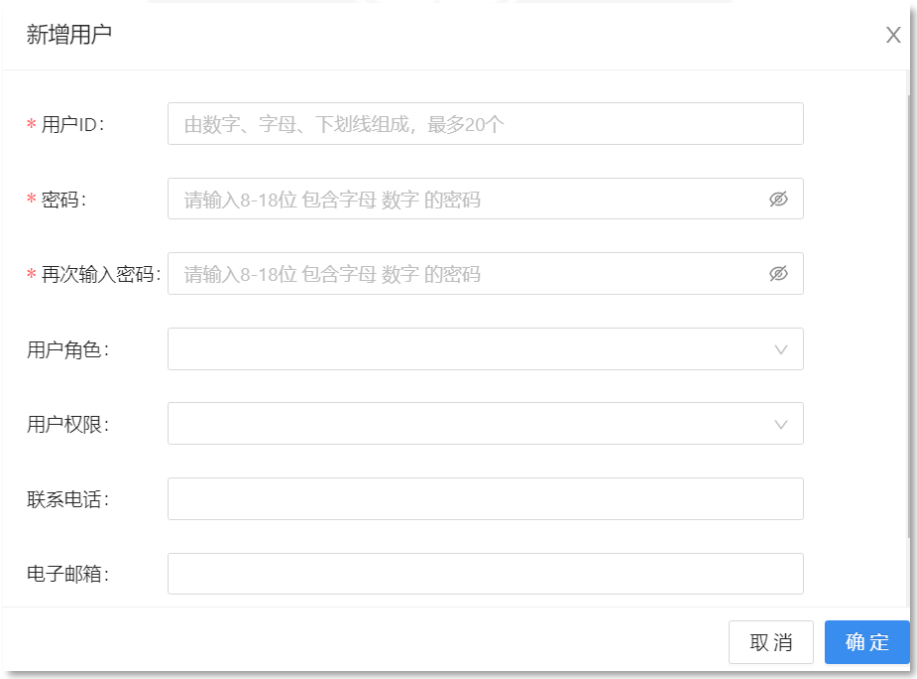
- 新增一个配置管理员用户

  通过新增角色，选择配置管理员的菜单权限，可选择统计分析、安全监控、配置中心和系统管理四大模块。

点击新增角色，按需开启角色权限，完成后点击确定按钮。

使用用户管理员登录，进入用户管理页面，点击“新增用户”按钮





用户 ID：配置管理员的 ID，用户 ID 只能包含数字，英文字符或下划线，长度范围 20 字符

密码：用户对应的密码，密码规则参照设备密码强度配置信息

再次输入密码：再次输入与上个输入框内相同的密码

用户角色：选择配置管理员以及已经完成创建的角色

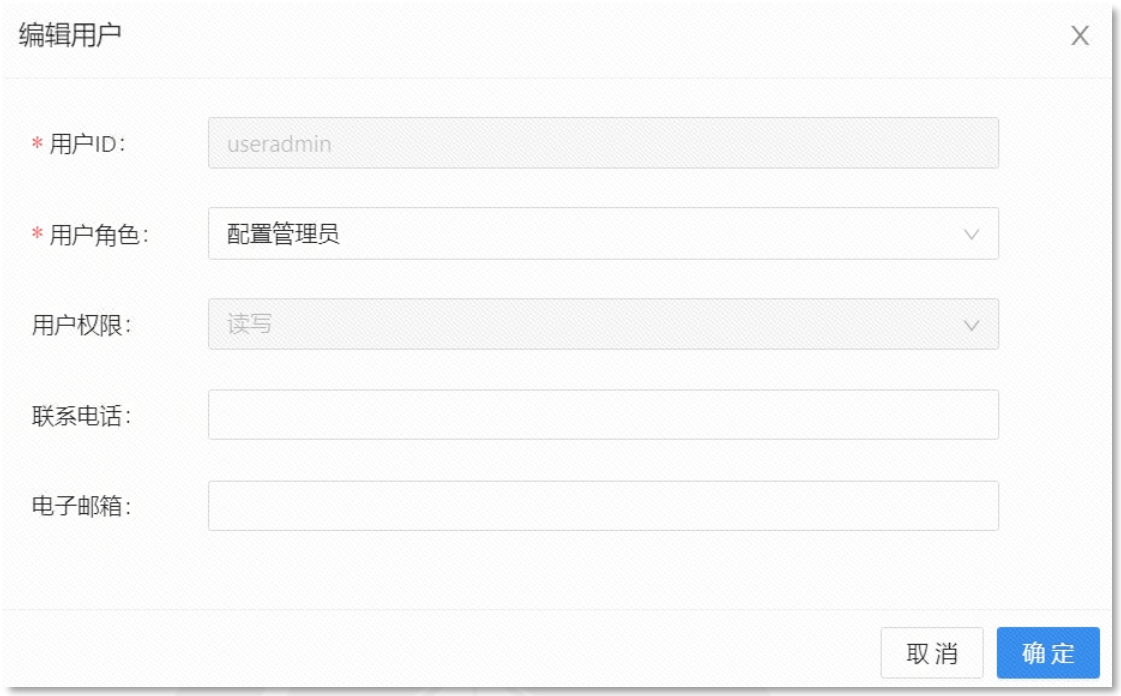
角色权限：配置管理员权限分为两种：只读和读写，默认选择读写

联系电话：填写管理员的联系电话

电子邮箱：填写管理员的电子邮箱地址

- 编辑配置管理员用户

用户管理员可以修改已经存在的配置管理员的可选配置信息。单击配置管理员后面的“编辑”弹出编辑用户对话框：



修改对应的项，只能修改用户角色、联系电话、电子邮箱三项信息，其余信息一旦创建了用户就不能再修改。然后点击“确定”按钮。

- 修改配置管理员密码

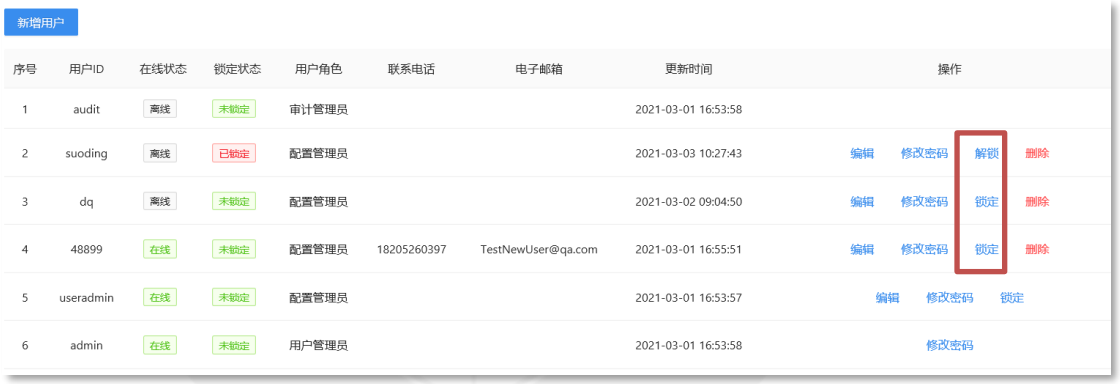
单击已新增的管理员、内置配置管理员以及用户管理员的“修改密码”弹出修改密码对话框：

新密码：需要修改的新密码，密码规则参考设备密码强度配置信息

再次输入新密码：再次输入与上个输入框内相同的密码

- 锁定配置管理员用户

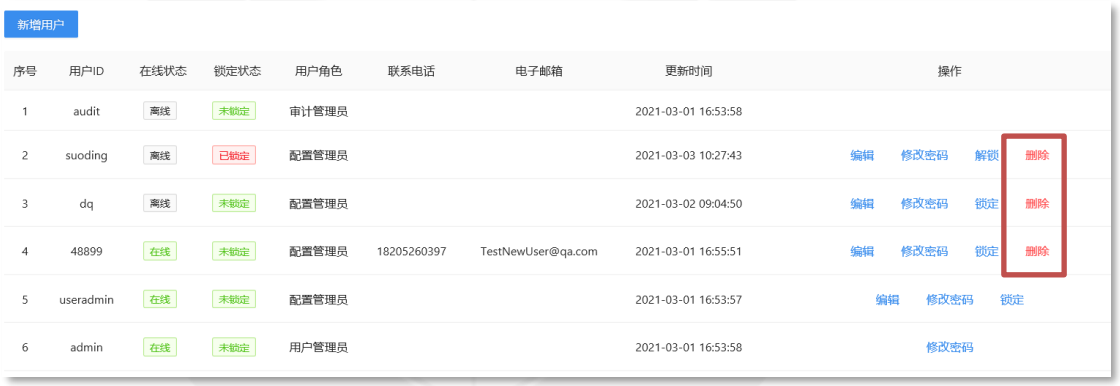
  用户管理员可以锁定已经存在的配置管理员用户。



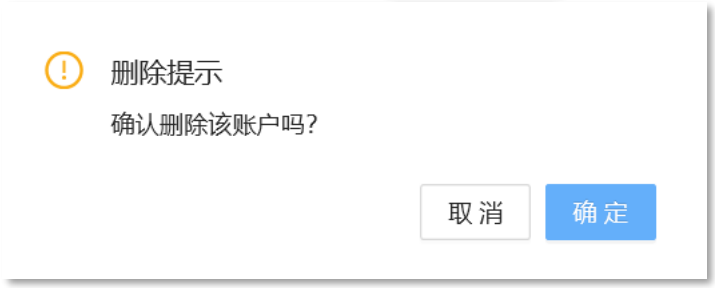
单击“锁定”弹出确认对话框：

单击确定锁定用户，锁定后用户无法登录页面，弹出以下界面。

- 用户管理员可删除非内置的管理员(配置管理员和审计管理员除外)



单击“删除”弹出确认对话框：

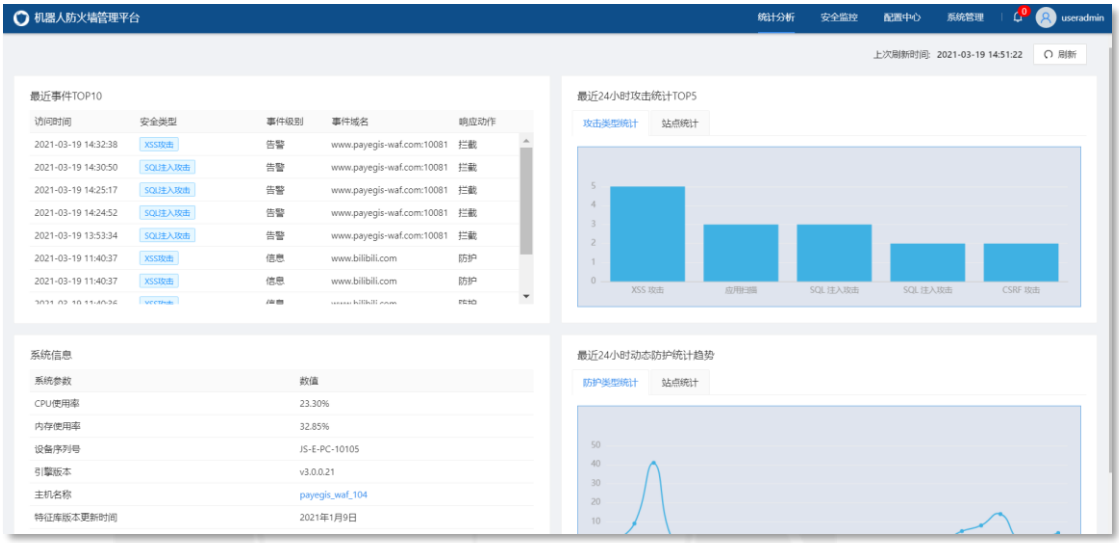


配置管理员

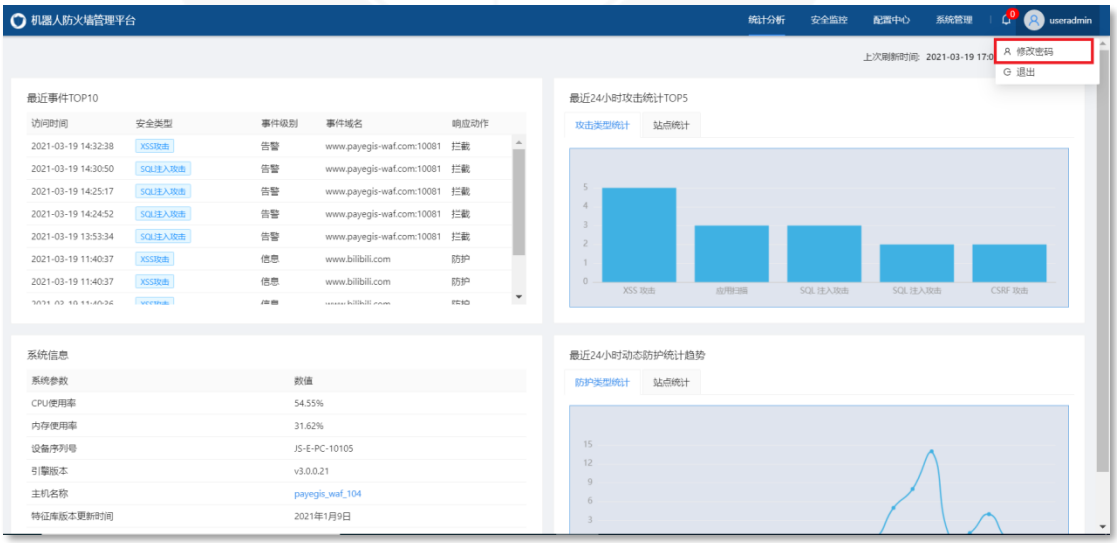
系统中可以有多个配置管理员，每一个配置管理员都有自己的配

置权限：读写或者只读。配置管理员可以根据自己的权限进行相应的配置管理操作。

系统中默认有一个配置管理员“**useradmin**”使用配置管理员登录设备将进入配置管理首页：

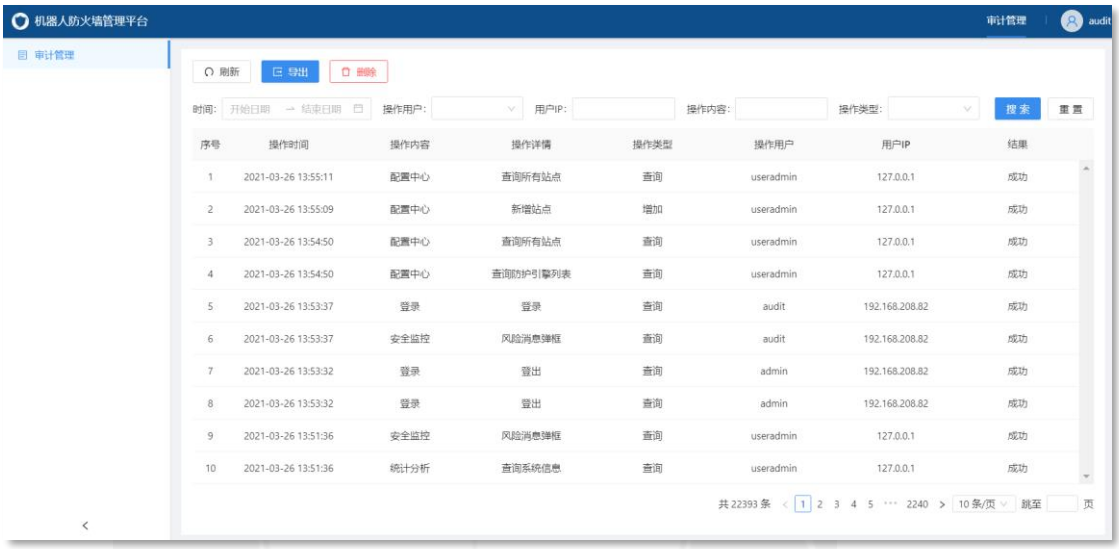


配置管理员可以通过工具栏上的“修改密码”功能，修改自身密码。

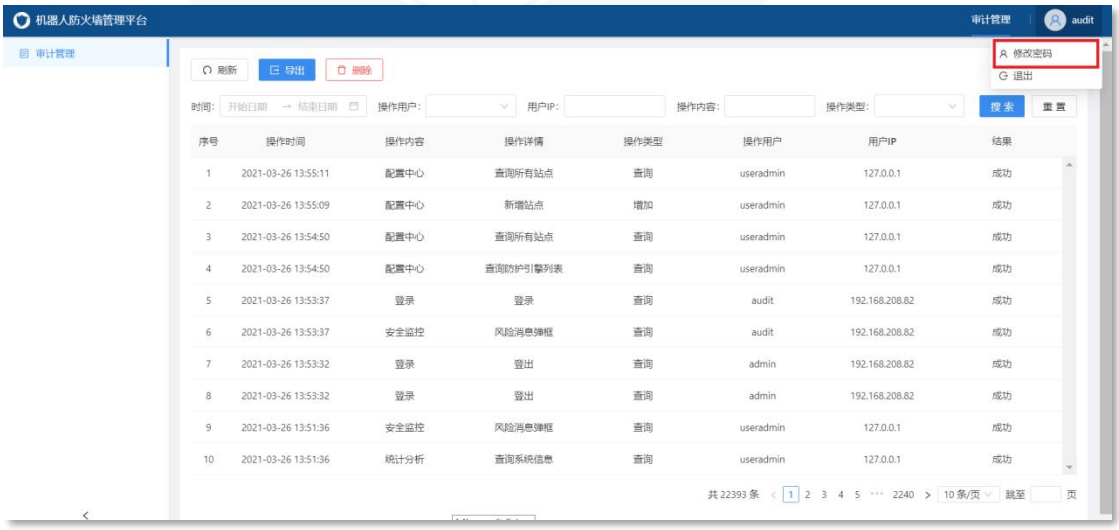


审计管理员

审计日志是记录用户操作的一种方法。审计日志中，记录了用户执行操作的时间、用户名、操作内容、用户 IP 和操作执行的结果等信息，使用审计员登录设备将进入审计管理首页，如下图：



审计管理员是系统固有的一个用户，默认用户名为 “**audit**”，审计员可以通过工具栏上的“修改密码”功能，修改自身密码。



强制修改密码

为保证用户登录系统的安全性，默认管理员（用户管理员、配置管理员、审计管理员）使用默认密码（tfd123456）或用户密码已过期在登录页面输入账密后，自动弹跳至修改密码页面。

当前密码：当前登录的用户的密码

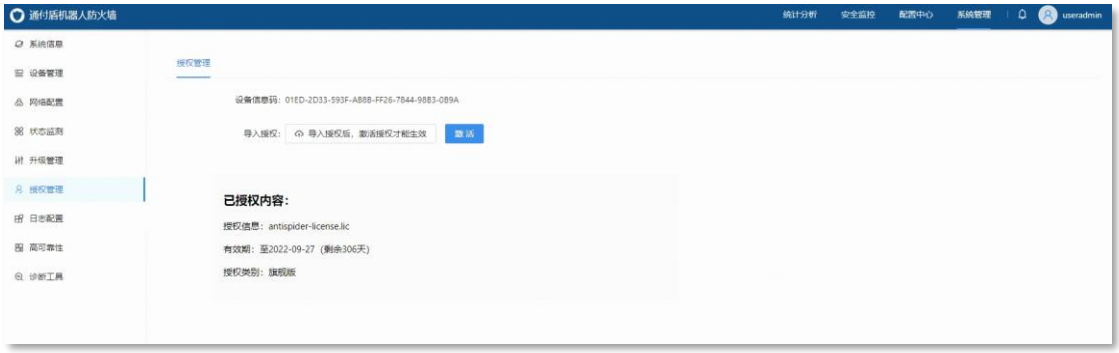
新密码：设置当前登录用户的新密码

确认新密码：再次输入新密码

一、典型配置案例

本章以动态 WAF 部署代理模式为例 ,以向导的方式介绍动态 WAF 基本功能的配置方式，帮助用户快速掌握和方便使用产品。

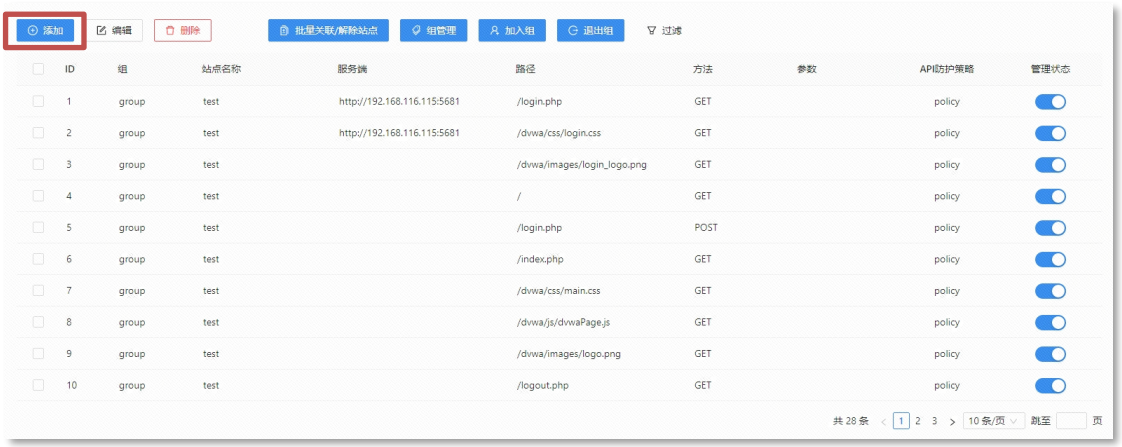
1、通过修改默认配置管理员 “**useradmin**”密码后，登录平台，进行授权导入，按照不同的授权支持不同的功能，具体可参考第四章配置中心→授权管理。



2、添加 Web 应用站点或 API 接口，选择防护模式及防护引擎，具体可参考第四章 配置中心—>4.1 站点防护。

在填写站点防护时，初次填写可在防护策略处选择默认防护策略或提前配置防护策略。

在填写 API 接口防护时，无需配置防护策略，需要 API 防护→API 资产管理进行详细配置，具体可参考第四章



3、完成配置后可以通过安全监控模块对系统进行全方位的监控，记录防护情况，具体可参考第三章 安全监控→安全事件监控。

二、统计分析

统计分析模块是系统摘要信息的集中汇总，以图表、列表、柱状图、折线图等方式展现。目的是让用户通过该页便可了解当前系统最重要的一些运行参数、运行状态和授权信息，该页展现摘要信息，功能的配置具体由相应的模块来完成。

由于系统是采用三权分立的原则来进行用户管理，不同的用户具有不同权限。统计分析模块只有“配置管理员”以及具有权限的角色可以访问。在“配置管理员”登录后，系统便会自动进入统计分析页面。

点击页面右上角的刷新，可选“1分钟”、“2分钟”、“5分钟”定时可对整体页面数据进行刷新，拉取最新数据，也可下拉“手动刷新”刷新页面数据（默认5分钟刷新页面数据）。

2.1 最近事件 TOP10

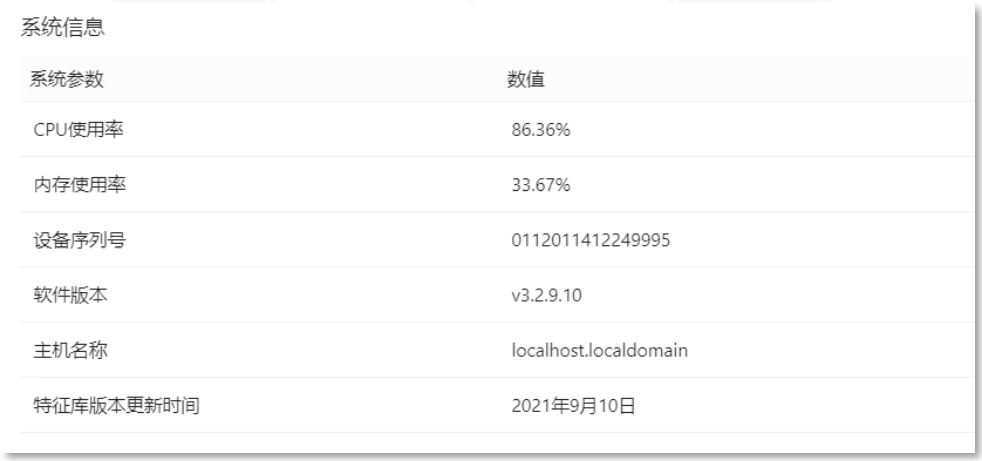
最近事件 TOP10 是指 Web 站点防护最近发生的安全事件，显示字段包括访问时间、安全类型、事件级别、事件域名、响应动作。


最近事件TOP10

访问时间	安全类型	事件级别	事件域名	响应动作
2021-03-02 09:39:08	Cookie注入防护	告警	payegis-dvwa_1.com:8989	防护
2021-03-02 09:37:35	CSRF防护	告警	payegis-dvwa_1.com:8989	防护
2021-03-02 09:37:34	CSRF防护	告警	payegis-dvwa_1.com:8989	防护
2021-03-02 09:37:33	CSRF防护	告警	payegis-dvwa_1.com:8989	防护

2.2 系统信息

系统信息显示系统当前的一些实时资源信息。(CPU 使用率、内存使用率、设备序列号、软件版本、主机名称、特征库版本更新时间、运行时间)。


系统信息

系统参数	数值
CPU使用率	86.36%
内存使用率	33.67%
设备序列号	0112011412249995
软件版本	v3.2.9.10
主机名称	localhost.localdomain
特征库版本更新时间	2021年9月10日

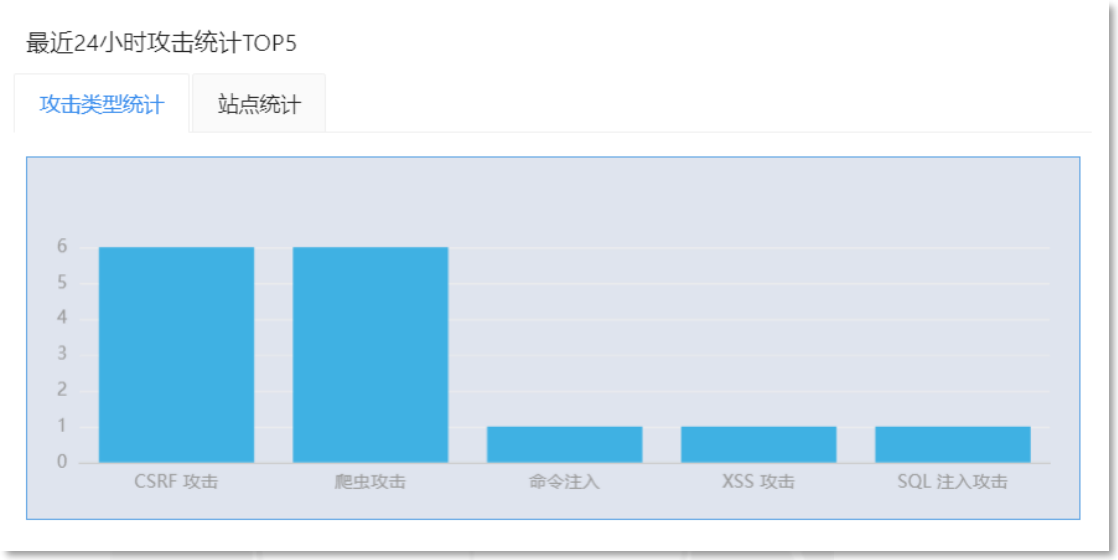
2.3 最近 24 小时攻击统计 TOP5

最近 24 小时攻击统计 TOP5 是指对当前时间点之前的 24 个小时内发生的存在攻击的事件按条件进行统计 ,统计条件包括攻击类型

统计以及站点统计。

- 攻击类型

以“攻击类型”为统计维度，统计访问事件中含有该攻击的事件个数，展示最近 24 小时的 TOP5 的攻击类别的柱状图。



- 站点统计

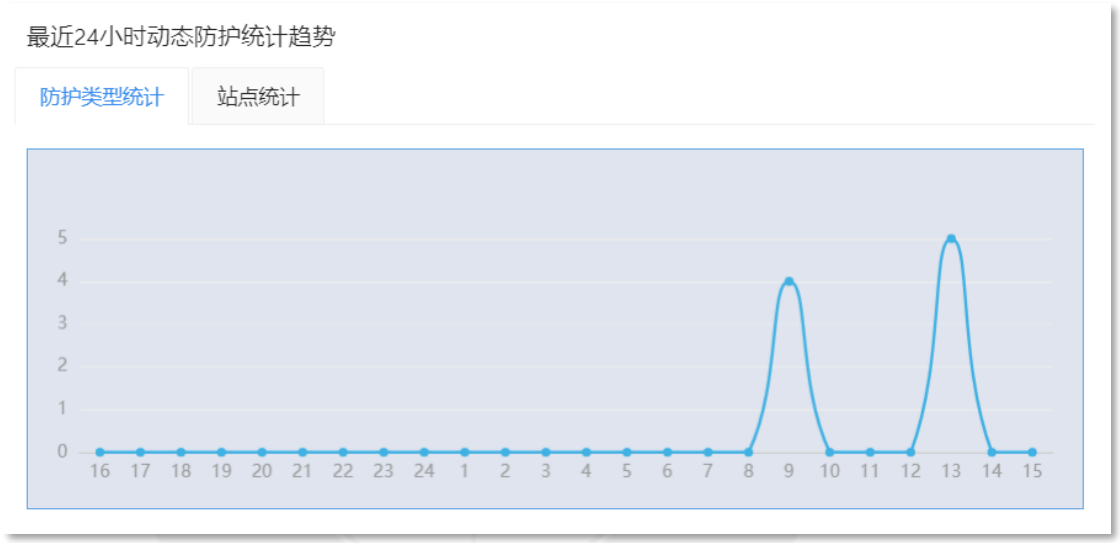
以“站点”为统计维度，统计该站点受到攻击的事件个数，并展示最近 24 小时的 TOP5 站点的柱状图。

2.4 最近 24 小时动态防护统计趋势

最近 24 小时动态防护统计趋势是指对当前时间点之前的 24 个小时内发生的存在防护的事件按条件进行统计，统计条件包括防护类型统计以及站点的统计。

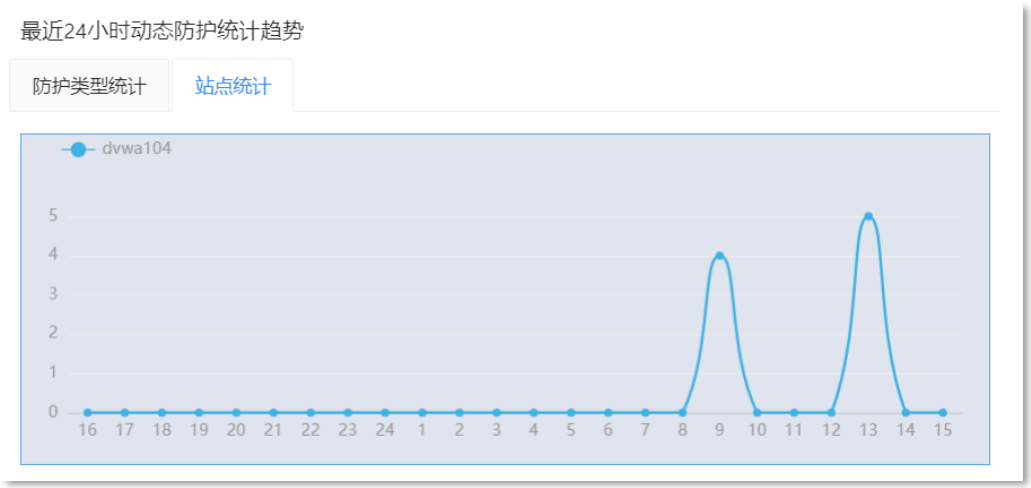
- 防护类型统计

以“时间”为统计维度，展示最近 24 小时的事件个数折线图。



- 站点统计

以“时间”为统计维度，展示最近 24 小时的选中站点的动态防护统计折线图。



三、安全监控

3.1 安全事件监控

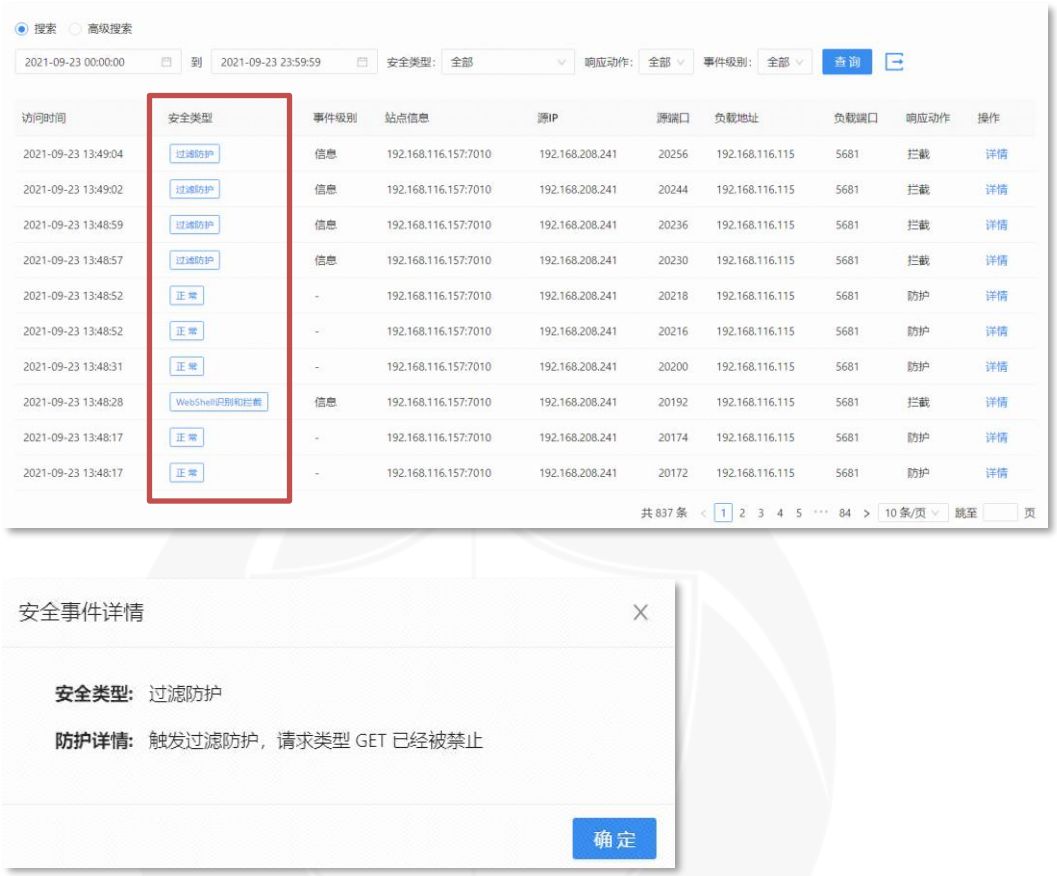
安全事件监控是指在 Web 页面查看所有的安全事件信息，以此来监测用户网络是否发生非法或恶意访问。

安全事件监控模块分为两种监控类型：安全事件详情、安全事件统计。

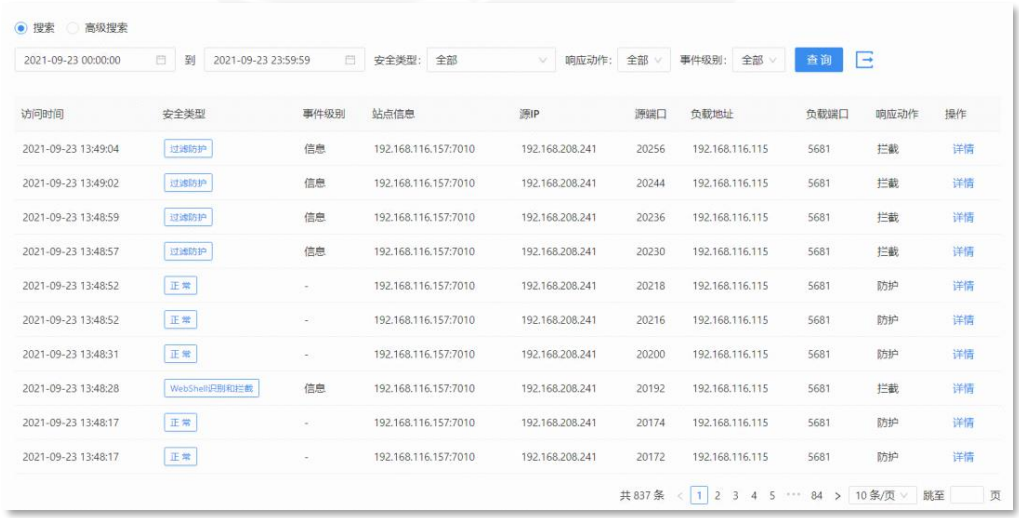
3.1.1 安全事件详情

安全事件详情页面主要通过列表的方式来显示安全事件的信息，通过选择不同的查询条件(时间、安全类型、事件级别、响应动作等) 来显示所关心的安全事件。页面列表中显示的是安全事件的防护信息，默认全部事件展示。列表包含访问时间、安全类型、事件级别、站点信息、源 IP、源端口、负载地址、负载端口、响应动作、操作展示详情信息。

通过点击安全类型下拉框，展示所有安全类型事件，点击某笔访问的安全类型展示该笔安全类型的具体详情。



通过点击“详情”展示该笔安全事件的具体详情信息。



详情包含访问时间，格式为“年-月-日 时-分-秒”、站点信息、安全类型、访问的 URL、源 IP+源端口、负载地址+负载端口、事件级别、响应动作、浏览器信息（即 UA）、引用页（即 Referer）。可将该笔访问快速添加入地址黑名单或者地址白名单中，如点击“添加地址黑名单”按钮，弹出编辑黑名单界面，源 IP 地址和目的 IP 地址/域名及目的端口自动填充，只需填写名称和事件级别，如下图：

点击“添加地址白名单”按钮，弹出如下“编辑白名单页面”：

3.1.1.1 搜索

按照搜索条件 1、时间段，开始时间、结束时间；2、安全类型，

选择全部或者某一项；3、响应动作，选择全部、防护或拦截；4 事件级别，选择全部、告警或信息。

点击“查询”按钮查询出想要的信息。

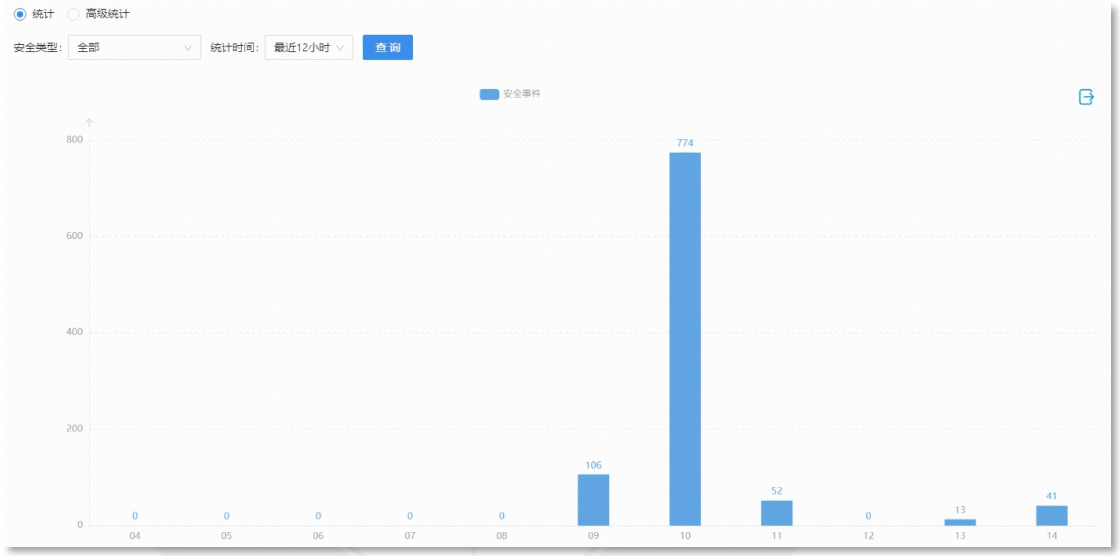
3.1.1.2 高级搜索

高级搜索的搜索条件除搜索的 4 个条件 ,另外新增 1、源 IP ;2、负载地址；3、站点信息，以上共七个搜索条件点击“查询”按钮查询想要的信息。

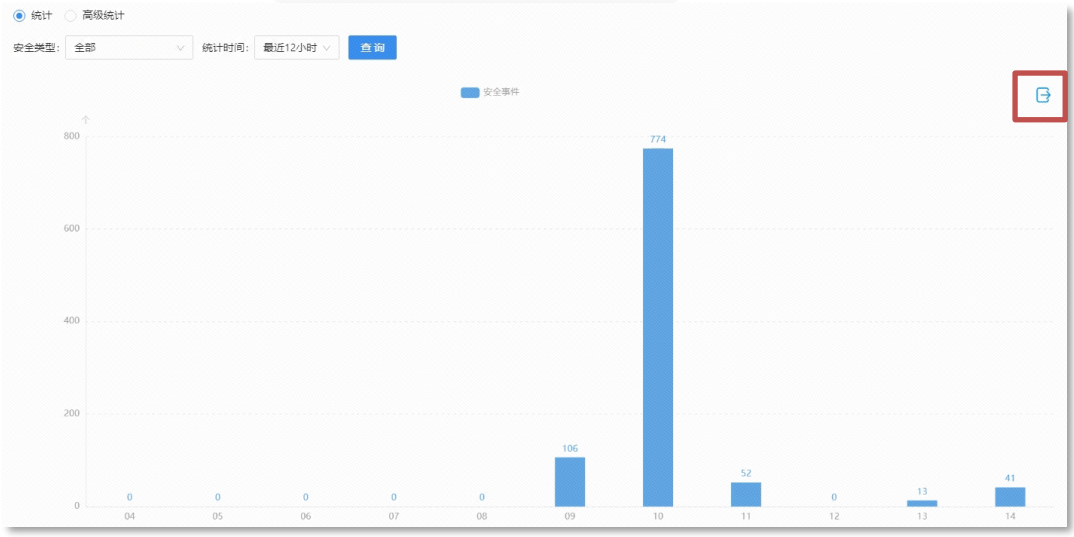
“搜索” “高级搜索”可按“导出”按钮导出当前条件下的所有安全事件信息，导出至 Excel 表格中保存到本地。

3.1.2 安全事件统计

安全事件统计页面主要是根据服务器进行安全事件类别的统计，统计时间可选“最近 12 小时”、“最近 24 小时”、“最近 7 天”的全部站点的某种安全类型或者全部安全类型的事件数量柱状图。横坐标为整的时间点，纵坐标为事件数量。通过该页面可了解所有站点在统计时间内受到的攻击情况。



可将当前查询情况，通过“导出”按钮导出。



3.2 临时阻断

当管理员发现有可疑流量时，可通过临时阻断设置在设定时间内精确阻断该流量。可看到阻断的站点安全事件信息，包括：访问时间、源 IP、站点地址、端口、剩余阻断时间（分钟）、操作。

3.2.1 临时阻断详情

触发临时阻断条件后产生的阻断详情界面详情展示

单击解除按钮后

解除后，该条信息在详情列表中删除，且去除针对该流量的阻断。

3.2.2 临时阻断设置

临时阻断，是对于在一定检测周期内，超过配置的检测拦截次数的源 IP 进行阻断处理，产生临时阻断列表，参考下图：

开关：启用按钮，启用攻击 IP 智能阻断模块（默认关闭）

检测周期：检测拦截次数的时间周期，1-120，单位：分钟

检测丢弃次数：某一源 IP 在检测周期内的丢弃次数，范围是 10-300 次

阻断时间：超过检测丢弃次数产生阻断的时间，1-120，单位：分钟

3.3 报表

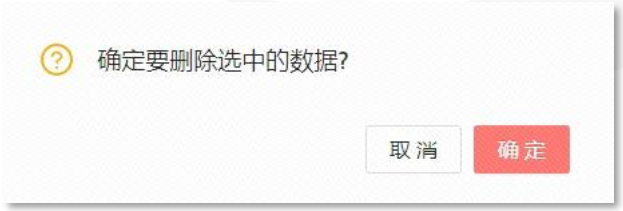
动态 WAF 支持报表功能。该功能通过对设备运行状态、站点风险详情、攻击类型详情的相关数据的统计和综合分析，为用户提供全方位、多角度的统计报告，从而帮助用户掌握站点防护情况，分析问题。统计报表结果即报表文件支持 doc、html、pdf 格式。

3.3.1 报表汇总

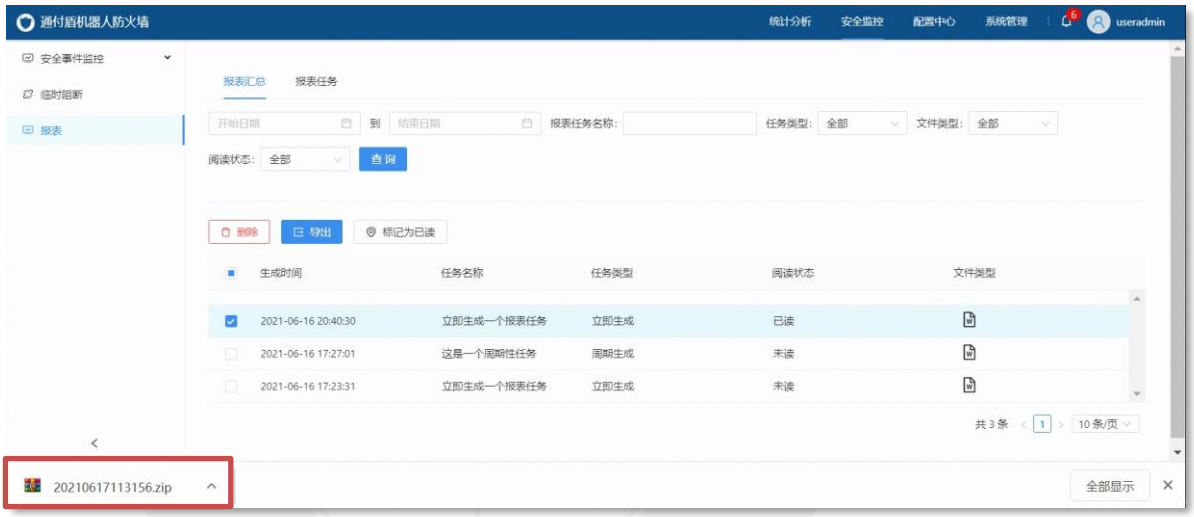
报表汇总通过列表的方式来展示已执行报表内容，并且通过选择不同查询条件（如时间、报表任务名称、任务类型、阅读类型、文件

类型）查询出所需的报表。

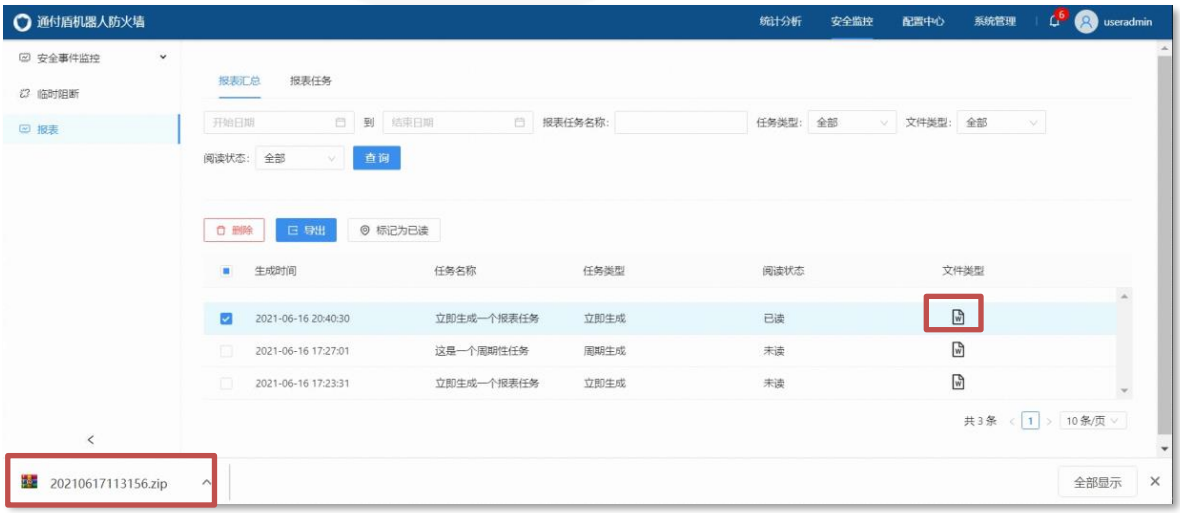
通过勾选所需删除的报表，点击“删除”按钮，如下图：



通过勾选所需导出的报表，点击“导出”按钮，导出报表为“.zip”文件，如下图：



也可通过点击该条报表的“文件格式”列中标志的图标，同样可以导出报表。



3.3.2 报表任务

报表任务通过列表的方式来展示报表待执行任务。选中所需报表点击“启用”或者“禁用”按钮，将选中报表启用或禁用,被禁用的报表任务不再执行任务。

通过勾选所需删除的报表任务，点击“删除”按钮，如下图：

通过“+添加”按钮添加报表任务，可定义报表输出的内容，包括基本信息、站点选择、报表项选择、生成时间、输出的文件格式等参数。如下图：

报表任务名称：报表名称，由汉字、数字、字母组成，最多 128 个字符

描述：描述本次报表内容

在左侧勾选所需产生报表的站点，可同时选中多个站点，点击“添加”按钮，添加至“已添加站点”框内；

在右侧勾选已添加站点，可同时选中多个站点，点击“删除”按钮，可删除已添加站点，或点击“全部删除”按钮，可将右侧已添加的站点全部删除。

在左侧勾选所需产生报表的类别，可同时选中多个报表类别，点击“添加”按钮，添加至“已添加站点”框内；

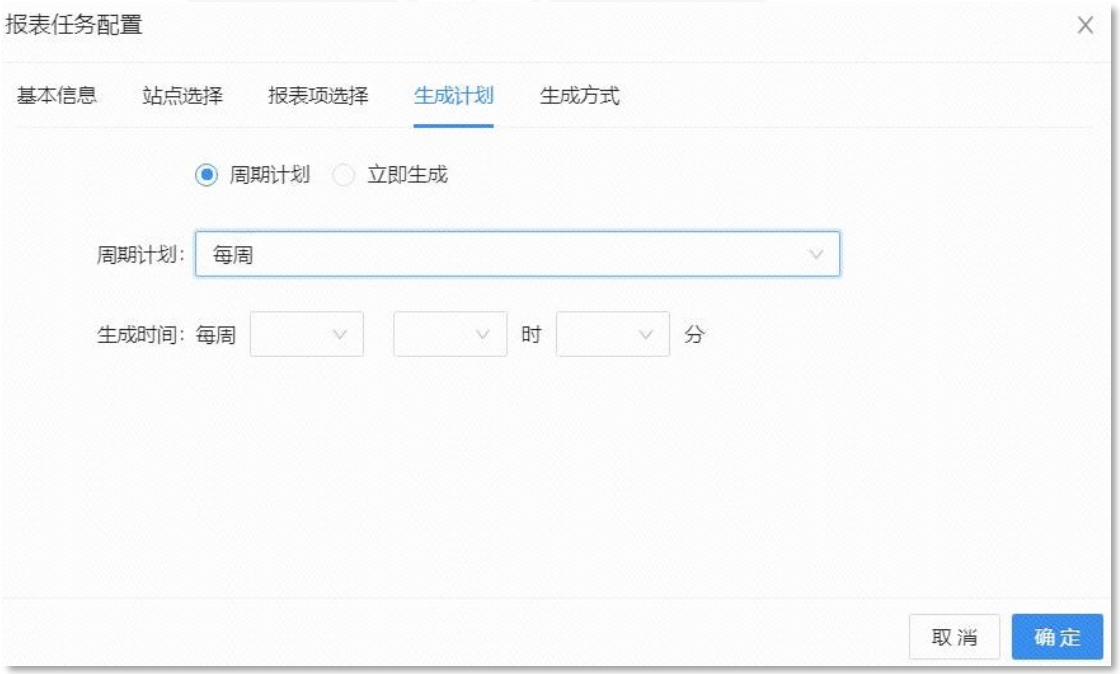
在右侧勾选已添加报表类别，可同时选中多个报表类别，点击“删除”按钮，可删除已添加站点，或点击“全部删除”按钮，可将右侧已添加的报表类别全部删除。

报表生成时间可选周期计划或立即生成两种方式

周期计划：可选每天、每周、每月、每季度、每半年、每年的时间周期，具体时间依据一下的生成时间

每天生成时间可以具体到每天的某时某分，如下图：

每周生成时间可以具体到每周几的某时某分生成，如下图：

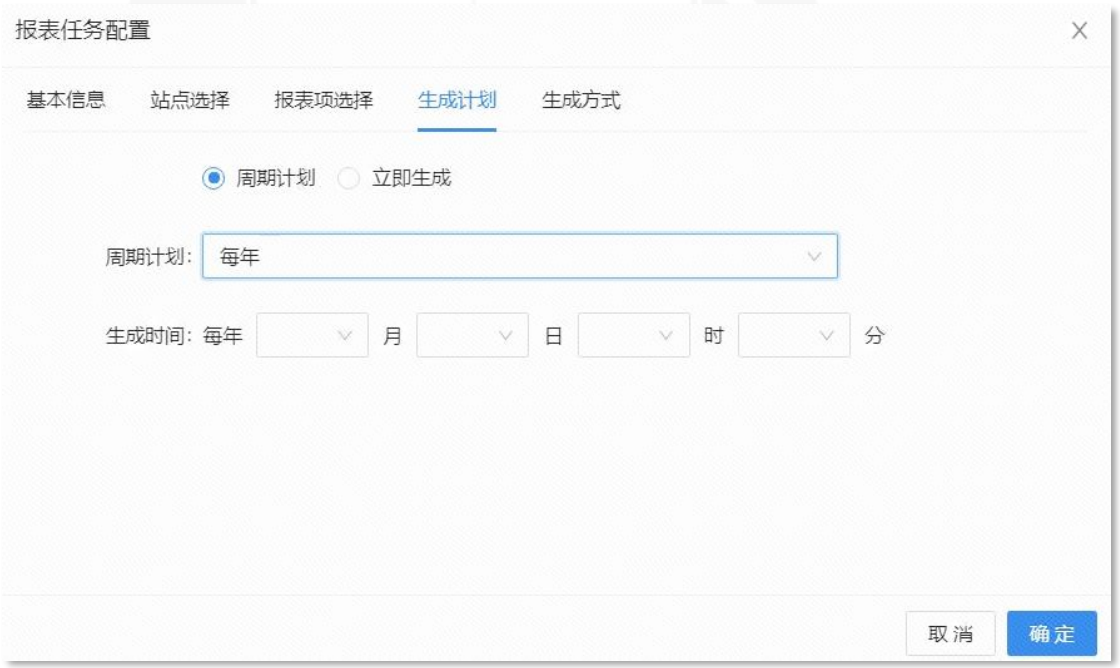


每月生成时间可以具到每月的几日某时某分生成，如下图：

每季度生成时间可以具到每季度的第几个月的几日某时某分生成，如下图：

每半年生成时间可以具到半年的第几个月的几日某时某分生成，如下图：

每年生成时间可以具到几月几日的某时某分生成，如下图：

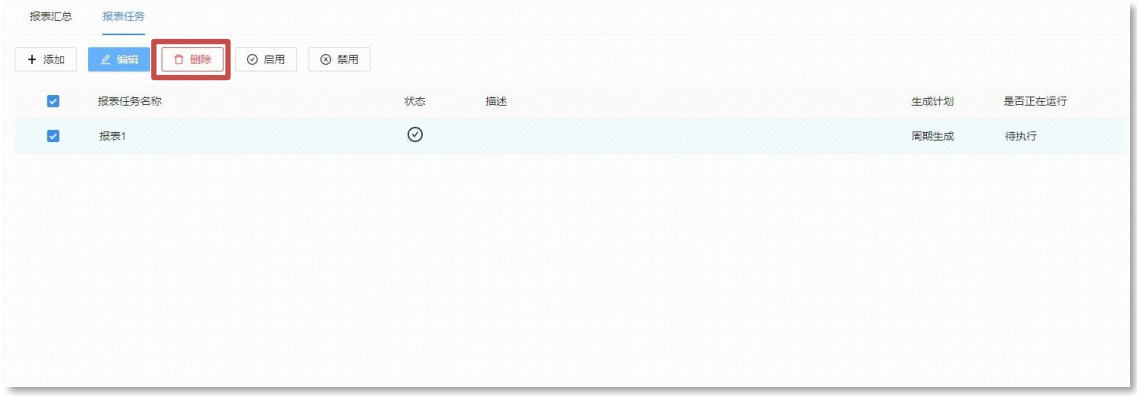


立即生成：该报表立刻产生

选择报表从开始时间收集数据和结束时间完成收集，并制成报表

输出方式：报表产生的生成方式为 word、html 或者 pdf 方式

勾选某一已产生的报表，点击“编辑”按钮，弹出编辑框内容，按需修改，操作如下：



可编辑已创建报表任务的所有配置项目。

四、配置中心

4.1 站点防护

站点防护页面主要通过列表的方式来显示需要防护的站点信息，包含站点的名称、接入类型、协议类型、站点地址、端口、负载地址、负载均衡、防护模式、防护策略。对站点的添加、编辑、删除导入导出操作。

可通过“+添加站点”来新增站点防护，以反向代理接入模式为例。

站点名称：用于防护的站点系统的名字，由汉字、数字、字母组成，最多 20 个字符

接入模式：接入模式可选反向代理或者透明代理

反向代理：用户直接访问反向代理服务器就可以获得被防护服务器的资源。同时，用户不需要知道被防护服务器的地址。

协议类型：可选择 http 协议或者 https 协议（单向/双向），https 需要上传证书文件，其中分为单向和双向，默认使用 crt、key、pem 格式：

- 单向 https 需要上传服务端证书公钥 server.crt、服务端私钥 server.key；
- 双向 https 需要上传上传服务端证书公钥 server.crt、服务端私钥 server.key 以及根证书 root.crt；

若选择 https 协议方式，可勾选“HTTP 强制跳转到 HTTPS”，对用户输入访问的站点自动跳转；

站点地址：匹配动态 WAF 站点的 IP 地址或者域名

端口：配置源站地址防火墙和被防护站点之间的端口

负载地址：即需要防护的站点的地址，可配置多个起负载均衡的作用

防护模式：对该站点进行防护的模式，可选防控模式/监测模式/透传模式/禁止访问四选一

- 防控模式：对站点进行安全检测、记录及动态防护，并对风险访问进行拦截
- 监测模式：对站点进行安全检测、记录及动态防护，但不进行拦截
- 透传模式：对站点不进行拦截、监控和动态防护
- 禁止访问：拦截对站点的所有访问

负载均衡：默认使用 IP HASH 负载方式，可通过下拉框选择轮询负载方式；

防护策略：该站点所使用的某个防护策略。

通过“+添加站点”来新增站点防护，以透明代理接入模式为例。

站点名称：用于防护的站点系统的名字，由汉字、数字、字母组成，最多 20 个字符

接入模式：接入模式可选反向代理模式或者透明代理模式

透明代理：用户直接访问被防护服务器的资源。

网桥选择：网桥下拉可选，具体可参考第五章 系统管理→网络管理→透明桥

协议类型：可选择 http 协议或者 https 协议，https 需要上传证书文件，默认使用 crt、key、pem 格式;https 协议需要上传服务端证书公钥 server.crt、服务端私

钥 server.key

若选择 HTTPS 协议方式，可勾选“HTTP 强制跳转到 HTTPS”，对用户输入访问目的站点自动跳转

防护域名：输入被防护站点的域名地址，通过点击“解析域名”按钮，解析出防护地址，自动填充，也可手动添加

负载地址：即需要防护的站点的地址

防护模式：对该站点进行防护的模式，可选防控模式/监测模式/透传模式/禁止访问四选一

- 防控模式：对站点进行安全检测、记录及动态防护，并对风险访问进行拦截
- 监测模式：对站点进行安全检测、记录及动态防护，但不进行拦截
- 透传模式：对站点不进行拦截、监控和动态防护
- 禁止访问：拦截对站点的所有访问

负载均衡：默认使用 IP HASH 负载方式，可通过下拉框选择轮询负载方式

防护策略：该站点所使用的某个防护策略

动态 WAF 支持健康状态检测，向后端 Web 服务器发出 HTTP 请求和接收响应的方法，检测后端 Web 服务器的健康状态。如果服务器处于健康状态，站点防护的负载地址显示其状态为 up；如果服务器处于失败状态，站点防护的负载地址显示其状态为 down。处于失败状态的服务器将不再分配到 HTTP 请求。

开关：开启健康状态检测，默认关闭

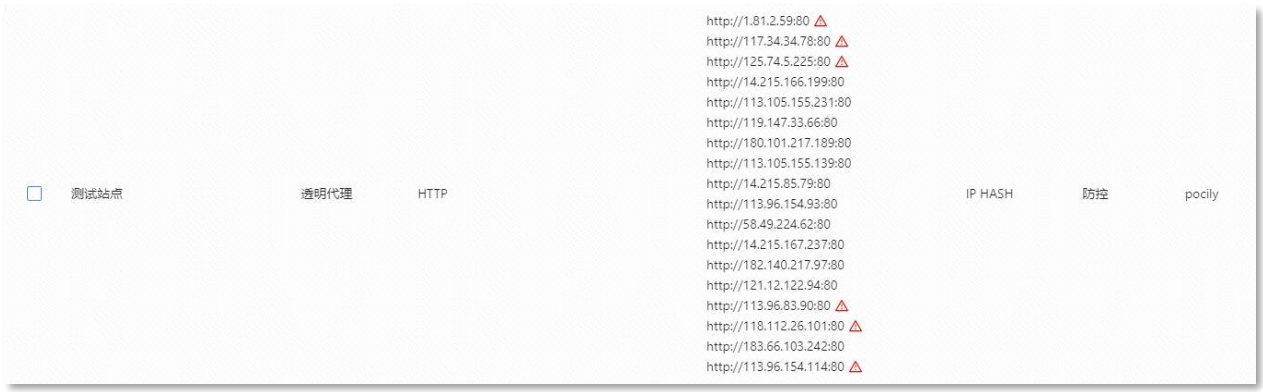
间隔时间 :向后端负载服务器发送请求的间隔时间 默认 10 秒 ,可输入范围 5~300 秒

失败界定次数：向后端负载服务器发送请求失败超过设定次数则认定为失败，默认 3 次，可输入范围 1~30 次

成功界定次数：向后端负载服务器发送请求成功超过设定次数则认定为成功，默认 3 次，可输入范围 1~30 次

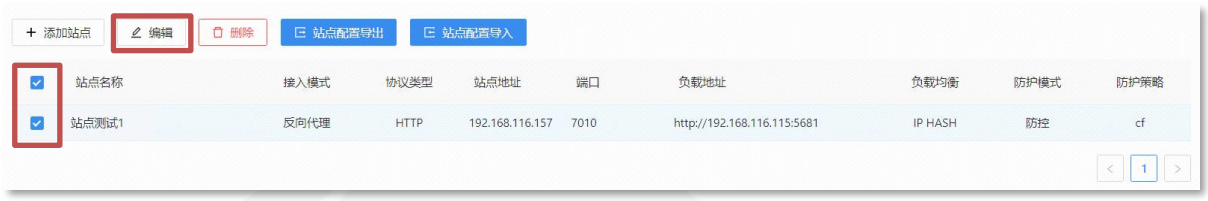
检查页面：向后端负载服务器发送请求界定成功或失败的页面，默认为 “/”

以下站点展示处于成功和失败状态的负载服务器:



防护模式和防护策略可通过下拉框选择所需要使用的模式和策略，不同防护策略对应不同的配置的防护，具体可参考第四章 配置中心—>4.2 防护引擎。

可通过勾选所需站点，点击“编辑”按钮来修改已添加站点的信息。



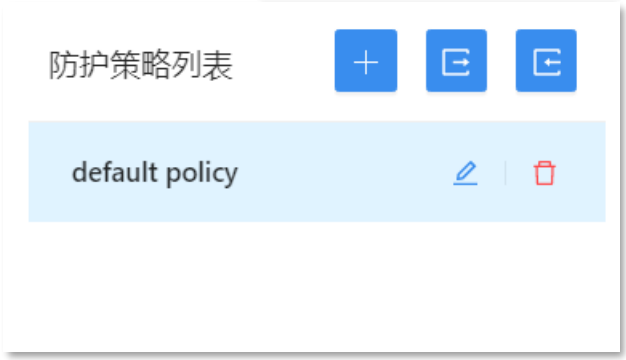
可通过勾选所需站点，点击“删除”按钮来修改已添加站点的信息。注意：删除后的站点不受动态 WAF 防护。

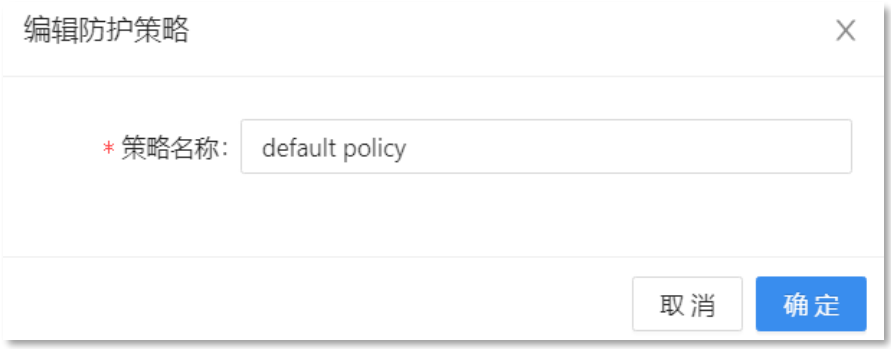
4.2 防护策略

防护策略为整个防火墙系统的核心，在设备中为 web 服务器起到安全保护的关键。防护策略由攻击防护引擎、爬虫防护引擎、动态防护引擎及过滤防护引擎四大引擎组成，来完成对 web 服务器的全方位保护。

防护策略列表左上角“+”按钮，可用作新增防护策略，输入新增的防护策略的名称，名称由汉字、数字、字母组成，长度最多 20 个字符，且唯一不可重复。

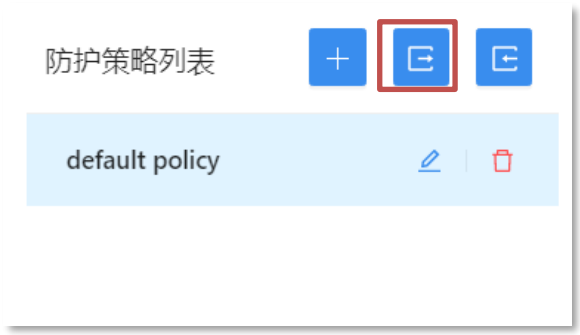
可通过各个防护策略对应的“编辑”按钮来修改策略列表的名称，注意策略名无法重名。



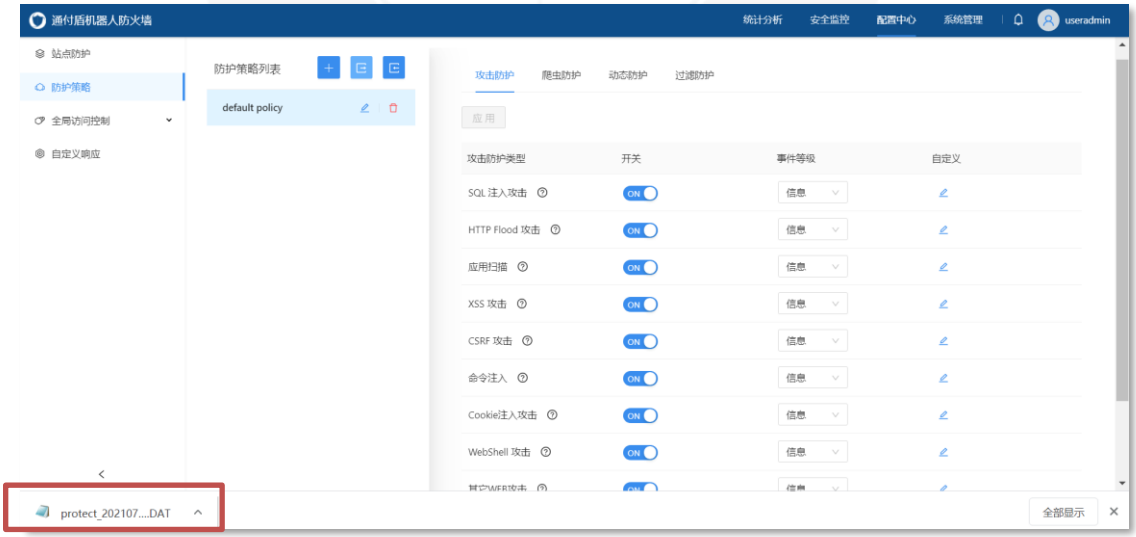


通过“删除”来删除对应的策略，但是被站点已经引用的策略无法删除。

防护策略列表左上角“导出”按钮，将已创建的防护策略导出。

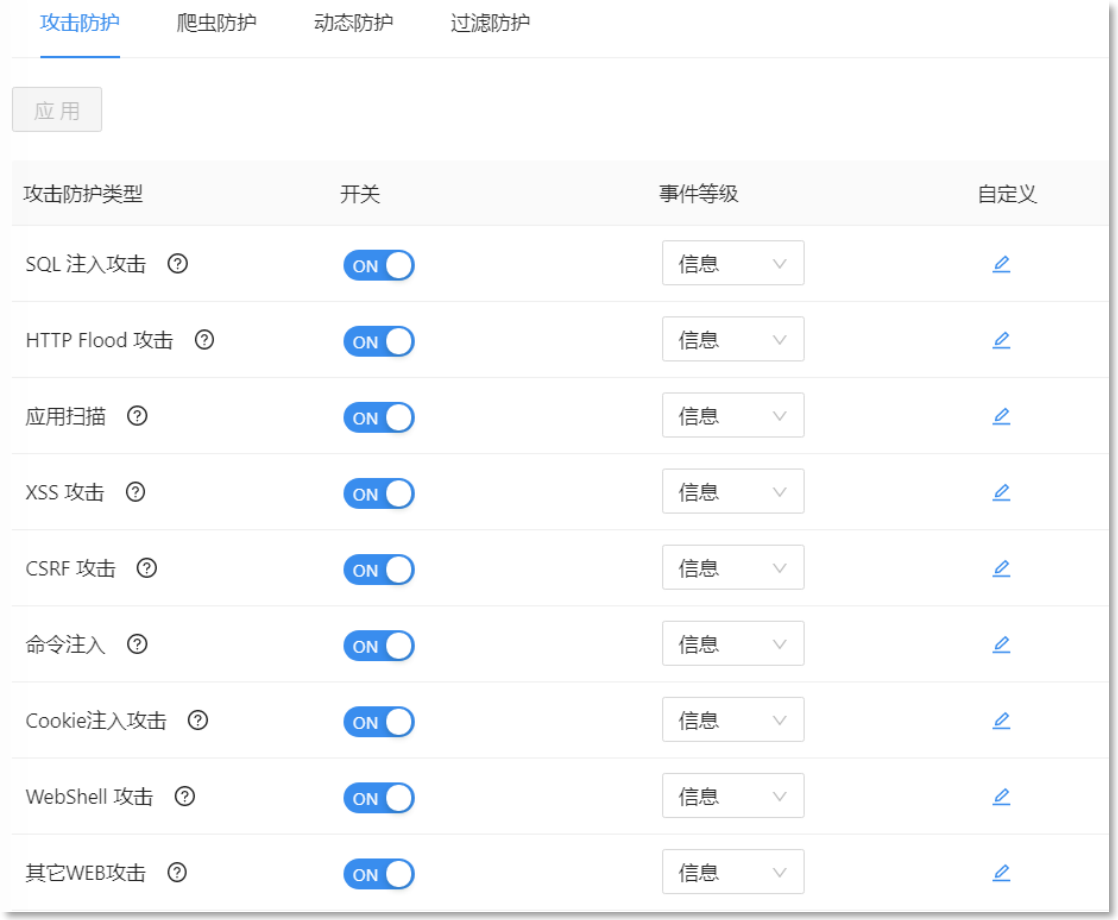

防护策略列表
default policy


选择需要导出的防护策略
所有防护策略
default policy
全选
添加
删除
全部删除
已选择的防护策略
default policy
取消
导出


通付盾机器人防火墙
统计分析
安全监控
配置中心
系统管理
useradmin
站点防护
防护策略
全局访问控制
自定义响应
防护策略列表
default policy
攻击防护
爬虫防护
动态防护
过滤防护
应用
攻击防护类型
开关
事件等级
自定义
SQL 注入攻击
HTTP Flood 攻击
应用扫描
XSS 攻击
CSRF 攻击
命令注入
Cookie注入攻击
WebShell 攻击
protect_202107....DAT
全部显示

4.2.1 攻击防护引擎

攻击防护引擎的内容包含 SQL 注入攻击防护、HTTP Flood 防护、应用扫描防护、XSS 攻击防护、CSRF 防护、命令注入防护、Cookie 注入攻击防护、WebShell 攻击防护、其他攻击防护等防护功能。

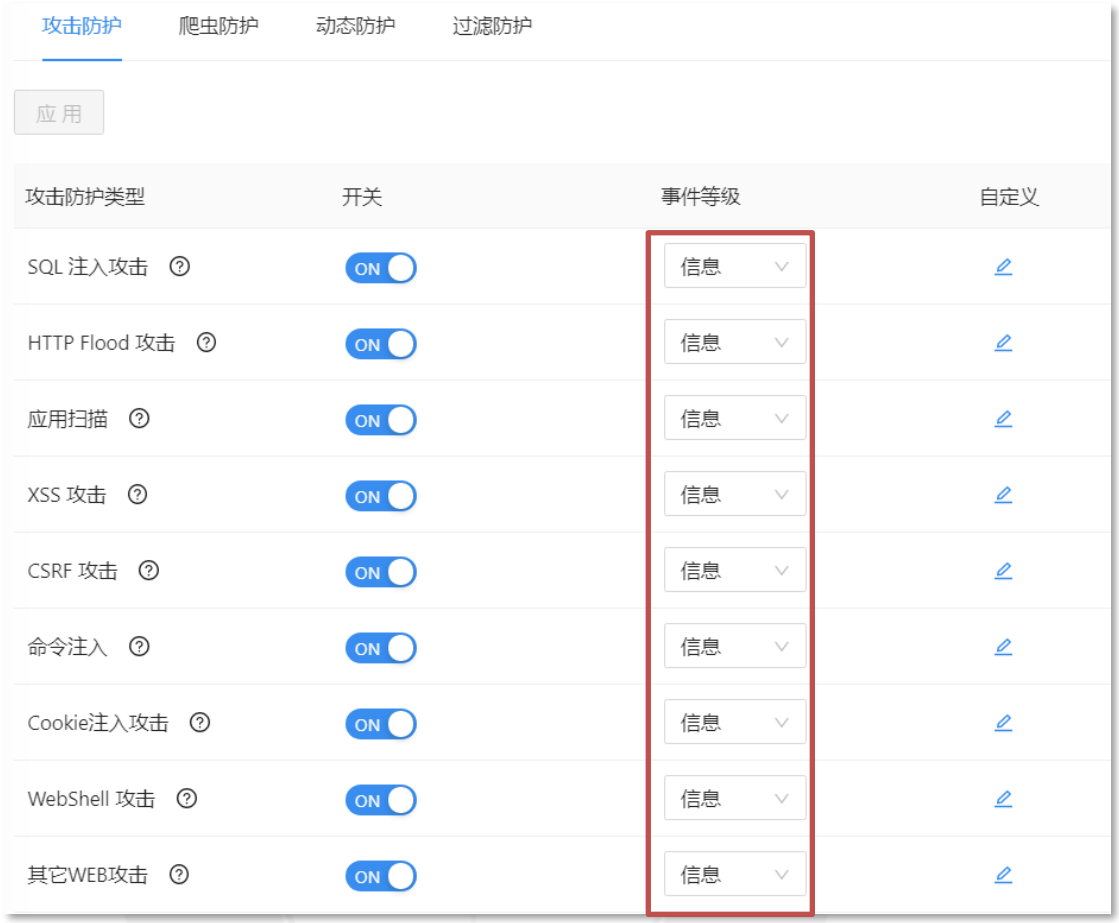


当表格的内容作出了修改后，“应用”按钮高亮可点击，点击后启用最新设置的攻击防护功能，“应用”按钮置灰不可点击，由下次检测内容修改后再高亮可点击。

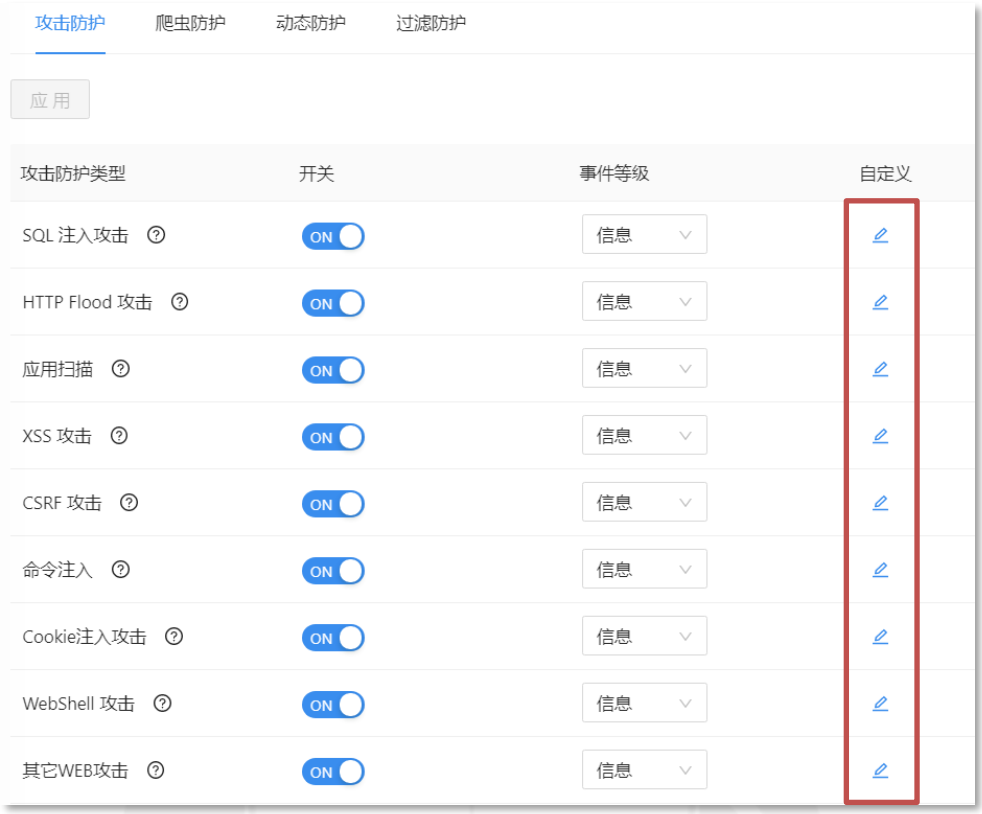
每个攻击防护类型对应的开关为“ON”时，即启用对应攻击防护功能，为“OFF”时，关闭对应攻击防护功能。

引擎中事件等级列可选择每个攻击防护的等级（告警、信息），

最终具体可参考 Syslog 日志中的日志信息。

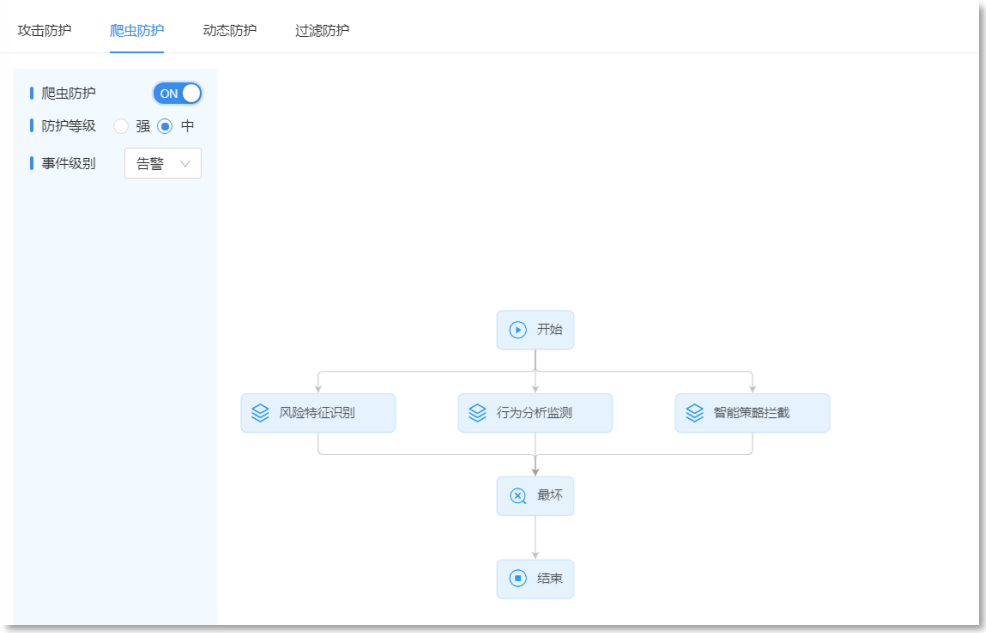


在攻击防护中如需自定义，也可通过自定义下的“编辑”按钮输入自定义信息。



4.2.2 爬虫防护引擎

开启爬虫防护可防止页面信息爬取，保护被防护页面的安全。爬虫防护页面可配置爬虫防护的开关、防护等级。

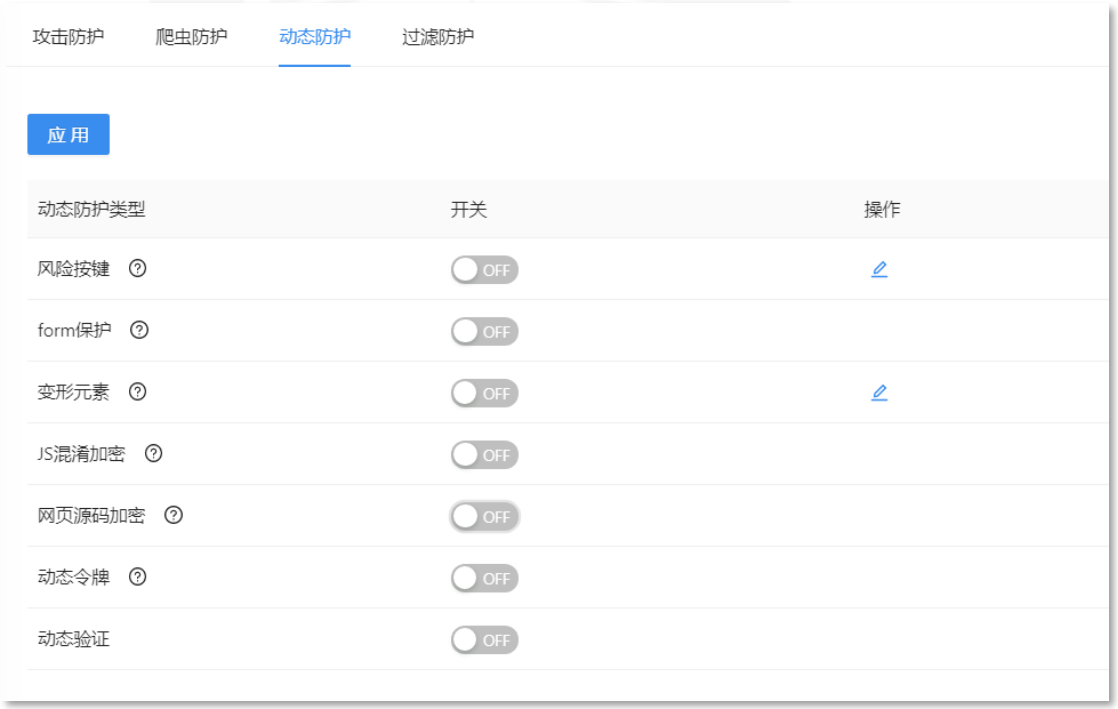


爬虫防护引擎开关为“ON”时，即启用爬虫防护功能，为“OFF”时，关闭爬虫防护功能。

防护等级可单选“强”或者“中”。等级强弱会对应着爬虫防护规则的强弱，每笔访问会经过流计算引擎的规则判断来确定是否为爬虫攻击。

4.2.3 动态防护引擎

动态防护引擎的内容包含风险按键、form 保护、变形元素、JS 混淆加密、网页源码加密、动态令牌等动态防护。



应用按钮是在表格的内容作出了修改后，“应用”按钮高亮可点击，点击后启用最新设置的动态防护功能，“应用”按钮置灰不可点击，由下次检测内容修改后再高亮可点击。

每个防护类型对应的开关为“ON”时，即启用对应防护功能，为

“OFF”时，关闭对应防护功能。

风险按键可通过“编辑”操作编辑各自特定的需求。

选择需要防护的风险按钮，如“防复制”、“防调试”等等。同时也可以自定义输入其他需要特殊防护的按键。

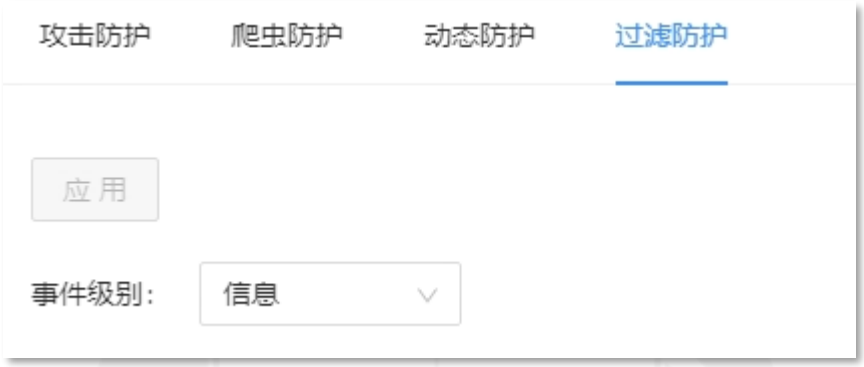
选择网页中易受到攻击的关键元素，如 useradmin、password 类似这样的元素加入到变形元素中，在元素清单输入框内可自定义输入防止被攻击。

若需要特殊设置指定页面作动态防护，或者指定页面不做动态防

护，可至全局访问控制的动态访问控制页面进行配置。

4.2.4 过滤防护引擎

过滤防护引擎主要采用过滤技术对用户的访问根据设置的过滤规则进行过滤操作。可在页面最上方设置过滤防护事件的事件级别。

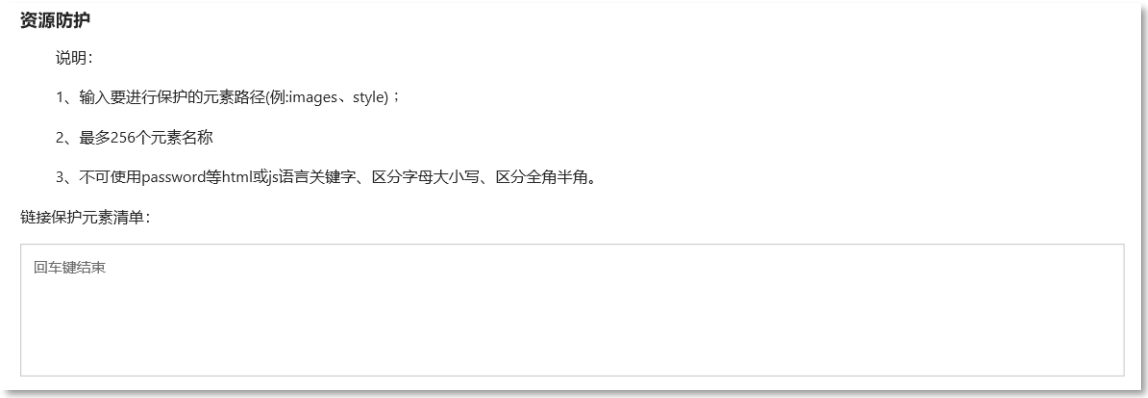


当过滤防护的内容作出了修改后，“应用”按钮高亮可点击，点击后启用最新设置的动态防护功能，“应用”按钮置灰不可点击，由下次检测内容修改后再高亮可点击。

4.2.4.1 资源防护

资源防护可对包含指定元素的路径进行过滤防护，如 images、style，最多支持 256 个元素名称（注意不可使用 password 等 html 或 js 语言关键字、区分字母大小写、区分全角半角）

可通过在下图的输入框中输入需要防护的元素，点击提交至下方的元素清单。



4.2.4.2 请求类型过滤

可根据不同 HTTP 请求的类型进行过滤，类型包含：GET、POST、PUT、HEAD、OPTION。根据过滤规则可控制请求被允许或禁止访问。

通过开关列控制启动或关闭，“开”代表启用该项请求类型的过滤，“关”代表关闭该项请求类型的过滤。

4.2.4.3 协议头长度设置

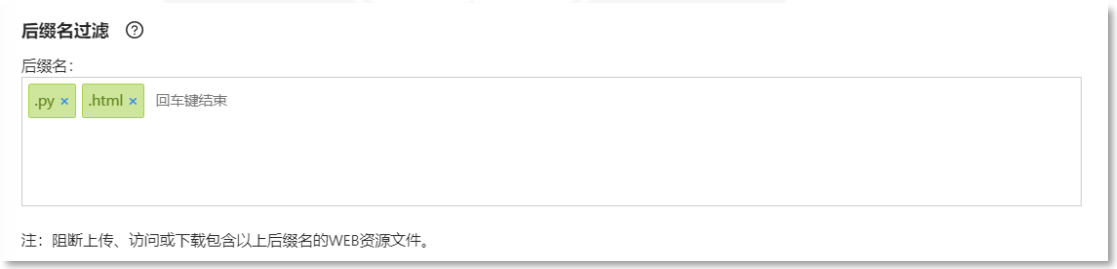
根据不同 HTTP 协议头 ,包括 general-header、request-header、response-header 中的所需要的字段，如 user-agent 设置最大长度

为 20 位，实际访问超出 20 位，并根据配置的规则拦截超出长度的访问。

4.2.4.4 后缀名过滤

通过配置不能够被访问的文件后缀名，如：rar、doc、exe、asp、html 等，当访问携带有配置过滤中的某一个后缀名被配置了的文件时，该访问会被禁止。

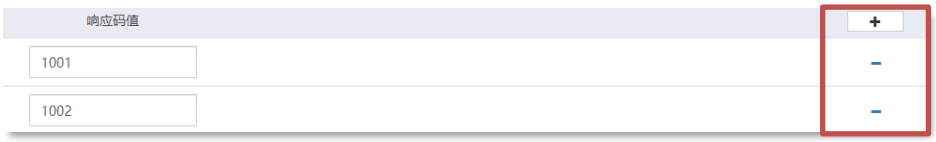
在下图的输入框中输入需要过滤的后缀名，点击最上方“应用”即可。



4.2.4.5 响应码过滤

通过响应码过滤将根据配置的服务器返回的响应码值进行禁止访问，在下图中的右上角点击“+”按钮，可新增一行，在新增的一行的输入框中填写需要过滤的响应码值，点击“-”可删除对应行，

即去除对该响应码的过滤。



4.2.4.6 URL 关键字过滤

对所请求的 URL 中的内容关键字设置过滤条件，对涉及到敏感的关键字信息进行禁止访问。

在下图中的右上角点击“+”按钮，填写对应的需要被禁止访问的关键字内容，点击多次“+”号，可添加多个被禁止访问的关键字。应用后，包含关键字被配置的 URL 会被禁止，点击“-”可删除对应行，即去除关键字信息的过滤。

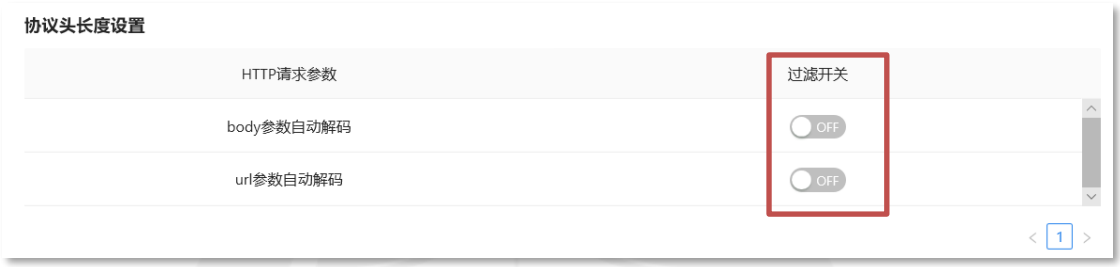
4.2.4.7 返回内容过滤

针对 web 服务器返回的内容设置过滤条件，对涉及到敏感的关键字信息进行禁止返回到页面展示。

在下图中点击右上角的“+”号，填写对应的需要被禁止返回的关键字内容，点击多次“+”号，可添加多个被禁止返回的关键字。应用后，包含关键字被配置的请求返回会被禁止，点击“-”可删除对应行，即去除关键字信息的过滤。

4.2.4.8 请求参数解码

可针对不同编码方式的客户端 HTTP 请求，如 UNICODE、BASE64、二进制、十六进制等，自动转换成 ASCII 明文。



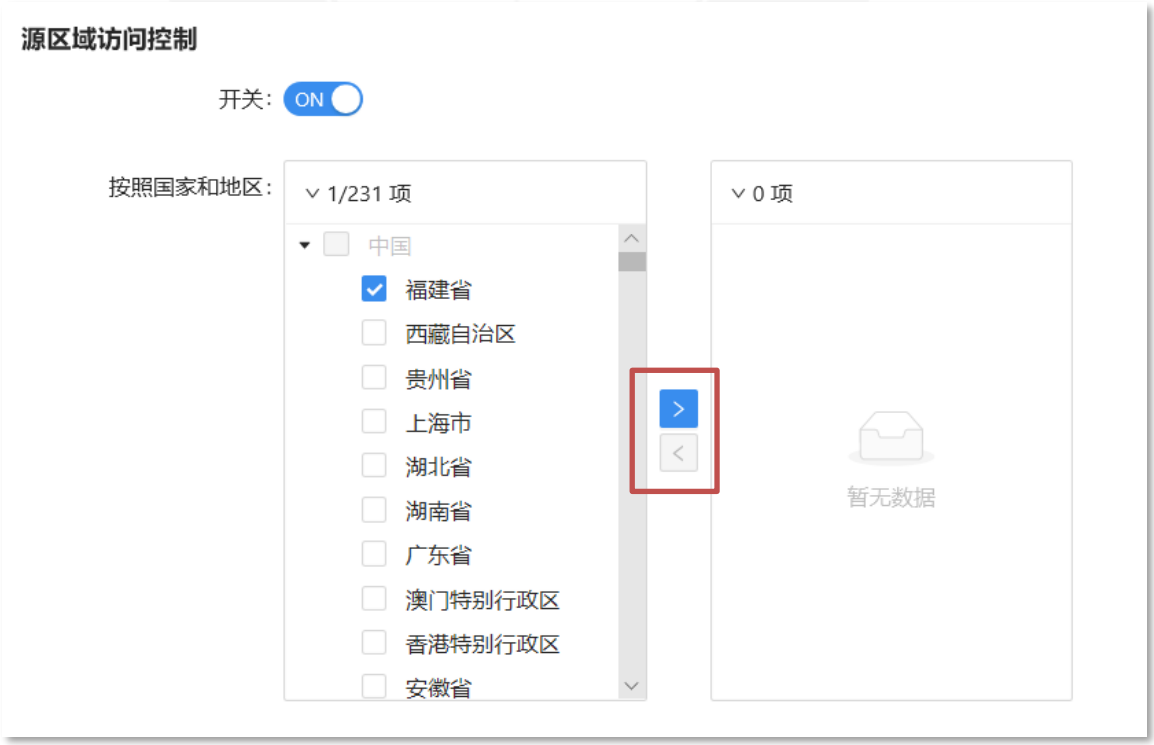
如果用户需要防火墙能够自动识别 HTTP 请求中 URL 参数或者 BODY 参数的编码方式并且能够自动转换成 ASCII 明文，则打开相应的过滤开关；如果客户端和服务端已经约定好编码方式，不需要防火墙自动识别编码方式并且自动转换成 ASCII 明文，则关闭相应的过滤开关。

4.2.4.9 源区域访问控制

对访问用户的 IP 所在的区域进行限制，禁止配置区域的 IP 访问服务器，允许其他访问。

通过开关开启则为开启源区域访问控制功能，默认不启用。

按国家和地区：左侧一栏显示可选中国以外的国家和中国境内省份及自治区，选中某个国家后，通过 → 图标，增加区域；通过 ← 图标，删除区域。



4.3 全局访问控制

引入黑白名单，其在设备中起到全局访问控制的作用。当符合白名单的配置时，将不进行相关检测直接放行；匹配到黑名单配置时，则直接拦截报文。当收到数据报文时，把该报文的方向、源地址、目的地址、协议、端口等信息和用户配置的黑白名单匹配，来确定是否符合黑白名单，从而确定如何处理该流的后续报文。

4.3.1 地址访问控制

地址访问控制为对访问的源 IP 进行控制，拦截或是直接放行其访问服务器的所有地址或指定地址。

4.3.1.1 黑名单

黑名单为配置的直接拦截的 IP 地址，其配置包括名称、源 IP 地址、目的 IP 地址/域名、目的端口、事件级别、名单生效时间、状态设置等。

通过点击“+添加”按钮，添加需要拦截的 IP 地址。

名称：黑名单名称，由汉字、数字、字母组成，最多 20 个字符

源 IP 地址：客户端访问的 IP 地址即需要拦截黑名单 IP 地址

目的 IP 地址/域名：目的 IP 地址或域名，默认 any 即为全部禁止

目的端口：目的端口，默认 any 即为全部禁止

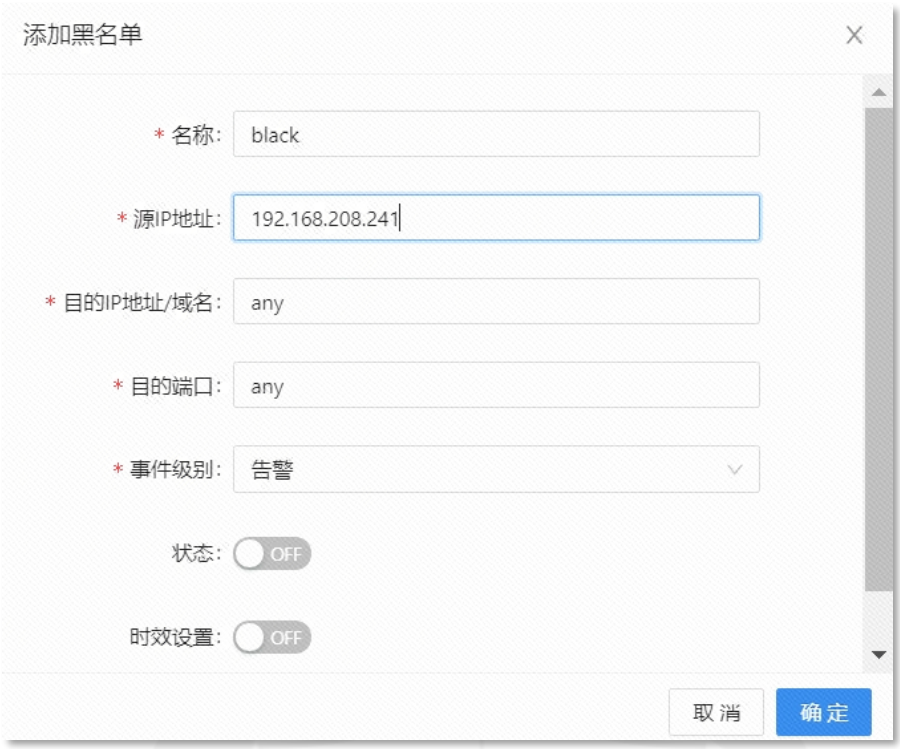
事件级别：可选择“信息”或“告警”两个其中一个级别，默认选择告警级别

状态：开启表示启用，关闭表示不启用

时效设置：启用，不配置则默认永久生效，也可以选择具体生效的日期，具体到日

点击“确定”

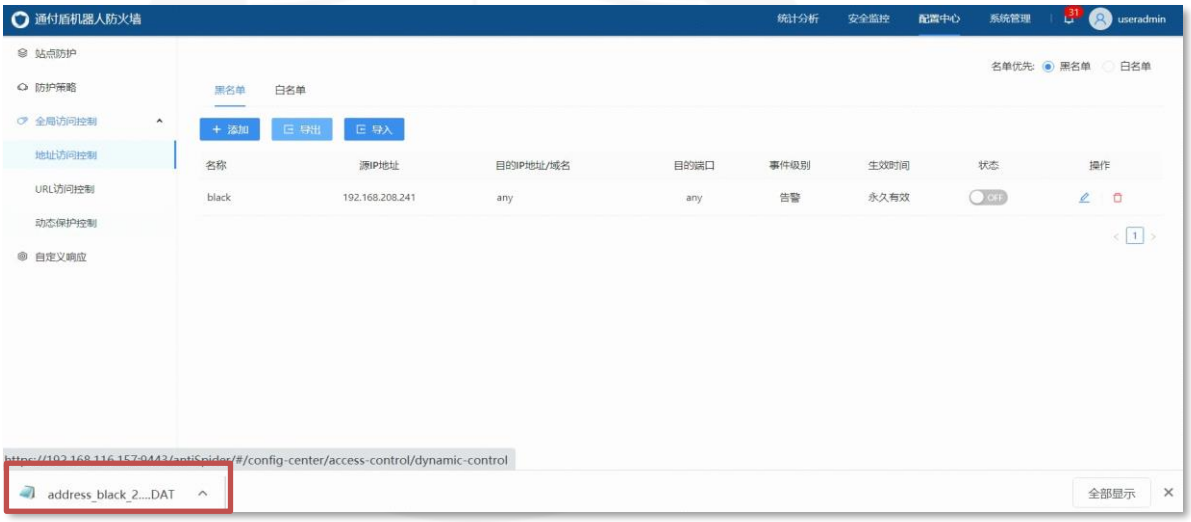
通过点击对应黑名单下的“编辑”操作，对黑名单进行修改。



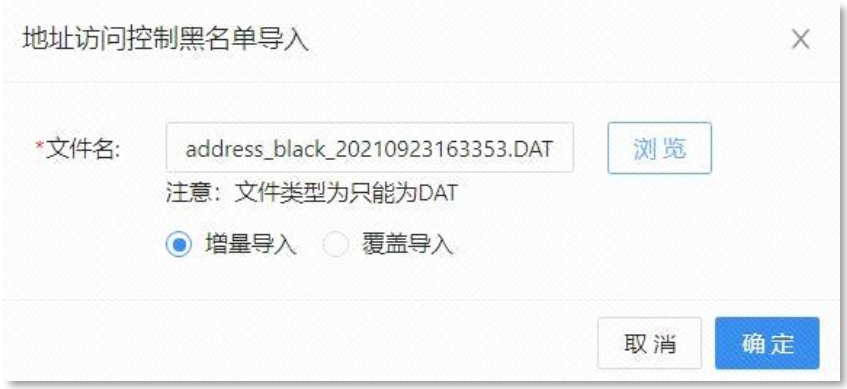
点击对应黑名单下的“按钮”，弹出确认对话框可以删除黑名单，如下图：

通过点击下图对应状态栏下的启用滑框，即可启用。反之关闭时，不启用。

通过点击“黑名单导出”按钮，将配置的黑名单一键导出，生成“.DAT”文件，如下图：



通过点击“导入”按钮，将需要的黑名单上传进行导入，如下图：



增量导入：比对现有黑名单信息和需要导入文档，增加现有平台中没有的黑名单信息。

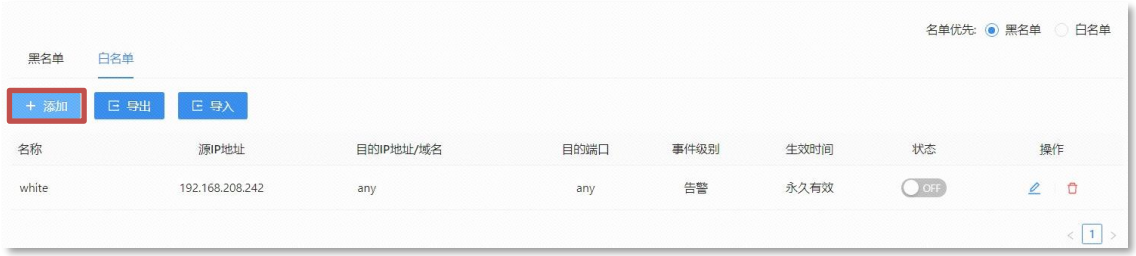
覆盖导入：覆盖现有黑名单信息，导入文档中的黑名单信息。

通过单选按钮选中黑名单优先，则以黑名单优先否则白名单优先选中，以白名单优先。（默认黑名单优先）

4.3.1.2 白名单

白名单为配置的可以直接放过而不做检查的源 IP，其配置包括名称、源 IP 地址、目的 IP 地址/域名、目的端口、事件级别、状态、名单生效时间设置。

通过页面点击“+添加”按钮



名称：白名单名称，由汉字、数字、字母组成，最多 20 个字符

源 IP 地址：客户端访问的 IP 地址，即可直接放过 IP 地址

目的 IP 地址：目的 IP 地址或域名，默认 any 即为全部放过

目的端口：目的端口，默认 any 即为全部放过

事件级别：可选择“信息”或“告警”两个其中一个级别，默认选择告警级别

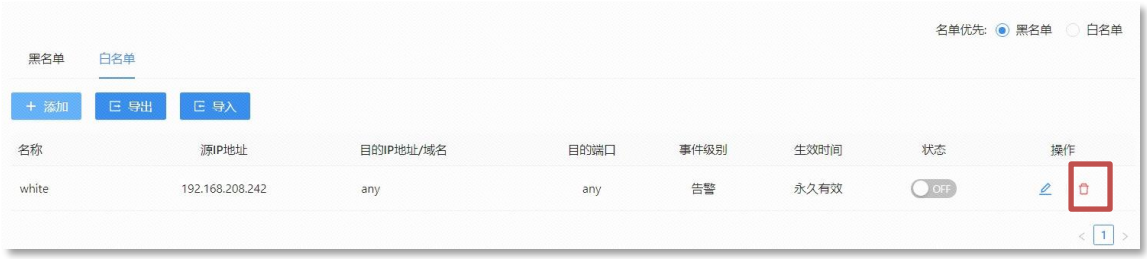
状态：开启表示启用，关闭表示不启用

时效设置：启用，不配置则默认永久生效，也可以选择具体生效的日期，具体到日

点击“确定”

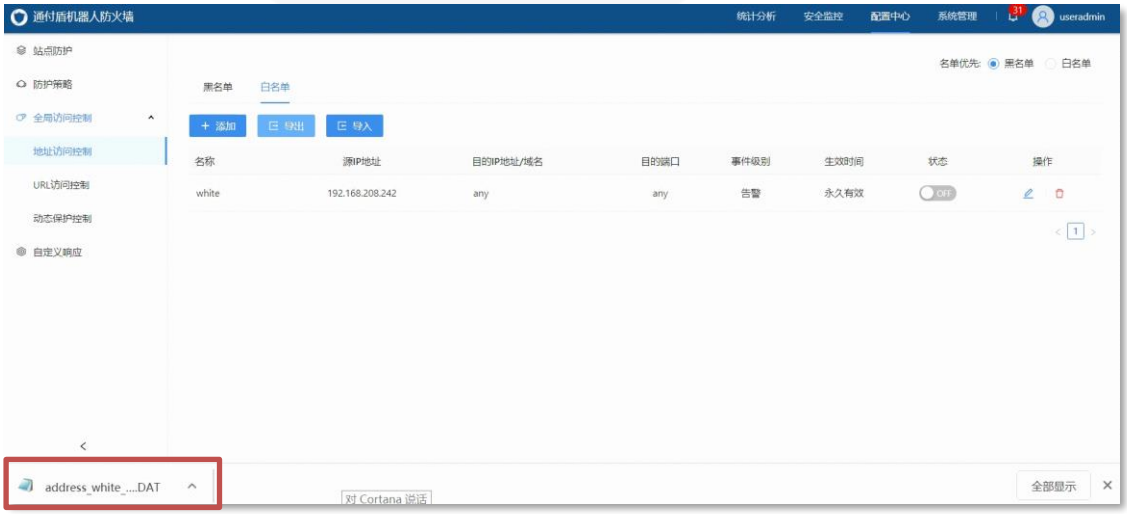
通过点击对应白名单下的“编辑”按钮，编辑白名单信息。

通过点击对应白名单下的“删除”，弹出对话框，可以删除白名单。

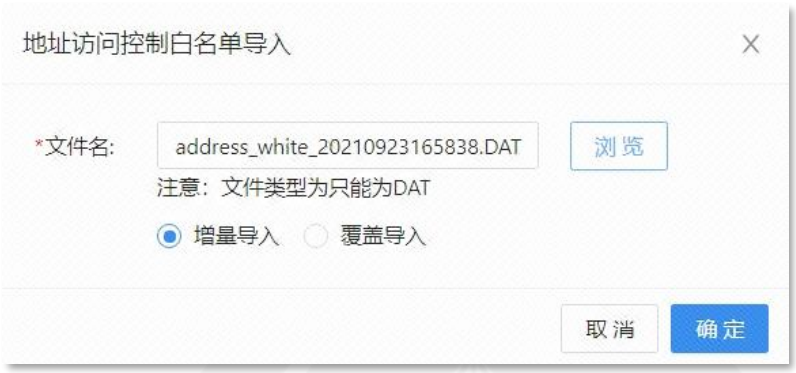


通过点击下图对应状态栏下的启用滑框，即可启用。反之关闭时，不启用。

通过点击“导出”按钮，将配置的白名单一键导出，生成“.DAT”文件，如下图：



通过点击“导入”按钮，将需要的白名单上传进行导入，如下图：



增量导入：比对现有白名单信息和需要导入文档，增加现有平台中没有的白名单信息。

覆盖导入：覆盖现有白名单信息，导入文档中的白名单信息。

通过选中白名单优先，则以白名单优先否则黑名单优先选中，以黑名单优先。（默认黑名单优先）

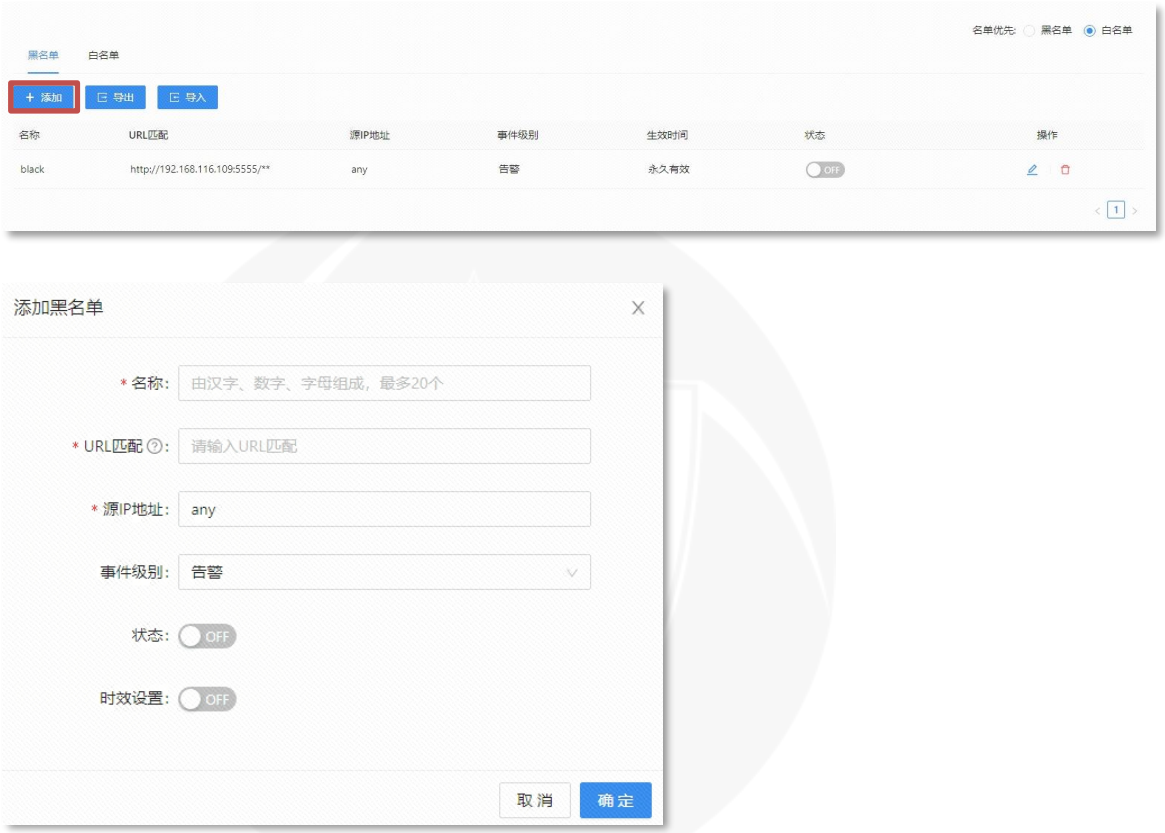
4.3.2 URL 访问控制

针对虚拟服务中的域名(Host)，可以设置黑白名单。黑白名单可针对 URL 配置，被配置进黑名单的 URL 不允许访问，白名单表示访问不做检测直接放行。

4.3.2.1 黑名单

黑名单为配置的直接拦截的 URL，其配置包括内容包括名称、URL 匹配、源 IP 地址、事件级别、状态、名单生效时间设置等。

通过点击“+添加黑名单”，添加 URL 黑名单。



名称：黑名单名称，由汉字、数字、字母组成，最多 20 个字符

URL 匹配：输入需要禁止访问的 URL，若以/*结尾则为部分匹配，否则为完全匹配

源 IP 地址：访问客户端 IP，默认 any 即为全部禁止

事件级别：可选择“信息”或“告警”两个其中一个级别，默认选择告警级别

状态：开启表示启用，关闭表示不启用

时效设置：启用，不配置则默认永久生效，也可以选择具体生效的日期，具体到

日

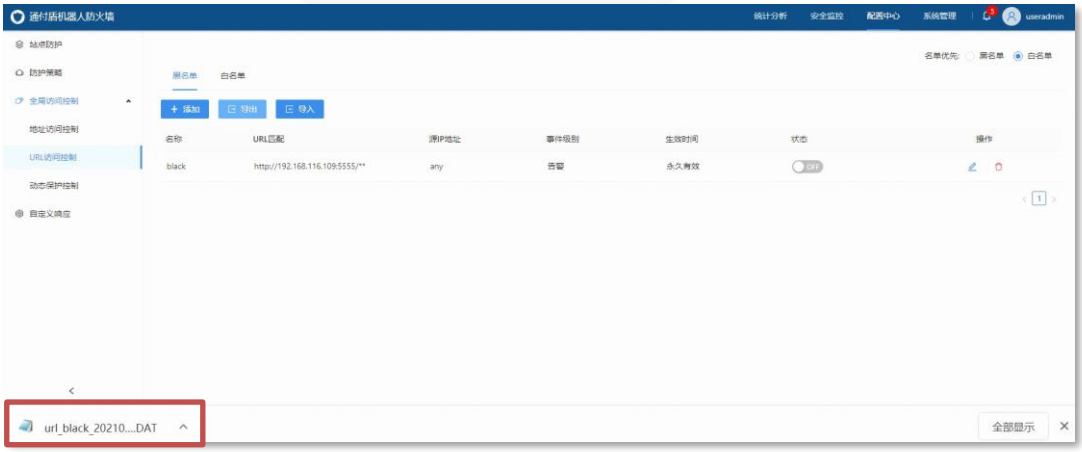
点击“确定”

通过点击对应黑名单下的“编辑”按钮，修改 URL 黑名单信息。

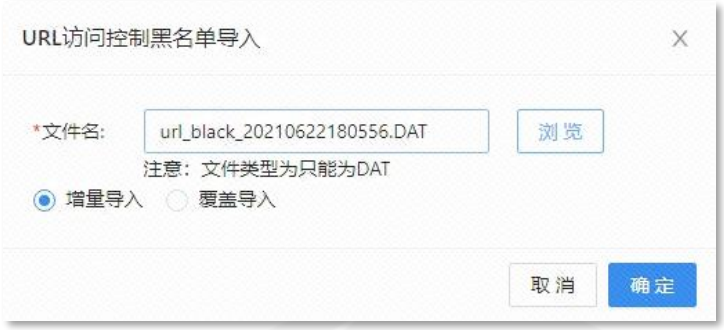
通过点击对应黑名单下的“删除”，弹出确定对话框，可以删除黑名单。

通过点击下图对应状态栏下的状态滑框，即可启用。反之关闭时，不启用。

通过点击“导出”按钮，将配置的黑名单一键导出，生成“.DAT”文件，如下图：



通过点击“导入”按钮，将需要的黑名单上传进行导入，如下图：



增量导入：比对现有黑名单信息和需要导入文档，增加现有平台中没有的黑名单信息

覆盖导入：覆盖现有黑名单信息，导入文档中的黑名单信息

通过选中名单优先中的黑名单，则以黑名单优先否则白名单优先选中，以白名单优先。（默认黑名单优先）

4.3.2.2 白名单

白名单为配置的直接放行的 URL，其配置包括内容包括名称、URL 匹配、源 IP 地址、事件级别、状态、名单生效时间设置等。

通过点击“+添加”，添加白名单。

名称：白名单名称，由汉字、数字、字母组成，最多 20 个字符

URL 匹配：输入需要放行的 URL，若以/*结尾则为部分匹配，否则为完全匹配

源 IP 地址：访问客户端 IP，默认 any 即为全部放行

事件级别：可选择“信息”或“告警”两个其中一个级别，默认选择告警级别

状态：开启表示启用，关闭表示不启用

时效设置：启用，不配置则默认永久生效，也可以选择具体生效的日期，具体到日

点击“确定”

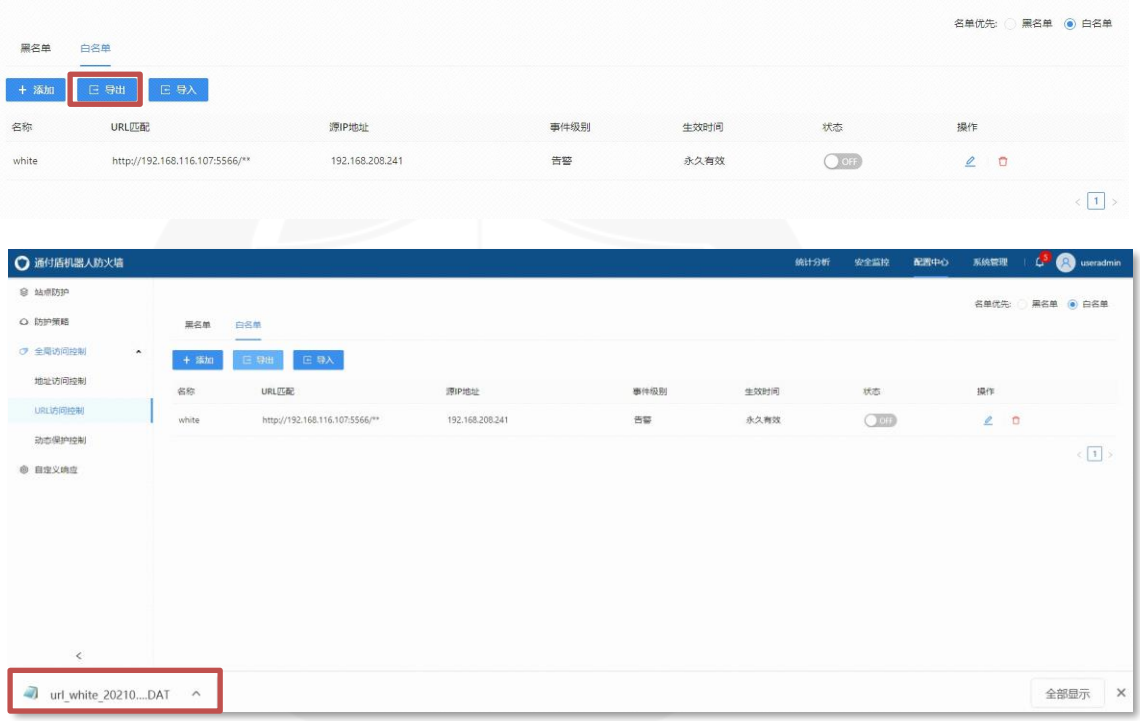
点击对应白名单下的“编辑”进行修改 URL 白名单信息。

通过点击对应白名单下的“删除”弹出确认对话框，可以删除白名单。

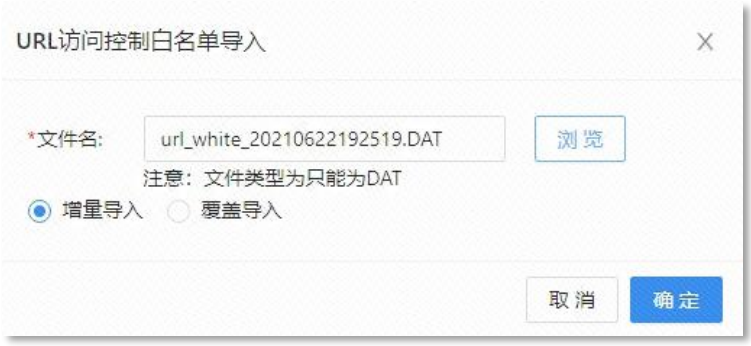
通过点击下图对应状态栏下的启用滑框，即可启用。反之关闭时，

不启用。

通过点击“导出”按钮，将配置的白名单一键导出，生成“.DAT”文件，如下图：



通过点击“导入”按钮，将需要的白名单上传进行导入，如下图：



增量导入：比对现有白名单信息和需要导入文档，增加现有平台中没有的白名单信息。

覆盖导入：覆盖现有白名单信息，导入文档中的白名单信息。

通过选中白名单优先，则以白名单优先否则黑名单优先选中，以黑名单优先。（默认黑名单优先）

4.3.3 动态保护控制

针对需要动态防护或不需要动态防护的具体网址，可以单独进行配置。

4.3.3.1 Form 保护

form 保护可设置针对特定的页面进行保护，具体操作配置通过进入全局访问控制>动态保护控制>form 保护，点击“+添加”。

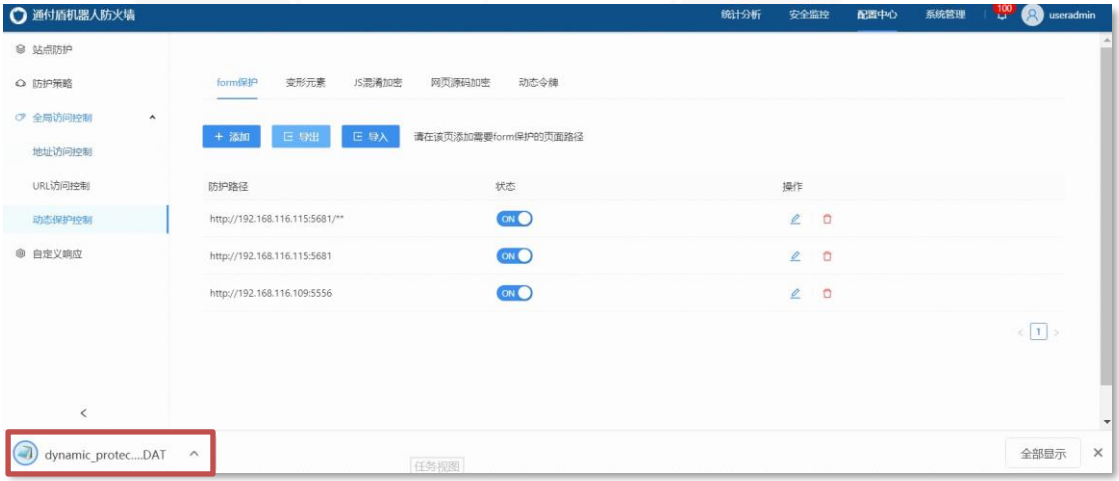
防护路径：配置需要进行 form 保护的路径页面

状态：开启表示启用，关闭表示不启用

通过点击“编辑”按钮，对已配置的页面路径进行编辑，如下图:

通过点击“删除”按钮，对已配置的页面路径进行删除，如下图：

通过点击“导出”按钮 ,将配置的防护路径一键导出 ,生成“.DAT”文件，如下图：



通过点击“导入”按钮，将需要的防护信息上传进行导入，如下图：

增量导入：比对现有防护路径和需要导入文档，增加现有平台中没有的防护路径信息。

覆盖导入：覆盖现有防护路径，导入文档中的防护路径信息。

4.3.3.2 变形元素

对重要的防护页面进行动态变形，保护网页不易受到攻击，具体操作为进入全局访问控制>动态保护控制>变形元素，点击“+添加”。

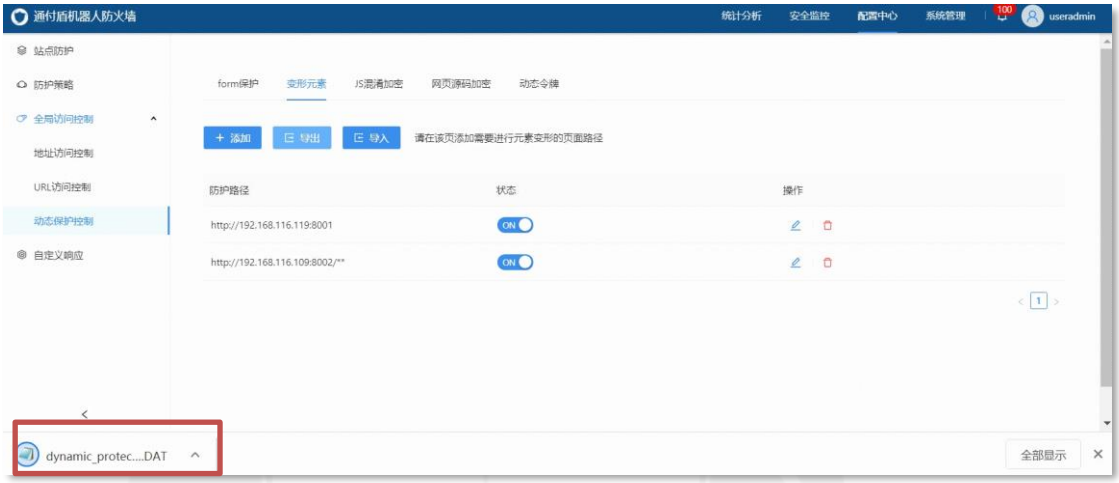
防护的元素： 配置需要进行元素变形的页面路径

状态：开启表示启用，关闭表示不启用

通过点击“编辑”按钮，对已配置的页面路径进行编辑，如下图：

通过点击“删除”按钮，对已配置的页面路径进行删除，如下图：

通过点击“导出”按钮，将配置的防护路径一键导出，生成“.DAT”文件，如下图：



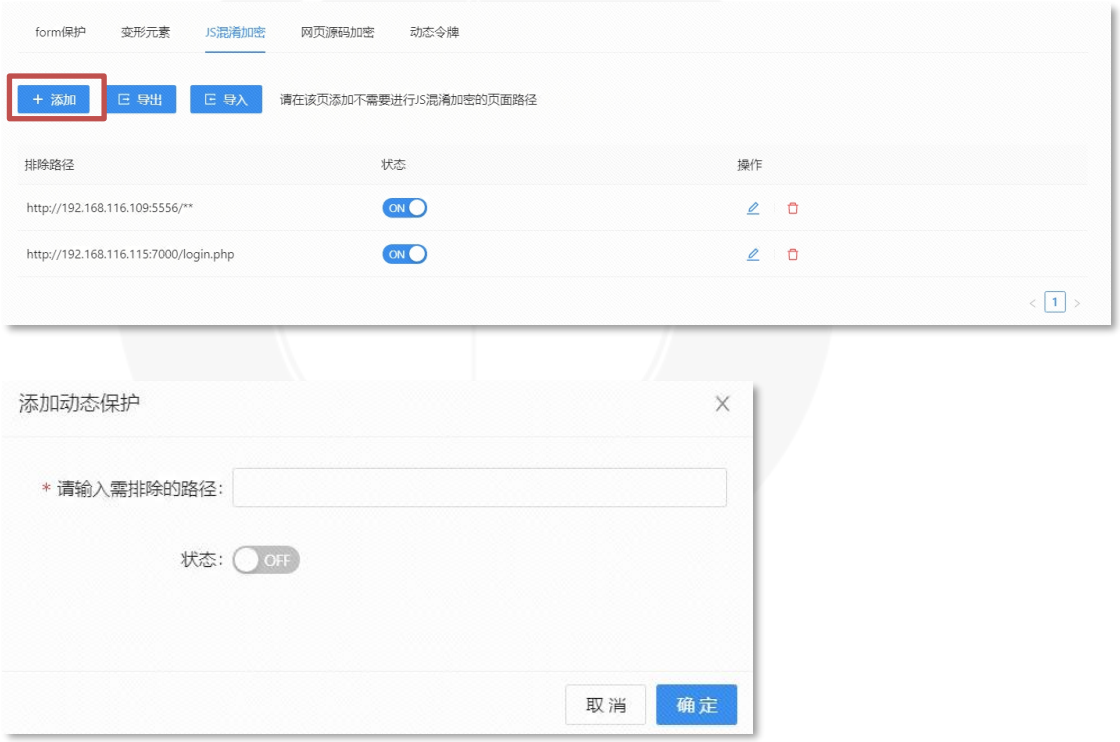
通过点击“导入”按钮，将需要的防护信息上传进行导入，如下图：

增量导入：比对现有防护路径和需要导入文档，增加现有平台中没有的防护路径信息。

覆盖导入：覆盖现有防护路径，导入文档中的防护路径信息。

4.3.3.3 JS 混淆加密

动态 WAF 默认将已防护的服务器中所有页面进行 JS 混淆加密保护，如有需要该特殊页面不需要保护，可通过全局访问控制>动态保护控制>JS 混淆加密，点击“+添加”。



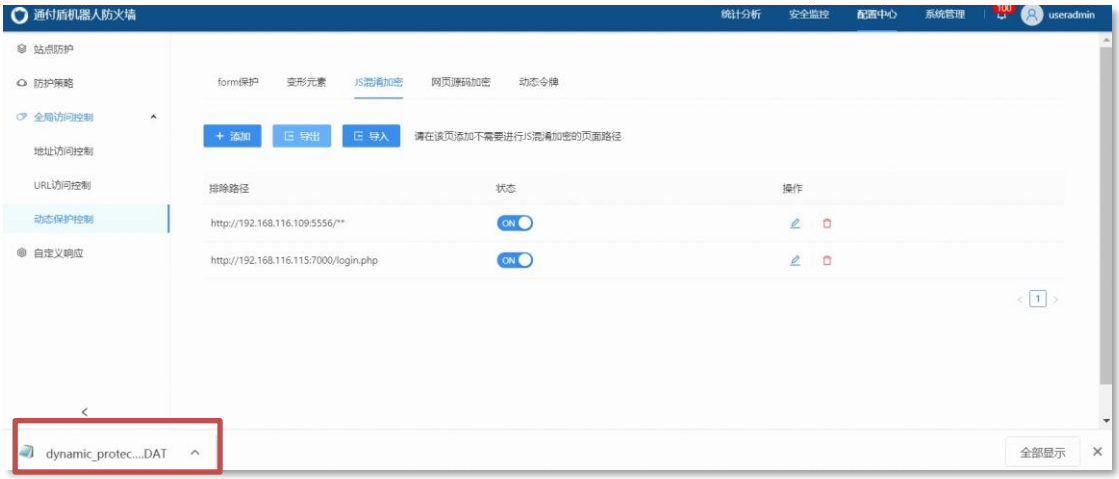
排除路径：配置不需要进行 JS 混淆加密的路径页面

状态：开启表示启用，关闭表示不启用

通过点击“编辑”按钮，对已配置的页面路径进行编辑，如下图：

通过点击“删除”按钮，对已配置的页面路径进行删除，如下图：

通过点击“导出”按钮，将配置的不需要进行 JS 混淆加密的路径页面进行导出，生成“.DAT”文件，如下图：



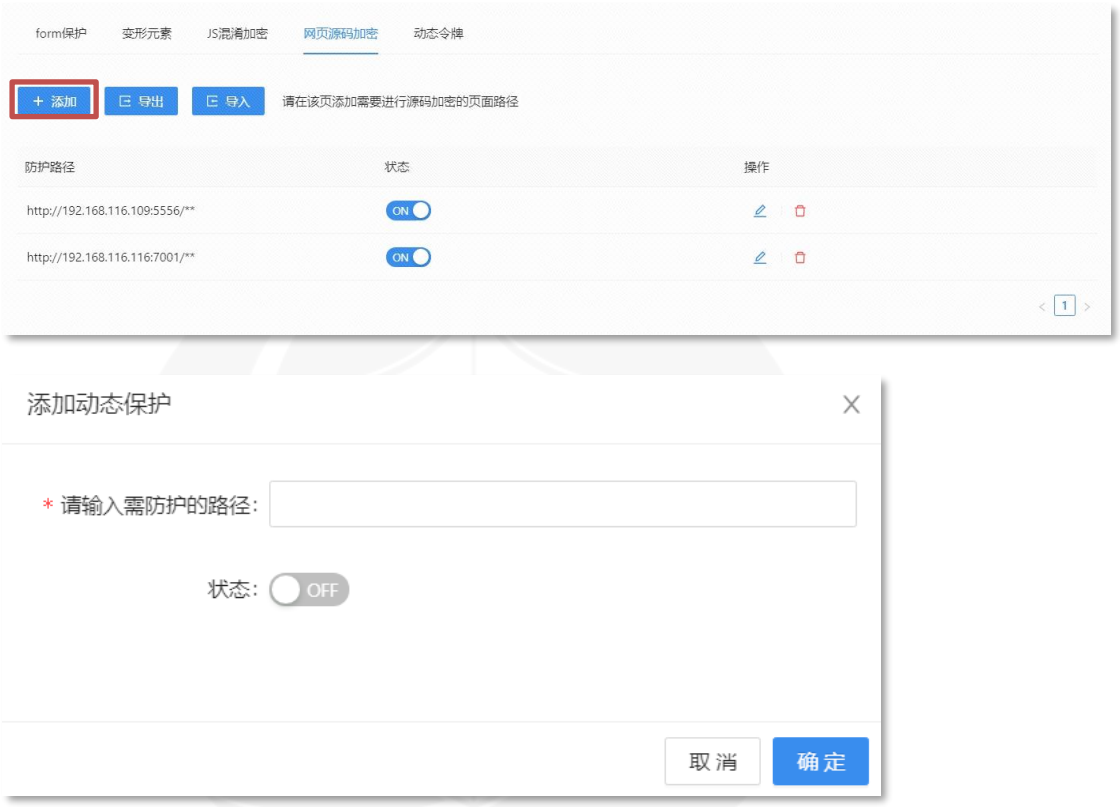
通过点击“导入”按钮，将需要排除 JS 混淆加密的文件上传进行导入，如下图：

增量导入：比对现有排除路径和需要导入文档，增加现有平台中没有的排除路径信息。

覆盖导入：覆盖现有排除路径，导入文档中的排除路径信息。

4.3.3.4 网页源码加密

动态 WAF 对网页源码进行加密，通过该加密，增加了攻击被防护页面的成本。如有关键页面需要特殊防护可通过全局访问控制>动态保护控制>网页源码加密，点击“+添加”。



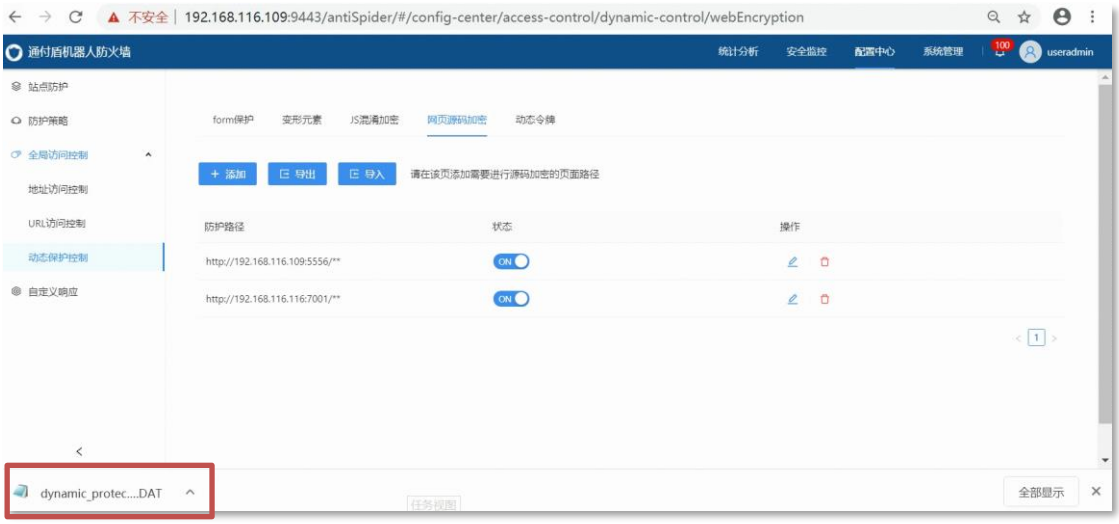
防护路径：配置需要进行网页源码加密的路径页面

状态：开启表示启用，关闭表示不启用

通过点击“编辑”按钮，对已配置的页面路径进行编辑，如下图：

通过点击“删除”按钮，对已配置的页面路径进行删除，如下图：

通过点击“导出”按钮，将配置的防护路径一键导出，生成“.DAT”文件，如下图：



通过点击“导入”按钮，将需要的防护信息上传进行导入，如下图：

增量导入：比对现有防护路径和需要导入文档，增加现有平台中没有的防护路径信息。

覆盖导入：覆盖现有防护路径，导入文档中的防护路径信息。

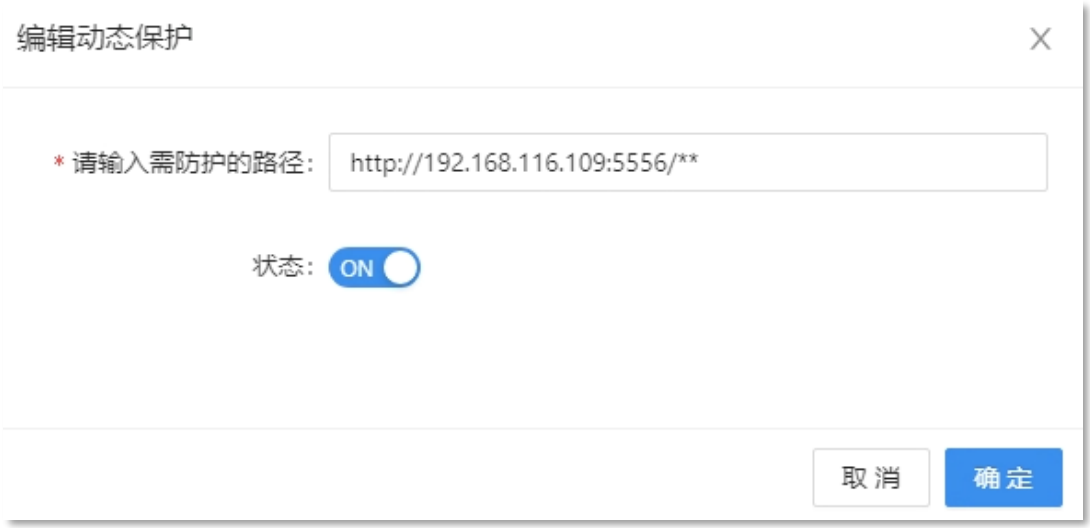
4.3.3.5 动态令牌

动态 WAF 可通过客户端产生的动态口令，提交至被防护的服务器，用来鉴别客户端身份。通过进入全局访问控制>动态保护控制>动态令牌，点击“+添加”。

防护路径：配置需要进行动态令牌的路径页面

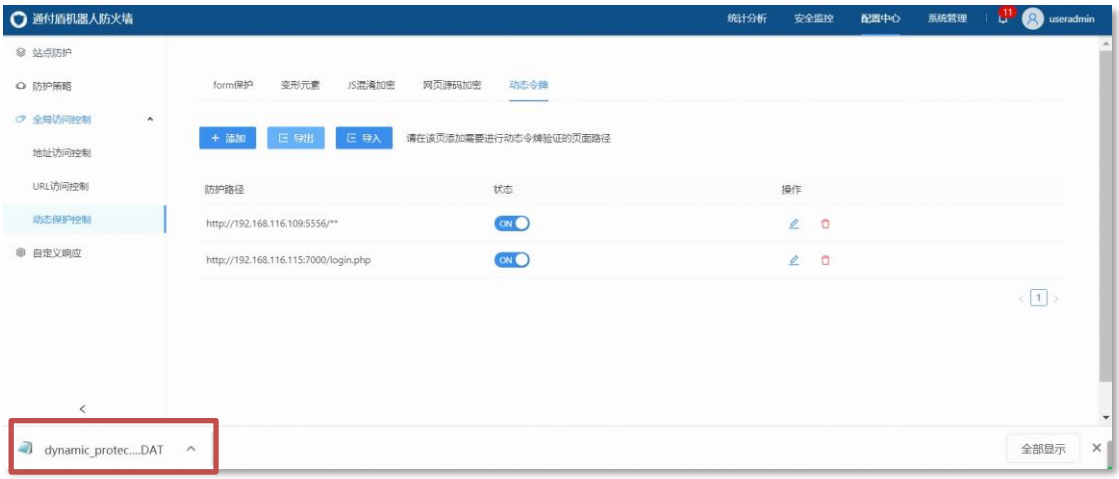
状态：开启表示启用，关闭表示不启用

通过点击“编辑”按钮，对已配置的页面路径进行编辑，如下图：



通过点击“删除”按钮，对已配置的页面路径进行删除，如下图：

通过点击“导出”按钮，将配置的不需要进行 JS 混淆加密的路径页面进行导出，生成“.DAT”文件，如下图：



通过点击“导入”按钮，将需要排除 JS 混淆加密的文件上传进行导入，如下图：

增量导入：比对现有排除路径和需要导入文档，增加现有平台中没有的排除路径信息。

覆盖导入：覆盖现有排除路径，导入文档中的排除路径信息。

4.4 自定义响应

自定义响应指用户可以根据自己的需要设置触发事件后的响应，也可不进行设置，自定义响应包括自定义错误页面和自定义重定向 URL，两者只能二选一，开启自定义错误页面，自定义重定向 URL 则自动关闭，开始自定义重定向 URL，则反之。

若开启自定义错误页面，点击上传按钮，可上传自定义的 html 页面。

开关: 选择是否启用自定义错误页面

重新上传错误页面: 选择所要上传的错误页面，上传的页面格式必须是 html 或者 htm，且大小不能超过 64k，页面名称不能超过 127B。

若开启自定义重定向 URL，可在重定向 URL 框内输入重定向 URL

地址。

开关：选择是否启用自定义重定向 URL

重定向 URL：输入所要定向的 URL

五、系统管理

5.1 系统信息

用户可以在系统信息页面查看基本系统信息，包括设备序列号、主机名称、系统时间及运行时间、软件版本、特征库版本等。

5.2 设备管理

5.2.1 配置及操作

配置系统相关信息，配置如主机名、域名、软/硬 Bypass 等信息。

某些情况下，用户的网络环境中会配有一台以上设备，为区分这些设备，就需要为每一台设备指定不同的名称。设备的默认名称是其平台名称。

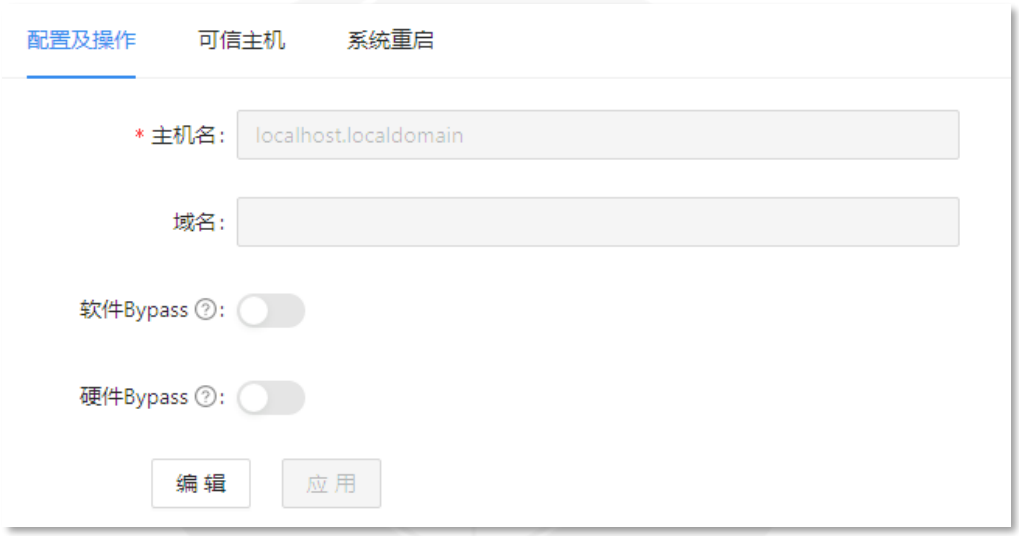
主机名称：在“主机名称”文本框中输入设备的主机名称，通过系统信息及统计分析页面展示主机名称。

域名：在“域名”文本框中输入设备的域名。

软件 Bypass：软件 Bypass 开启后，设备在特定状态下，如动态 WAF 系统软件出现故障，不能正常转发网络流量，但硬件设备正常运

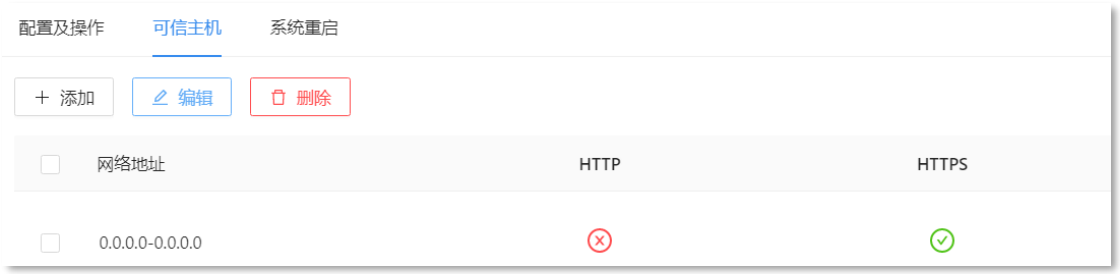
行，为保证业务的连通性，开启软件 Bypass 之后，防火墙系统将网络流量自动转发至防护站点，不做任何监测防护。

硬件 Bypass：硬件 Bypass 开启后，设备在特定状态下，如系统重启、设备断电，不能正常转发网络流量时，系统将自动进入 Bypass 状态（即自动启用状态）。在 Bypass 状态下，互为 Bypass 的接口对在物理上直接连通，两接口之间相当于连接了一根网线，流量将直接通过。

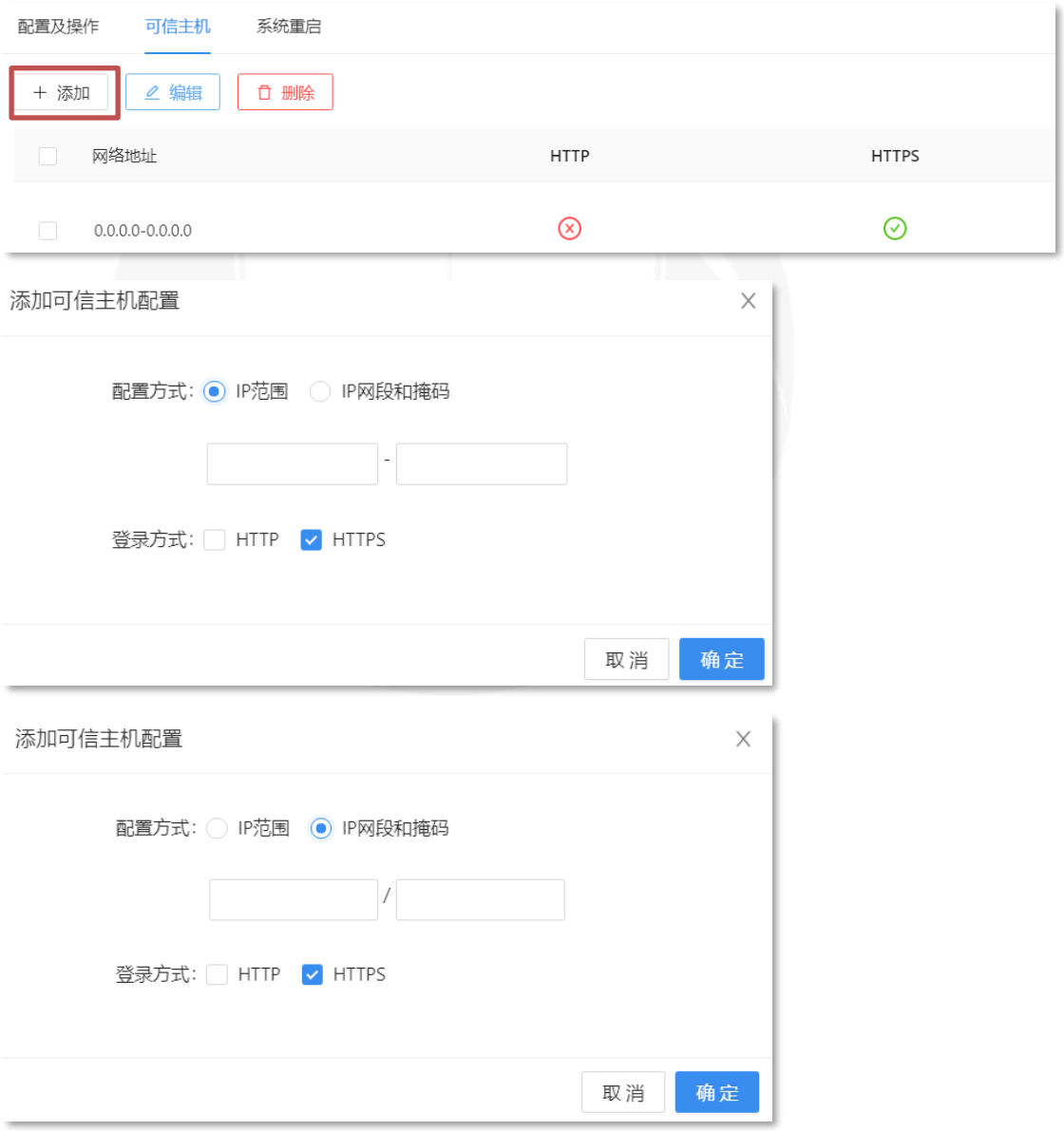


5.2.2 可信主机

设备使用可信主机来进一步保证系统安全。管理员可以指定一个 IP 地址范围，在该指定范围内的主机为可信主机。只有可信主机才可以对设备进行管理。出厂默认所有主机均可以访问动态 WAF ,如下图：

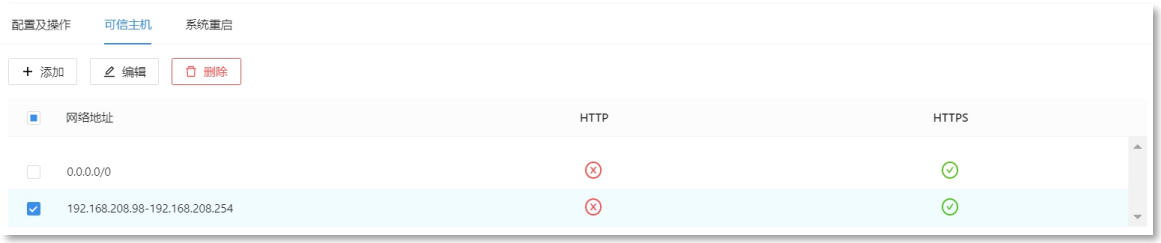


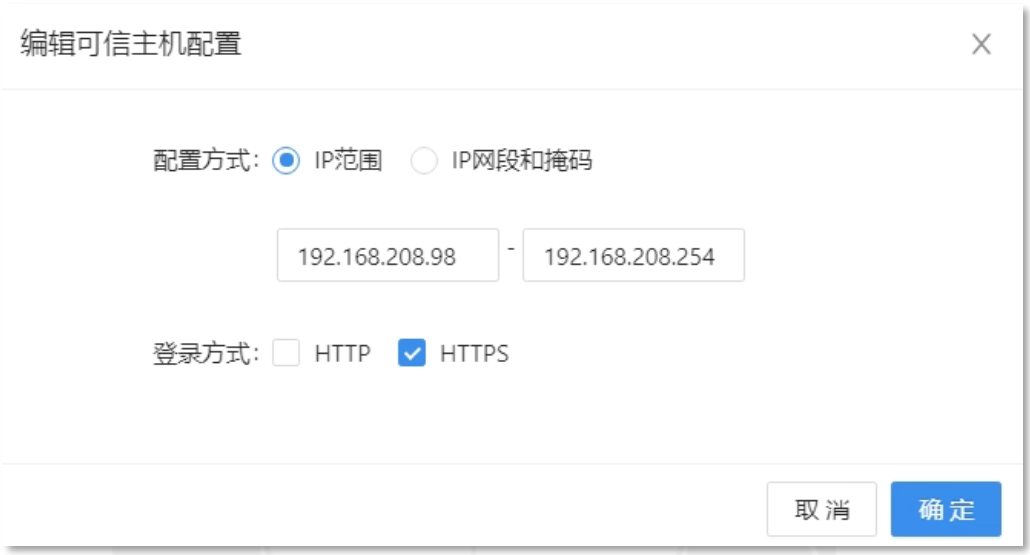
可通过“+添加”按钮，添加可信主机对防火墙的访问，可选择“IP 范围”和“IP 网段和掩码”两种方式。（注：如果不删除 0.0.0.0-0.0.0.0 默认可信主机配置，所有主机均可通过 https 协议访问）



可通过勾选需编辑的可信主机配置，点击“编辑”按钮，编辑已

添加的可信主机，可编辑配置方式及登录方式。





可通过勾选需删除的可信主机配置，点击“删除”按钮删除已配置的可信主机，删除后的地址不能访问动态 WAF。

5.2.3 系统重启

系统在安装许可证、系统升级等操作需要设备重启才能生效。具有两种重启方式：断电重启、软件重启。

断电重启：该重启方式包括硬件的断电和软件的重启；

软件重启：该重启方式仅支持动态 WAF 软件的重启；

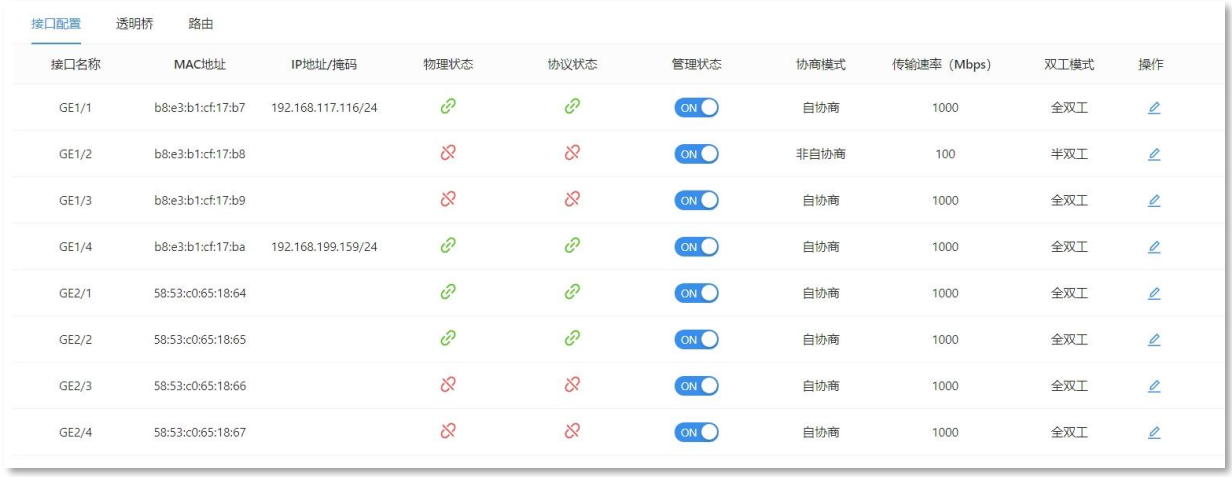
点击“断电重启”或“软件重启”，弹框二次确认是否重启。

5.3 网络配置

通过配置接口，可以实现通过网络方式对动态 WAF 设备的管理操作，可对该设备的接口 IP 地址、子网掩码以及配置透明网桥等操作。

5.3.1 接口配置

通过点击各个网口的“编辑”按钮，可修改该网口的 IP 地址、子网掩码，修改后点击完成，如要启用该网口点击“确定”即可。



接口名称：选择该接口的名称展示

IP 地址：配置该接口的 IP 地址

子网掩码：配置该接口的子网掩码

描述：描述该接口，输入内容在 20 个字符之内

管理访问：允许通过 Ping、HTTP、HTTPS 访问方式（默认开启 Ping、HTTPS 管理方式）

MTU：设置接口的 MTU 值，可输入范围 68-1500 数值，默认 1500B

自协商：对于非光纤接口通过选择非自协商模式，可选择相应的双工模式和速率

5.3.2 透明桥

透明网桥使用最方便，易于安装。当桥接入互连的局域网内，就能运行。它不会影响现存的局域网，原有的软硬件无须改变，对于用户来说，该网桥是透明的，即该网桥进入或离开整个网络，用户感觉不到。配置透明网桥后，需要将实际物理接口加入网桥中，这些接口被称为网桥组端口。

动态 WAF 平台支持透明桥功能，通过点击“编辑”按钮，接入透明桥界面编辑，如下图：

桥名称：透明桥组名称展示

IP 地址：配置该桥组的 IP 地址

子网掩码：配置该桥组的子网掩码

描述：描述该桥组，输入内容在 20 个字符之内

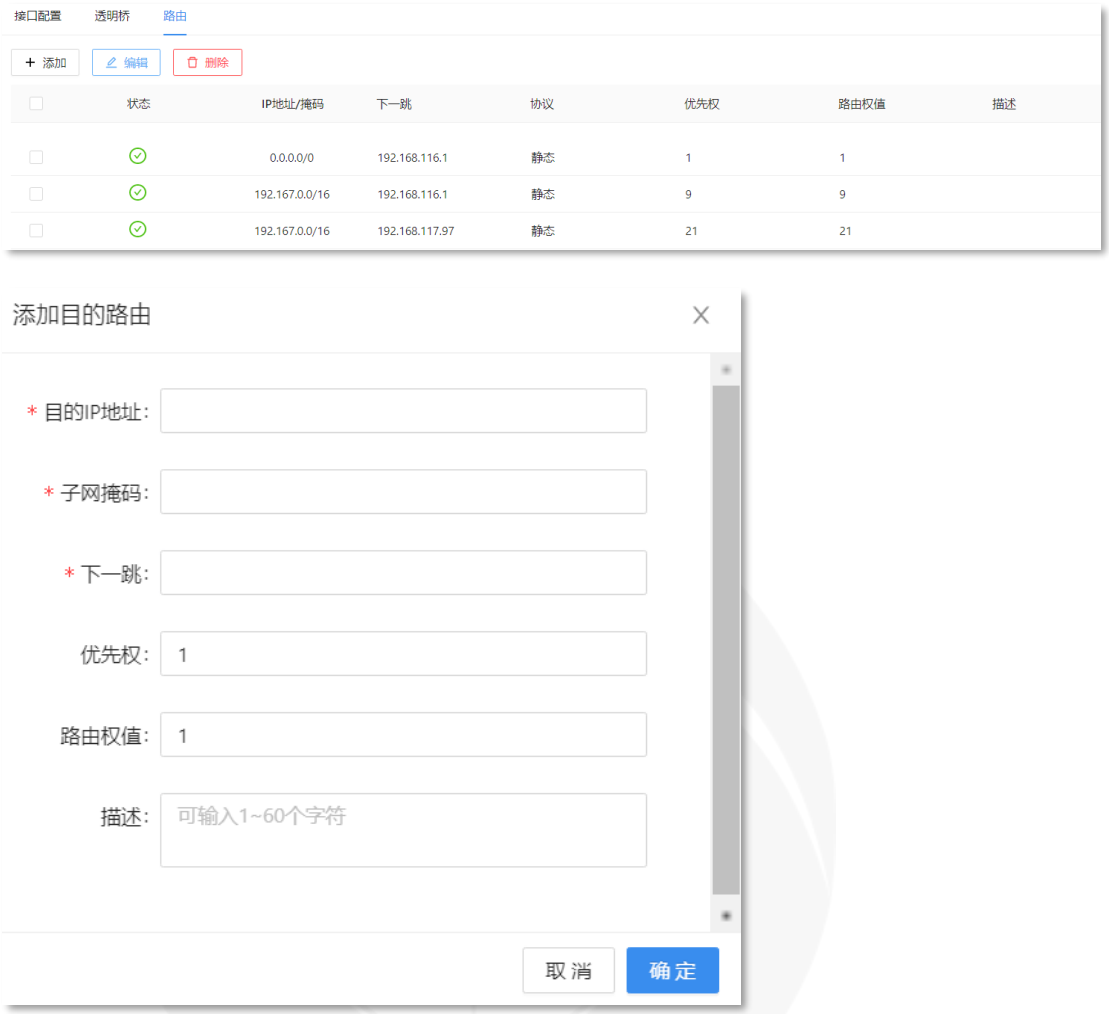
管理访问：允许通过 Ping、HTTP、HTTPS 访问方式（默认开启 Ping、HTTPS 管理方式）

接口列表：接口以 bypass pair 对展示，勾选实际的物理接口加入到桥组中（同一接口只能添加到同一网桥组中）

5.3.3 路由

动态 WAF 平台中支持路由配置，由配置管理员通过手动输入 IP 地址子网掩码和下一跳等配置形成路由。

通过点击“添加”按钮，弹出“添加目的路由”界面，如下图：



目的 IP 地址：配置路由的目的 IP 地址

子网掩码：配置路由的目的 IP 地址

下一跳：配置路由的下一跳地址

优先权：配置该条路由的优先权，可输入范围 1~255，默认为 1，该参数取值越小，优先级越高，而在多条路由选择的时候，优先级高的路由会被优先使用

路由权值：配置路由的路由权值，可输入范围 1~255，默认为 1，路由权值决定负载均衡中流量转发的比重

描述：配置目的路由的描述信息，可输入范围 0~60 字符

通过点击“编辑”按钮，弹出“编辑目的路由”界面，配置信息均可编辑，如下图：

通过勾选所需路由（自动生成的“直连”“主机”路由除外），点击“删除”按钮，弹出删除确认，如下图：

5.4 状态检测

5.4.1 资源监控

页面可展示防火墙 CPU、内存、硬盘使用情况，通过使用占比的方式可方便的看到异常情况，当 CPU、内存、硬盘超出所定义的阈值，可通过屏幕告警的方式告知管理员。

5.4.2 服务监控

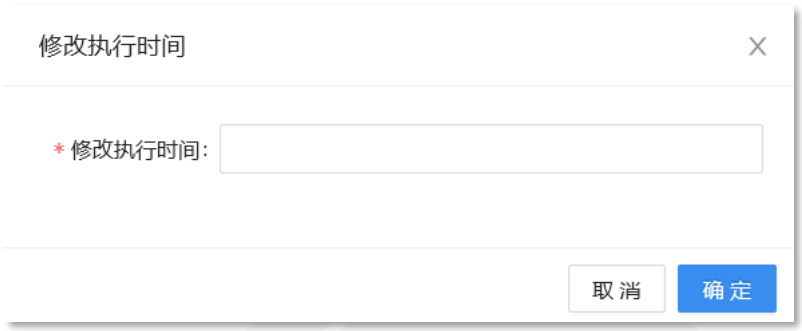
列表信息包括序号、Job 名称、Job 状态、当前运行状态、最后一次执行时间、最后一次执行结果、下一次执行时间、设定执行时间、Job 操作（修改执行时间、手动执行）。

统计报表数据处理支持对统计分析页面中所有图表、列表、柱状图、折线图以及安全监控模块下安全事件统计中图表信息展示的数据定期更新或手动更新。

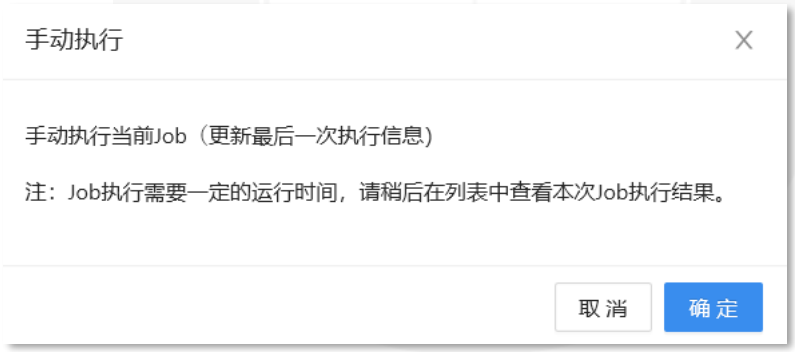
服务状态监控支持对平台所运行的服务进行监测，可对数据定期更新或手动更新。

序号	job名称	job状态	当前运行状态	最后一次执行时间	最后一次执行结果	下一次执行时间	设定执行时间	Job操作
37	统计报表数据处理	ON	等待中	2021-04-01 08:59:59	成功	2021-04-01 09:59:59	59 59 * * * ?	修改执行时间 手动执行
38	服务状态监控	ON	等待中	2021-04-01 09:56:00	成功	2021-04-01 09:56:59	0/59 * * * * ?	修改执行时间 手动执行

点击“修改执行时间”，提示弹窗，更改后 Job 运行时间更改。



点击“手动执行”，提示弹窗，确认后 Job 重新执行“最后一次执行”的信息并更新，执行成功后，更新列表中“最后一次执行时间”和“最后一次执行结果”。

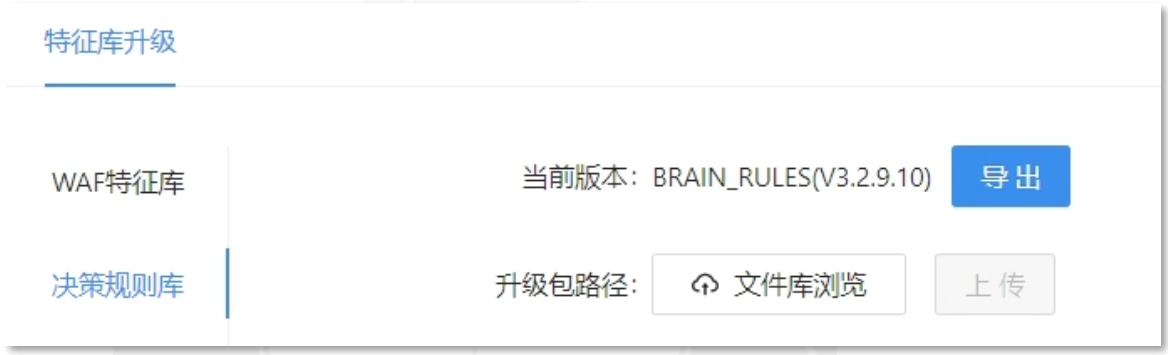


5.5 升级管理

5.5.1 WAF 特征库

对于攻击防护采用特征库的形式，如有新增特征，可通过上传.tar.gz 文件进行上传。

5.5.2 决策规则库



5.6 授权管理

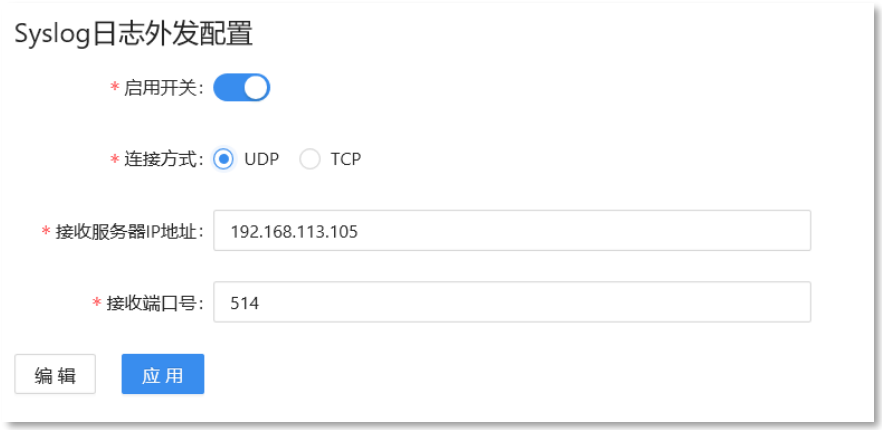
用户要正常使用设备，需要对设备的进行授权，如果没有授权，设备对数据流不进行检测。

授权方式分为两种 :正式授权和试用授权。正式授权按照基础版、标准版、企业版、旗舰版分类，不同版本对应不同的软件功能。

5.7 日志配置

系统日志是一种记录设备运行状况的方法。本设备支持标准的 Syslog 格式， 本地日志以及 Data-Center 日志，提供给用户掌握系统运行状况的方法。

日志发送的方式为产生一条发送一条 ,对于历史存留的日志不做发送。配置 syslog 服务器，默认端口是 514，可修改，可选择用的是 TCP/UDP 协议。



启用：选中表启用，不选表关闭

连接方式：按需选用 TCP 或者 UDP 方式连接

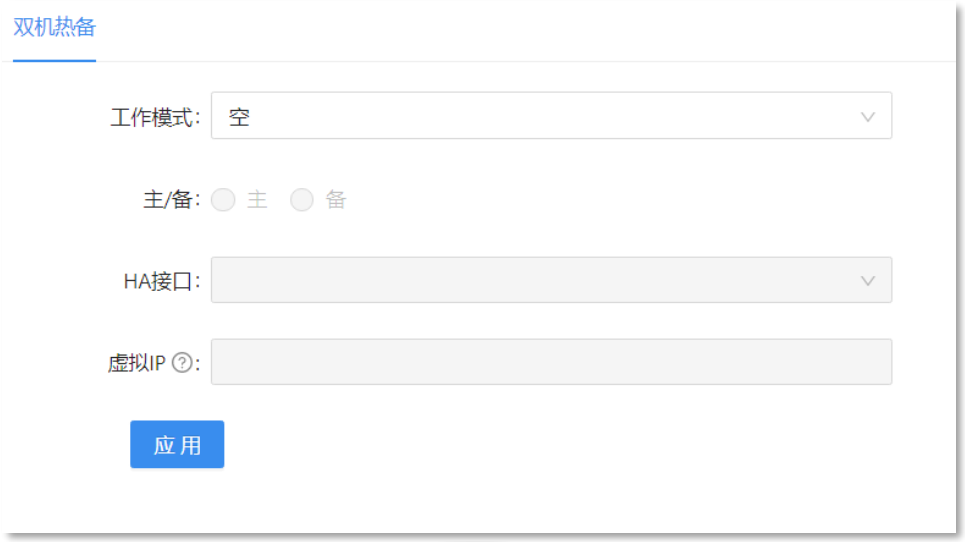
接收服务器 IP 地址：Syslog 服务器地址

接收端口号：Syslog 服务器端口

注意：若选择 TCP 连接方式，需要选择证书上传。

5.8 高可靠性

使用互为备份的两台防火墙共同执行同一服务，其中一台主机为工作机（Primary Server），另一台主机为备份主机（Standby Server）。在系统正常情况下，工作机为应用系统提供服务，备份机监视工作机的运行情况(工作机在工作的同时也在检测备份机是否正常)，当工作机出现异常，不能支持应用系统运营时，备份机主动接管工作机的工作，继续支持关键应用服务，保证系统不间断的运行。



工作模式: 默认为空，可选择为主/备的方式。

主/备: 选择该台设备为工作机或者备用机

HA 接口：选择哪个物理接口与另一台设备进行连接

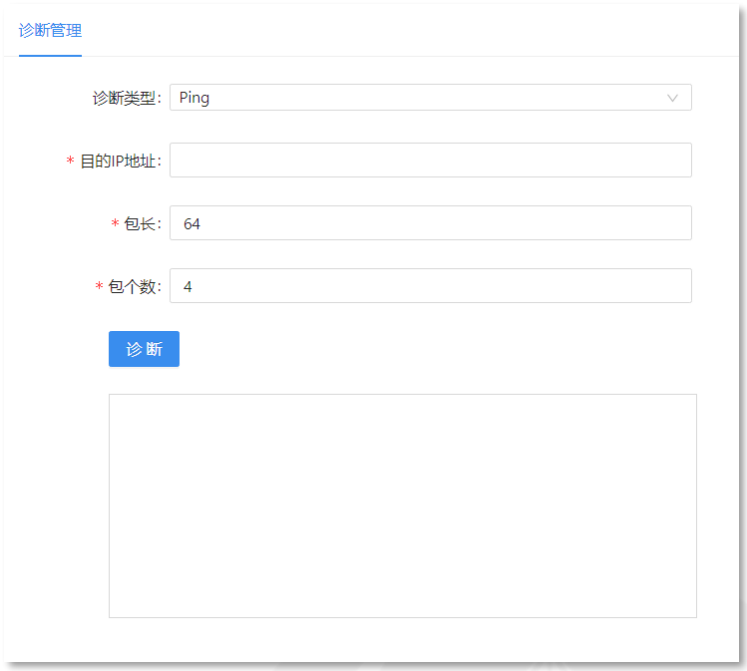
虚拟 IP：通过虚拟 IP，主备防火墙共用该 IP 地址，进行主备切换。

5.9 诊断工具

5.9.1 诊断管理（Ping）

设备提供了 Ping 命令用来检测网络的基本连接情况，Ping 命令发送 Internet Control Message Protocol (ICMP) 请求报文到网络中的某个 IP 设备。

如果在设定时间内没有收到目的设备响应报文，则不输出任何信息，否则显示响应报文的字节数、报文序号、TTL 、响应时间。



诊断类型：选择 ping 诊断

目标 IP 地址：目标地址

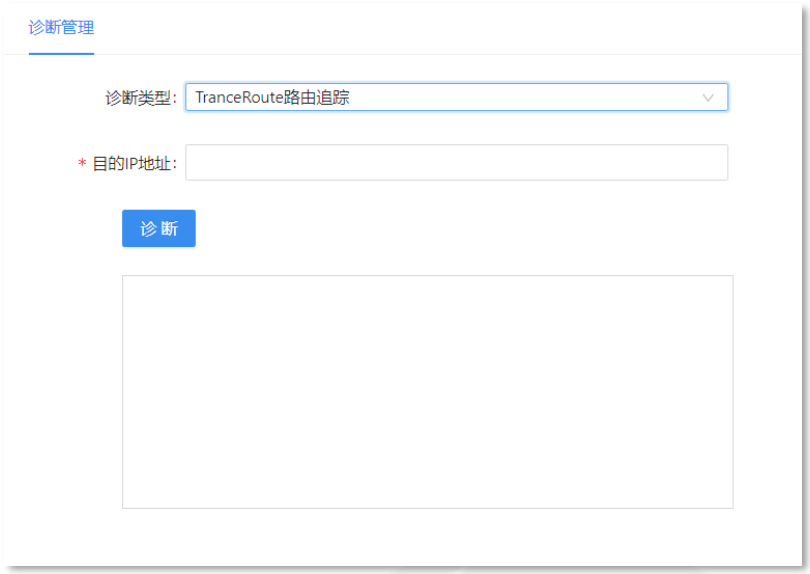
包长：每个诊断包的长度

包个数：每次诊断发送的包数

诊断结果：返回诊断结果

5.9.2 系统诊断（TraceRoute）

TraceRoute 是另一种检测网络连接情况的命令，它与 ping 命令不同的是它不但可以测试网络是否连通还可以获知数据包的传输路径中在哪一个地方出现问题。TraceRoute 命令的输出信息包括到达目的地所有经过的网关的 IP 地址和到此网关所用时间，如果某网关超时则显示“*”。另外，基于 TraceRoute 实现了对目标主机 UDP 端口探测的功能，可以检查目标主机某一 UDP 端口的开放状态。



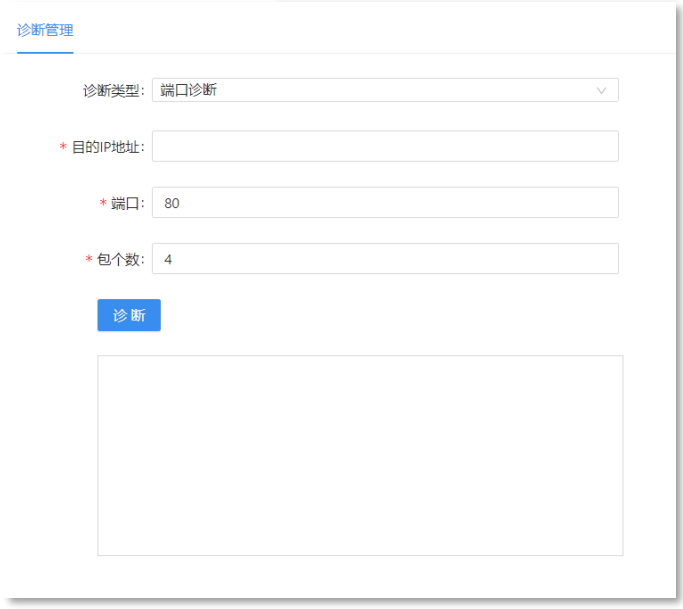
诊断类型：选择 TraceRoute 诊断。

目标 IP 地址：目标 IP 地址或域名。

诊断结果：返回诊断结果。

5.9.3 端口诊断

端口诊断显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运作。



诊断类型：选择端口诊断

目标 IP 地址：目标 IP 地址或域名。

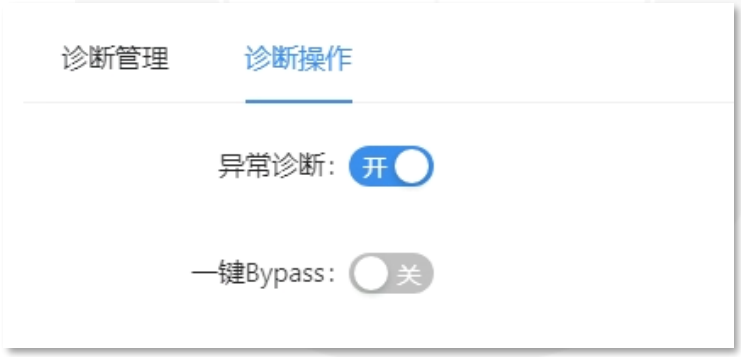
端口：输入侦听端口，如 80、8080 等。

包个数：输入包个数（0-10 之内）。

诊断结果：返回诊断结果。

5.9.4 诊断操作

为了避免客户登录具有较高的操作权限的动态 WAF 的 Linux Shell，默认关闭 telnet 和 ssh 等远程登录协议的 22 和 23 侦听端口，若排查异常现象，可将异常诊断打开。并且为了满足在产品在上线时接入前后的现象对比，可开启一键 Bypass 功能。



六、版权声明

七、免责申明

本文档依据现有产品信息制作，其内容如有更改，恕不另行通知。江苏通付盾科技有限公司在编写文档的时候，已尽最大努力保证其内容准确可靠，但本公司不对其中的遗漏、不准确或错误导致的损失和损害承担责任

通付盾®
Pay Egis

扫码注册通付盾云

扫码安装通付盾应用

北京·上海·广州·深圳·苏州·杭州·成都

客服电话：400-831-8116

官方网址：www.tongfudun.com

商务合作：info@tongfudun.com

售后服务：service@tongfudun.com