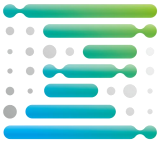

中云网安
ZYPROTECT

AI 防护者用户手册

应用安全防护解决方案

版本： 9.0

中云网安科技有限公司

目录

1 产品安装

1.1 Linux 环境安装

中云网安的 AI 防护者使用 RPM 包安装在 Linux 计算机上。下面列出了支持的 Linux 发行版：

- CentOS 7
- Redhat Enterprise Edition 7

Linux 系统上安装 AI 防护者，请打开终端/控制台，以 root 管理员身份登录，进入到 AI 防护者 RPM 安装包文件所在的目录，然后键入以下命令：

rpm -U --force zyWAF-9.0.1-336.centos7.x86_64.rpm

备注：9.0.1-336 是版本号，随着发版而变化

如图 1-1 所示：

```
[root@localhost src]# rpm -U --force zyWAF-9.0.1-336.centos7.x86_64.rpm
---------- Creating the MariaDB system databases and tables
---------- Starting the server..Done
---------- Creating/updating users
---------- Stopping the server.Done
---------- Starting the server..Done
---------- Creating zyWAF databases

---------- Stopping the server.Done
***** Starting upgrade at Mon May 30 18:12:38 2022
----- Info: Upgrading from version 9.0.1
----- Info: Skipping upgrade for 8.2.6
----- Info: Skipping upgrade for 9.0.0
***** Finishing upgrade at Mon May 30 18:12:38 2022
```

图 1-1 安装信息

注意：AI 防护者管理界面默认使用 TCP 端口 8020。

1.2Windows 环境安装

中云网安的 AI 防护者使用 EXE 程序安装在 Windows™ 操作系统上。以管理员权限安装 AI 防护者。 下面列出了支持的 Windows 版本：

- Windows Server 2016

Windows 系统上安装 AI 防护者，请打开终端/控制台，以 root 管理员身份登录，进入到 AI 防护者安装包文件所在的目录，运行 EXE 安装程序后可以看到一安装提示：（图 1-2）单击“下一步”继续安装。

图 1-2 Windows 安装界面

此页面显示许可协议。（图 1-3）单击“下一步”接受协议并继续。

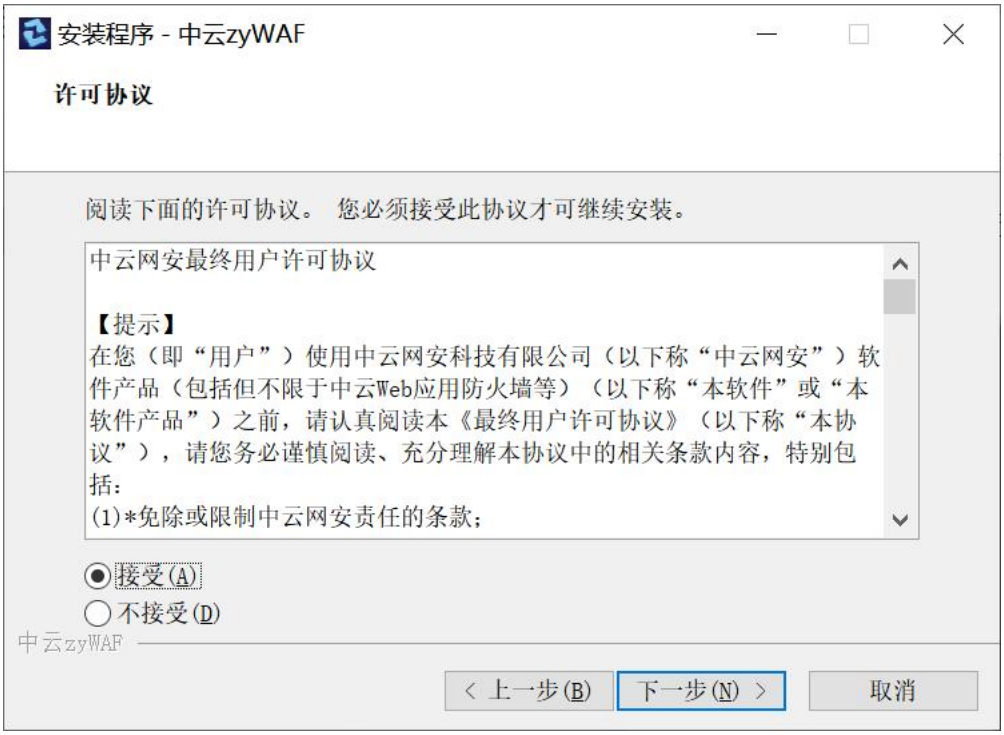

图 1-3 许可协议

单击“安装”后，将开始安装。（图 1-4）程序可执行文件和配置文件将安装到目录 C：Program Files (x86)\WAF。

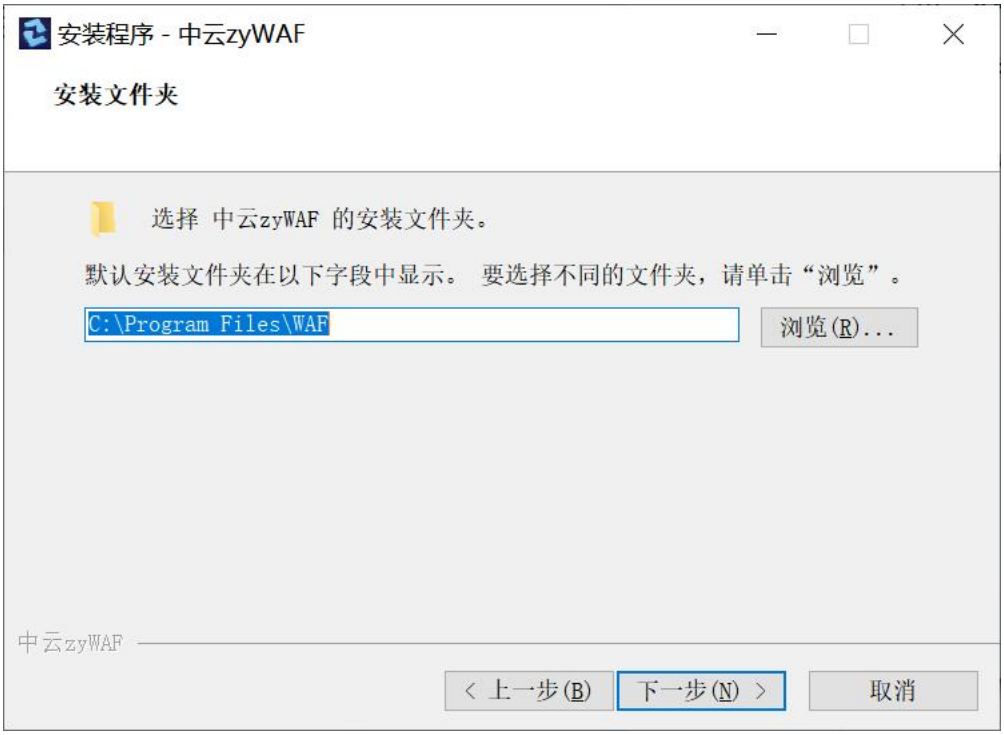
安装程序 - 中云zyWAF
安装文件夹
选择 中云zyWAF 的安装文件夹。
默认安装文件夹在以下字段中显示。 要选择不同的文件夹，请单击“浏览”。
C:\Program Files\WAF
浏览(R)...
中云zyWAF
< 上一步(B)
下一步(N) >
取消

图 1-4 准备安装

进度条显示安装过程 （图 1-5）

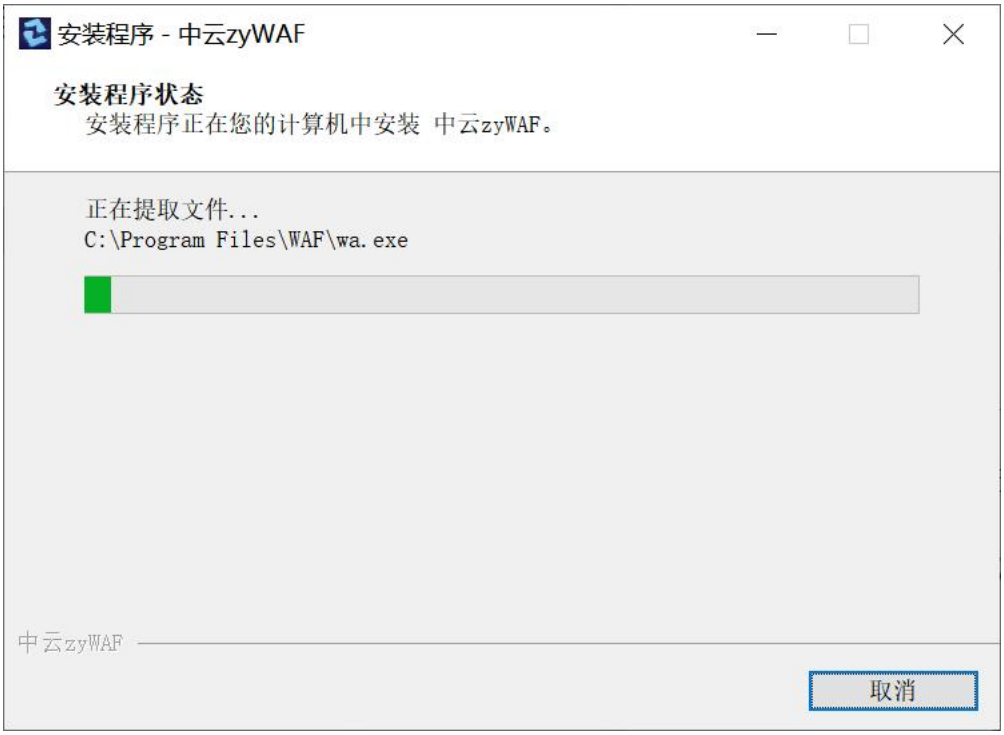

图 1-5 安装过程

在安装过程中，Web Application Firewall 将被注册为 Windows 服务。 如果系统上已经安装了安全软件，在您与安全软件确认允许安装之前，可能会阻止安装进度。安装完成后，可以看到一条确认消息。

单击 完成 按钮完成安装程序（图 1-6）。

图 1-6 安装完成

AI 防护者安装成功后，会使用 8020 端口启动服务“Web Application Firewall”。

注意：验证 Web Application Firewall 是否正在运行：在 Windows 任务管理器中选择进程，后台进程，应看到状态为“已启动”的服务“Web Application Firewall”。

（图 1-7）。

图 1-7 Windows 服务验证

注意：验证端口 8020 是否可用于 AI 防护者管理界面访问，请从 Windows 命令

提示符窗口键入以下命令。

netstat -an | findstr “8020”

输入此命令后，您应该会看到如图 1 8 所示的响应。

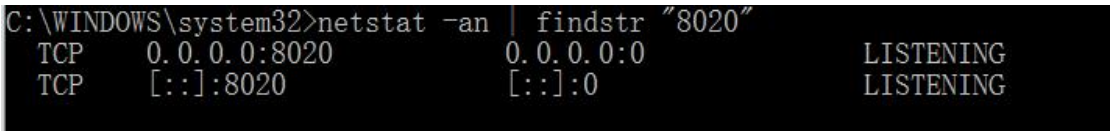

图 1-8 管理界面端口验证

1.3开始和停止 AI 防护者进程

AI 防护者完成安装后，进程会自动运行，无需手动启动。

基于便于运维的目的，下面列出了启动和停止 AI 防护者 的命令：

- CentOS 7 和 Redhat Enterprise Edition 7

  systemctl stop zywaf

  systemctl start zywaf

- Windows Server 2016

  步骤 1 -打开任务管理器并单击服务选项卡

  步骤 2 -右键单击或按住 AI 防护者 服务，单击停止或启动

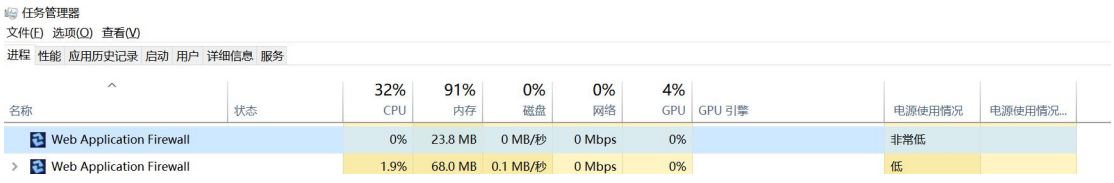

图 1-9 Windows 任务管理器

2 快速设置

AI 防护者管理控制台在安装成功后会监听 8020 端口。 推荐的浏览器是：Chrome 和 Firefox。 通过将浏览器定向到以下地址来访问管理控制台：

https://IP:8020　　https://192.168.1.3:8020

您的浏览器可能会显示该证书不受信任，因为控制台的默认证书是自签名的。 请接受默认证书，然后继续登录对话框。

对于初始登录（图 2-1），使用以下凭据登录管理控制台：

Username：　admin

Password：　admin

注意： 旧版本的 IE 浏览器必须启用 TLS 1.1 或 TLS 1.2 才能使用管理控制台。

图 2-1 登录页面

首次登录后，强制修改 admin 用户密码（图 2-2）

图 2-2 首次登录密码修改

完成密码修改后，AI 防护者默认启用快速设置，（图 2-3）。也可以在左侧菜单中选择“设置-服务器设置-添加服务器”进行更详细的设置，详情见目录 4.1。

注意：使用快速设置过程中会提示您输入许可证密钥（可选择试用证书进入到下一步配置）。

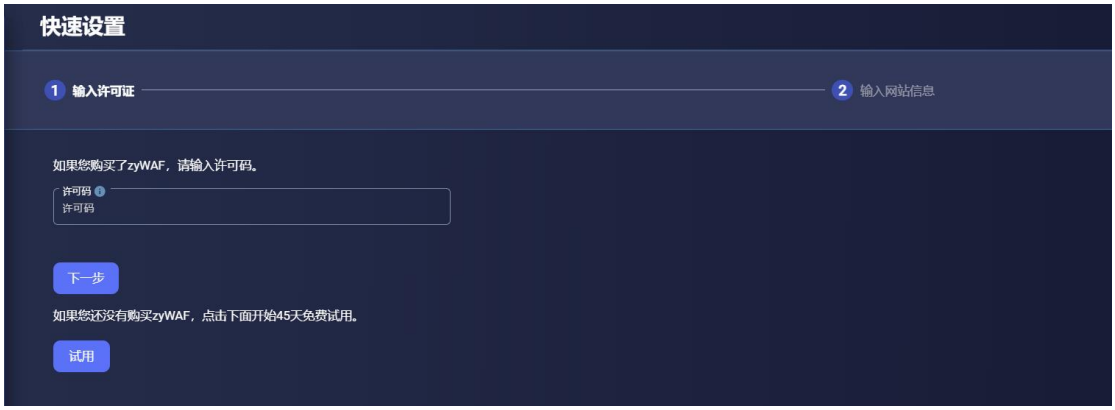

图 2-3 快速设置

在“输入网站信息”中输入被保护 Web 应用的信息，然后点击“开始学习”。（图 2-4）

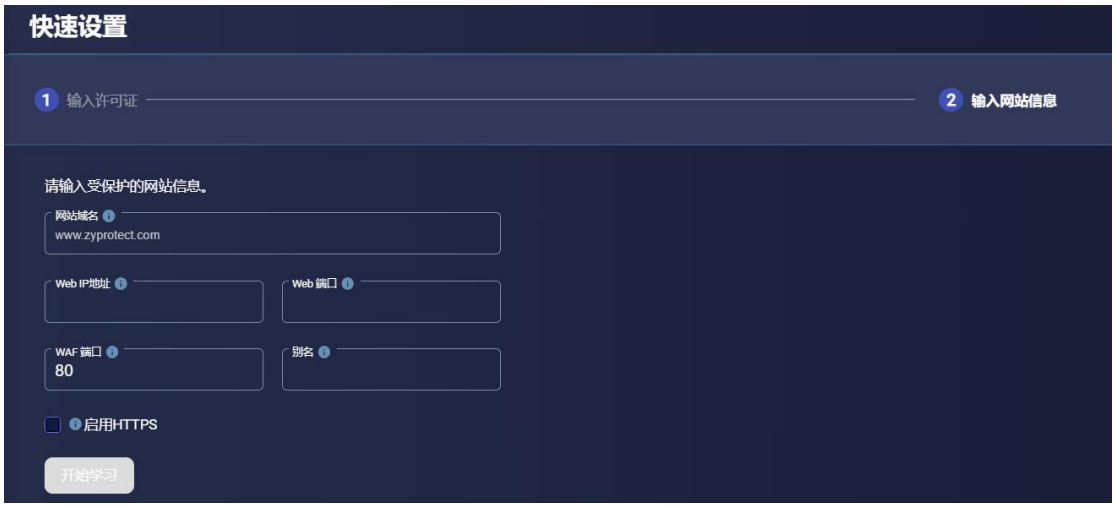

图 2-4 快速设置

AI 防护者开始安全发现 Web 应用的结构和内容。 此安全发现学习过程可能需要几分钟或几小时，具体取决于 Web 应用的复杂性。

如果需要进行监督学习（默认无监督学习），请从左侧菜单中选择学习>机器学习。需要提供一台或多台受信任计算机的 IP 地址。然后使用受信任的计算机浏览 Web 应用上的所有动态内容和所有受密码保护的内容。

注意：机器学习过程完成后，AI 防护者应在被动模式下运行，同时验证其操作。

另外，可以通过从左侧菜单中选择告警来查看告警日志。查看告警并检查任何未通过安全发现和机器学习的网站资源。 如果发现任何遗漏，可以将规则（UDP） 添加到 AI 防护者，以处理误报。 可以通过单击告警表中的告警来添加 UDP，以显示包含告警详细信息的对话框，然后单击添加 策略 按钮。

注意：无论检测/保护模式，AI 防护者将继续使用机器学习来学习 Web 应用。

3 仪表盘

仪表板可从左侧菜单访问。（图 3-1）左侧菜单可以空白区域点击展开或折叠。

图 3-1 访问仪表盘

仪表板显示有关受保护网站和 AI 防护者的信息。

3.1受保护网站

图 3-2 受保护网站

单击下拉列表会显示受 AI 防护者保护的所有网站的列表，选择后将显示该受保护网站的信息。

3.2时间范围

图 3-3 时间范围

时间范围选择下拉菜单用于指定显示多长时间范围内的数据，该下拉菜单有预制时间范围和可自定义时间范围两部分组成。

注意：仪表盘中 “过去 120 分钟内检测到的威胁”图表不受时间范围选择的影响。 显示的 CPU、内存和磁盘利用率数据是当前数据，不受时间范围选择的影响。

3.3检测到的威胁

检测到的威胁页面显示有关网站和 AI 防护者的简要信息。

检测到的威胁：AI 防护者在选定时间范围内检测到的受保护网站的威胁总数。

- **未知攻击：**一般是利用未知漏洞的攻击或尝试寻找未知漏洞的攻击总数。

- **其他攻击**：可分类的攻击总数，一般是利用已知漏洞进行的攻击。

3.4威胁历史

威胁历史显示指定时间内检测到的受保护网站的威胁数量分布。 威胁历史以柱状图显示。 每个柱状图的高度表示指定时间内检测到的威胁总数。 每个柱都用颜色编码以显示未知攻击和传统攻击。

每个栏提供的信息是：

- **未知攻击**：一般是利用未知漏洞的攻击或尝试寻找未知漏洞的攻击总数。

- **传统攻击**：可分类的攻击总数，一般是利用已知漏洞进行的攻击。

3.5威胁国家

“按国家/地区划分的威胁源”显示 AI 防护者在按威胁发起国家分类的指定时间范围内为受保护网站检测到的威胁数量。每个国家/地区的右侧是针对该国家/地区检测到的威胁计数。

3.6按 IP 地址阻止的 IP 请求

“按 IP 地址划分的威胁源”页面显示 AI 防护者在按发起威胁的 IP 地址分类的时间范围内为受保护网站检测到的威胁数量。每个 IP 地址的右侧是针对该 IP 地址检测到的威胁计数。

3.7按浏览器列出的威胁

按浏览器系列划分的威胁页面显示在指定时间范围内由 AI 防护者检测到的受保护网站的威胁百分比，该时间范围按发起威胁的浏览器类型分类。 每种浏览器类型的份额显示在

饼图中。

3.8威胁统计-周

按周统计的威胁页面显示 AI 防护者在本周时间范围内为受保护网站检测到的平均威胁数。显示当前周每天的威胁。

3.9威胁统计-天

按周统计的威胁页面显示 AI 防护者在当天时间范围内为受保护网站检测到的平均威胁数。显示天每小时的威胁。

3.10 威胁统计-过去 120 分钟

最近 120 分钟检测到的威胁页面显示最近 120 分钟内 AI 防护者检测到的受保护网站的威胁数量。不受时间范围选择的影响。

3.11 当前状态

受保护网站状态：显示了流向受保护网站的当前流量状态。

- **正常**：受保护的网站可从 AI 防护者访问。
- **异常**：AI 防护者无法访问受保护的网站。
- **zyWAF 状态**：显示 AI 防护者当前状态
- **正常**：AI 防护者运行状态正常。
- **异常**：AI 防护者运行状态异常。

流量等级：显示受保护网站的当前请求级别相对于时间范围内的平均请求级别。

- **正常**：最近一小时的流量低于该时间范围内每小时平均流量的 80%。
- **高**：最近一小时的流量等于或高于时间范围内平均小时流量的 80%。

威胁等级： 显示 AI 防护者检测到的受保护网站的当前威胁级别相对于时间范围内的平均威胁级别。

- 正常：最后一小时的威胁低于时间范围内平均每小时威胁的 80%。
- 高：最后一小时的威胁等于或高于时间范围内平均每小时威胁的 80%。

CPU 使用率： 显示当前的 CPU 使用情况。

- **正常**：当前 CPU 使用率低于 80%。
- **高**：当前 CPU 使用率等于或大于 80%。

内存使用率：显示了当前的内存使用情况。

- **正常**：当前内存使用率低于总内存的 80%。
- **高**：当前内存使用量等于或大于总内存的 80%。

磁盘使用率：显示了当前的磁盘使用情况。

- **正常**：当前硬盘使用率低于总驱动器空间的 80%。
- **高**：当前硬盘使用率等于或大于总驱动器空间的 80%。

3.12 TCP 连接

TCP 连接页面显示指定时间范围内受保护网站的 TCP 连接数。最大连接数是 AI 防护

者许可证/性能参数设置允许的最大连接数。

3.13 受保护的网站

受保护的网站页面显示所有受保护网站的网站和保护状态。

- **网站**：受保护网站的域名。（例如，www.zyprotect.com）。如果未输入域名，则会显示 IP 地址。
- **IP 地址**：显示被保护网站的 IP 地址（例如，59.110.169.239）。
- **端口**：显示被保护网站的端口（如，80）。
- **模式**：AI 防护者保护对此网站的防护模式。
    - **保护**：此网站的 AI 防护者处于保护状态，会阻止和记录威胁。
    - **检测**：此网站的 AI 防护者处于检测状态，仅记录威胁。
    - **透明**：该网站的 AI 防护者处于透明模式，AI 防护者不做任何检查，将所有流量转发到该网站。不会记录和阻止威胁。

3.14 威胁源–威胁类型

威胁源-威胁类型显示 AI 防护者在按威胁类型分类的指定时间范围内为受保护网站检测到的威胁数量。显示 TOP 10。每个栏的右侧是针对该威胁类型检测到的威胁计数。

3.15 威胁源 – IP 地址

威胁源-IP 地址页面显示在指定时间范围内由 AI 防护者检测到的受保护网站的威胁数量，按威胁源的 IP 地址分类。显示 TOP10。每个 IP 地址的右侧是针对该 IP 地址检测到的威胁计数。

3.16 威胁源 - URL

威胁源 - URL 页面显示在指定时间范围内由 AI 防护者检测到的受保护网站的威胁数量，按威胁的目标 URL 分类。 出现次数最多的 URL 显示在水平条形图中。 每个 URL 的右侧是针对该 URL 检测到的威胁计数。

3.17 系统资源使用 -CPU 使用率

系统资源使用 –CPU 使用率页面显示 AI 防护者和系统的资源使用情况。

- **WAF**：此图显示了以百分比显示的 AI 防护者的 CPU 使用率。
- **系统**：此图显示了运行 AI 防护者系统的 CPU 使用率（以百分比显示）。

3.18 系统资源使用-内存使用率

系统资源使用 - 内存使用页面显示 AI 防护者应和系统的资源使用情况。

显示的信息是：

- **WAF**：此图表显示了以百分比显示的 AI 防护者的内存使用率。
- **系统**：此图显示了运行 AI 防护者系统的内存使用率（以百分比显示）。

4 设置

设置菜单允许配置基本的 AI 防护者操作参数。

4.1 服务器设置

服务器设置显示当前已配置的受保护 Web 服务器的状态。

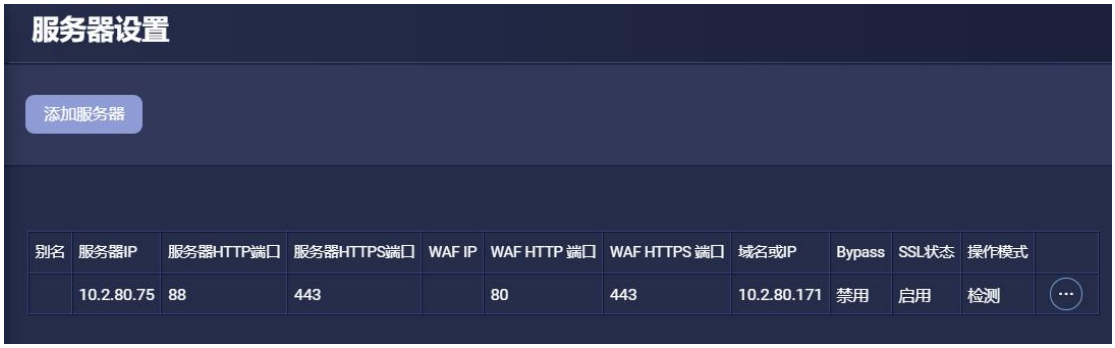

图 4-1 服务器设置

别名：受保护 Web 服务器的用户创建名称。

服务器 IP：受保护的 Web 服务器的 IP 地址。

服务器 HTTP 端口：受保护 Web 服务器应用端口号。

服务器 HTTPS 端口：受保护 Web 服务器应用端口号（加密）。

WAF IP：多 IP 地址时可以选择监听的 IP 地址。如果为空，AI 防护者将接收来自所有 IP 地址的传入请求。

WAF HTTP 端口：AI 防护者反向代理，对外提供应用服务的端口号（非加密）。

WAF HTTPS 端口：AI 防护者反向代理，对外提供应用服务的端口号（加密）。

域名或 IP：受保护 Web 服务器的域名或 IP 地址，用于校验 HTTP 头的 HOST 字段。

Bypass：如果显示为“启动”，则所有到 Web 服务器的流量都不进行检查。默认为“禁用”，表示 AI 防护者会检查所有到受保护 Web 服务器的流量。

SSL 状态：如果显示为“启用”，AI 防护者将使用 SSL 连接。默认为“禁用”，使用非 SSL（安全性较低）连接。

操作模式：如果值为“保护”，则 AI 防护者开启阻断模式，会阻断所有攻击行为。默认为为“检测”，AI 防护者仅对威胁告警提示，不会阻止。

添加服务器

服务器设置页面顶部的添加服务器按钮用于创建新的受保护 Web 服务器。

图 4-2 添加服务器

协议：必须指定 AI 防护者和 Web 服务器之间使用的传输协议。 默认值：HTTP。

别名：可以输入信息名称。 此名称将由 AI 防护者显示以识别此服务器。 默认值：无。

启用透明管理：选中后，流量将不经检查直接传递到 Web 服务器。勾选该选项后，将不会产生告警信息。 默认值：禁用。

注意：在透明模式中运行时，AI 防护者不会使用机器学习来学习网站。

隐藏服务器信息：选中后，将会隐藏受保护 Web 服务器信息。Web 服务器信息包括服务器类型、版本号和操作系统。 默认值：启用

添加 X-Forwarded-Proto 头：选中后，AI 防护者将使用源连接的原始协议添加 X-Forwarded-Proto 头。一般在 HTTPS 流量转换为 HTTP 流量时使用。 默认值：禁用。

保护模式：此选项指定 AI 防护者保护模式。 可用的保护模式有：

- **保护：**威胁被阻止和记录。
- **检测：**威胁仅被记录，不阻止。

注意：在两种模式下，AI 防护者都会持续学习受保护应用。

Web IP：受保护 Web 服务器的地址（域名或 IP）。 默认值：空。

Web 端口：受保护网站 HTTP 应用的服务端口（TCP）。 默认值：80。

WAF IP： AI 防护者监听的 IP 地址 默认值：空。

WAF 端口：AI 防护者反向代理提供服务的 TCP 端口。 默认值：80。

绑定 IP：指定 AI 防护者在使用多网卡时，使用哪个网卡与受保护 WEB 服务器连接。如果为空，则依赖系统通信规则。 默认值：空。

客户端主机验证：启用后，AI 防护者将验证流量中主机头 HOST 字段是否与指定的域名或 IP 地址匹配。 默认值：启用。

域名或 IP 地址：指定验证访问受保护网站流量中 HOST 字段的域名或 IP，可填写多个

（如果值有多个，一个匹配即可通过）。 默认值：空。

SSL 设置

加密到 Web 服务器：选中后，AI 防护者将使用加密方式将数据转发给受保护 Web 服务器。 默认值：启用。

将 HTTP 流量重定向到 HTTPS 端口：选中后，AI 防护者会将浏览器发送的 HTTP 流量重新封装为 HTTPS 流量发送到受保护 Web 服务器。 默认值：禁用

WAF IP：AI 防护者应该监听 HTTPS 流量的 IP 地址。 默认值：空。

WAF 端口：用于接收 HTTPS 流量的 TCP 端口。 默认值：443。

Web 端口：受保护 Web 服务器的 TCP 端口，用于接收 HTTPS 流量。 默认值：443。

证书文件：AI 防护者用于解密 HTTPS 流量的 X.509 证书文件。 X.509 证书是一个 ASCII PEM 编码 (Base64) 格式的文件。 PEM 证书通常具有 .pem 或 .cer 的扩展名。 默认值：空。

证书密钥文件：证书文件对应的私钥。 不支持需要密码的密钥文件。 私钥通常具有 .key 的扩展名，并且必须是 Base64 编码的 ASCII 文件。 默认值：空。

CA 证件文件：证书的 CA 文件。 此文件还必须采用 ASCII PEM 编码 (Base64) 格式。 默认值：空。

4.2高级功能

高级功能菜单页面允许配置高级功能参数。

注意：该设置支持全局策略或指定受保护网站策略，通过 

和 

来标识策略是否生效。

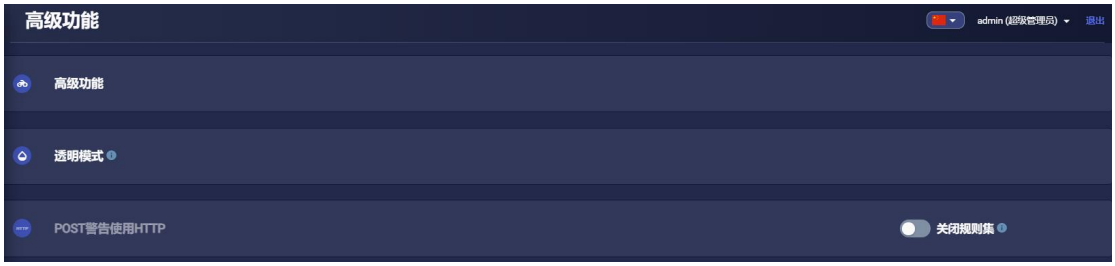

图 4-3 高级功能

4.2.1 高级功能

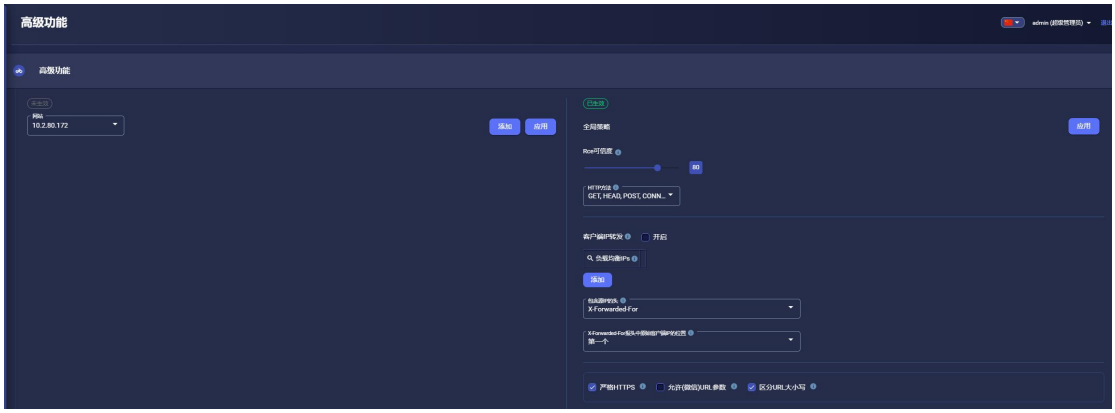

图 4-4 高级功能

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

RCE 可信度：RCE 可信度介于 10 和 100 之间。10 校验最简单，100 校验最严格。 默认

值：80。

HTTP 方法：AI 防护者允许的 HTTP 方法。 默认值：GET、HEAD、POST、CONNECT。

客户端 IP 转发：勾选“开启”后，AI 防护者将客户端 IP 或本机（反向代理）IP 添加到 X-Forwarded-For 字段中。 默认值：禁用。

显示列表

负载均衡 IPs：勾选 启用客户端 IP 转发 后，来自列表中 IP 的请求，都会默认是负载均衡设备转发来的流量，AI 防护者会将 X-Forwarded-For 字段中的客户端 IP（而非数据包的源 IP）作为日志中的源 IP 默认值：空。

包含源 IP 的头：将请求的源 IP 写入选择的 Header 字段，该选项支持自定义。 默认值：X-Forwarded-For。

X-Forwarded-For 报头中原始客户端 IP 的位置：允许设置源 IP 在 X-Forwarded-For 中的位置。 默认值：第一个。

严格 HTTPS：勾选后启用，受保护 Web 服务器使用 HTTPS 协议时，将阻止基于 HTTP 请求。 默认值：启用。

允许（微信）URL 参数：勾选后启用，AI 防护者将加强引擎识别微信 URL 参数的能力。默认值：禁用。

区分 URL 大小写：勾选后启用，URL 区分大小写。 默认值：启用。

4.2.2 透明模式

图 4-5 透明模式

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

显示列表

管理 IP 地址：来自这些 IP 地址的请求将不会被检查，直接转发到网站（此功能常用于对应用的漏洞扫描或测试）。

4.2.3 Post 告警使用 HTTP

图 4-6 Post 告警使用 HTTP

开启：启用后，每当创建告警时，通知（XML 格式）将通过 HTTP 协议发送到指定的 IP。

默认值：禁用。

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有收保护网站。

告警原因：多选列表，勾选后，将发送已勾选类型的告警。当未选择告警原因时，将发送所有告警。默认值：未勾选。

服务器名称：告警接收服务器的域名或 IP 地址。默认值：空。

服务器端口：告警接收服务器的端口。默认值：80。

来自：用于说明告警来源（用于注释，方便日志平台筛选）。默认值：空。

URL：告警接收服务器接收告警的 URL。默认值：空。

4.3规则设置

规则菜单页面可配置定制化规则。

注意：该设置支持全局策略或指定受保护网站策略，通过 

和 

来标识策略是否生效。

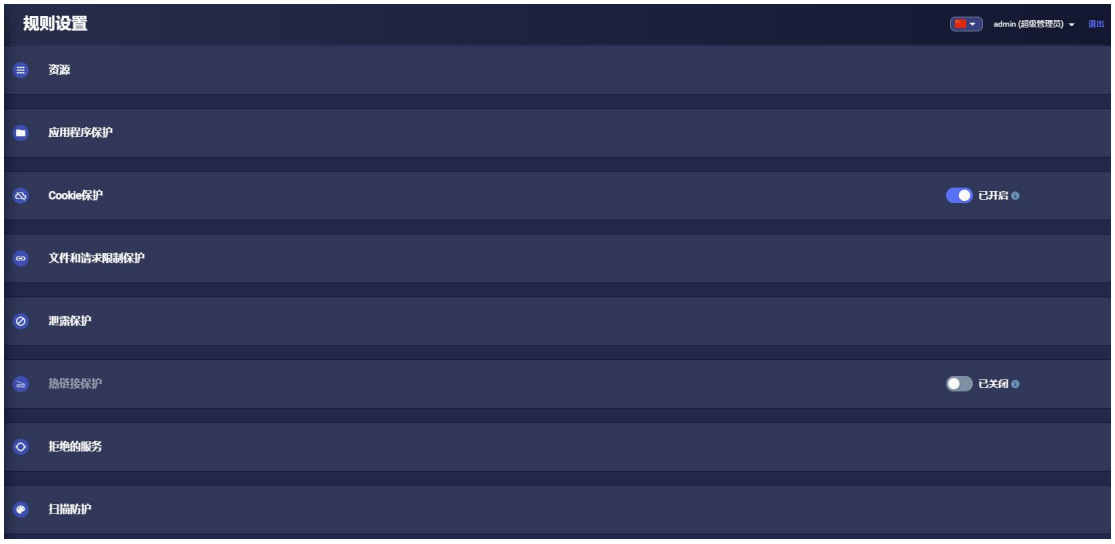

图 4-7 规则设置

注意：该设置支持全局策略或指定受保护网站策略，通过 

和 

来标识策略是否生效。

4.3.1 资源

可以自定义受保护网站上的 UDP（URL 白名单）。

图 4-8 资源

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

显示列表

URI 路径：允许的 UDP。默认： “/” 。

进入节点：启用或禁用 UDP。 默认值：均启用。

仅允许 HTTPS：选中后，这个 URI 仅允许 HTTPS 连接。 默认值：禁用。

区分大小写：选中后，将区分 URI 大小写。 默认值：禁用。

正则表达式：启用后，允许以正则表达式方式设置 URI。 默认值：禁用。

UDP	允许	阻止
/default.asp\?var=*	/default.asp?var=123 /default.asp?var=123&var2=456	/default.asp /default.asp?x=123 /default.aspXvar=123
/default.asp\?var=##	/default.asp?var=12	/default.asp?var=1 /default.asp?var=123 /default.asp?var=ab
/default.asp\?v1=*&v2=#*&v3=???	/default.asp?v1=1a&v2=12&v3=abc /default.asp?v1=a&v2=34&v3=123	/default.asp?v1=1a&v2=1a&v3=1a

图 4-9 使用正则表达式的文件路径 URL 示例

4.3.2 应用程序保护

可以在这些页面中配置 AI 防护者对表单、XML 数据和 JSON 数据的保护设置。

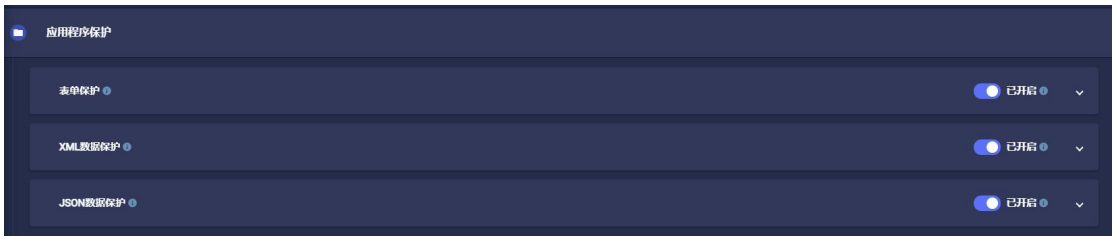

图 4-10 应用程序保护

表单防护

使用表单验证以防止注入攻击。 增加“表单保护”的列表，可以允许对指定 URI 下的表单、字段名添加白名单。

图 4-11 表单防护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

全局策略开启：确定是否将对文本表单上输入的数据进行验证。 默认值：启用。

表单注入：HTML 支持三种类型的文本输入表单：文本、文本域、和密码。对于每种类型的文本输入表单，可以单独指定保护动作。

- **操作**：当文本表单的数据未通过验证时，将执行指定的操作。 默认值：阻止。
    - **阻止**：阻止向网站提交表单。
    - **删除**：从输入的数据中删除违规的特殊字符，然后将过滤后的表单提交到网站。
- **告警**：选中后，当文本表单的数据未通过验证并采取所选操作时，将记录告警。默认值：启用。

通过向表单提供 URL 列表，可以允许未经验证的表单输入到受保护网站上的指定表单。不会验证对表中列出的表单字段的输入。

URI：禁用验证的一个或多个表单 URI。URL 中支持通配符。 默认值：空。

表单名称：禁用验证的表单名称。 默认值：空。

字段名称：表单中禁用验证的字段名称。 默认值：空。

字段类型：表单中禁用验证的字段类型。 默认值：任何字段类型。

XML 数据保护

将对请求 Payload 数据进行验证，以防止注入攻击。 可以允许对指定 URI 下的 XML 数据添加白名单。

图 4-12 XML 数据保护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

全局策略开启：确定是否将执行 XML 数据威胁检测。默认值：启用。

告警：选中并检测到 XML 数据的威胁时，将生成告警。默认值：启用

阻止：选中并检测到 XML 数据的威胁时，将阻止请求。默认值：启用

通过提供具有根元素名称和字段名称的 URL 列表，可以允许受保护网站上的 URL 未经验证的数据输入。输入将不会被验证。

URI：禁用 XML 数据验证的一个或多个 URI。URL 中支持通配符。默认值：空。

根元素名称：禁用数据验证的最外层 XML 元素的名称。默认值：空。

字段名称：根元素中禁用数据验证的字段名称。默认值：空。

JSON 数据保护

将对请求 payload 中的 JSON 数据进行验证，以防止注入攻击。可以允许对指定 URI 下的 JSON 数据添加白名单。

图 4-13 JSON 数据保护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

全局策略开启：确定是否将执行 JSON 数据威胁检测。 默认值：启用。

告警：选中并检测到对 JSON 数据的威胁时，会生成告警。 默认值：启用

阻止：选中并检测到对 JSON 数据的威胁时，将阻止请求。 默认值：启用

通过提供具有顶级对象名称和字段名称的 URL 列表，可以允许受保护网站上的 URL

未经验证的数据输入。输入将不会被验证。

URI：禁用 JSON 数据验证的一个或多个 URI。URL 中支持通配符。 默认值：空。

顶级对象名称：禁用数据验证的最高级别 JSON 对象 XML 的名称。 默认值：空。

字段名称：JSON 对象中禁用数据验证的字段名称。 默认值：空。

4.3.3 Cookie 保护

图 4-14cookie 保护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

全局策略开启：确定是否将执行 cookie 验证。 默认值：启用。

行为：当 cookie 验证失败时采取指定的行动。 默认值：删除。

- **删除**：选择时，不会拒绝没有正确签名的 cookie 请求，而是将 cookie 传递到网站（删除不正确的 cookie 内容）。
- **阻止**：选中后，在客户端请求中收到的任何没有正确签名的 cookie 都将被拒绝，

并返回 HTTP 代码 400–错误请求。

Cookie 保护延迟：初次部署后启用 cookie 验证时使用此选项。在过渡期间，将允许无法验证的 cookie 属性和值。

- **启用/禁用**：确定在指定时间段内是否允许验证失败的 cookie。 默认值：启用。
- **天数和小时数**：允许未通过验证的 cookie 的天数和小时数。 默认值：6 天。

通过提供 cookie 名称列表，可以在受保护的网站上允许未经验证的 cookie 输入。输入将不会被验证。

Cookie 名称：不会验证的 cookie 名称。

4.3.4 文件和请求限制保护

可以在这些页面中配置 AI 防护者文件上传、下载和请求头保护的设置。

图 4-15 文件和请求限制保护

文件上传限制

图 4-16 文件上传限制

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

全局策略开启：确定文件上传（到网站）限制是否处于活动状态。 默认值：禁用。

文件名验证：启用后，文件名仅限于由 Unicode 字母和数字类别以及 ASCII 特殊字符（连字符、下划线、空格和句点）组成。默认值：启用。

最大长度：定义文件名（包括扩展名）中允许的最大字符数。 默认值：255。

特殊字符：文件名中允许的特殊字符列表。 默认值：无。

允许的文件上传：选中后，定义允许的文件扩展名。 通过单击“(...)”按钮，可以在显示的列表中添加和删除单个文件扩展名。 这种白名单方法是使用文件上传限制时的推荐策略。默认值：启用。

拒绝文件上传：选择后，拒绝文件类型列表定义被阻止的文件扩展名。 通过单击“(...)”

按钮，可以在显示的列表中添加和删除单个文件扩展名。 使用文件上传限制时，不建议使用这种应用文件上传限制的黑名单方法。 默认值：禁用。

文件下载限制

图 4-17 文件下载限制

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

全局策略启动：确定文件下载（从网站）限制是否处于活动状态。 默认值：禁用。

文件名验证：启用后，文件名仅限于由 Unicode 字母和数字类别以及 ASCII 特殊字符（连字符、下划线、空格和句点）组成。默认值：启用。

最大文件名长度：定义文件名中允许的最大字符数（包括扩展名）。 默认值：255。

特殊字符：文件名中允许的特殊字符列表。 默认值：无。

文件下载白名单：选中后，允许的文件类型列表定义允许的文件扩展名。 通过单击“(...)”按钮，可以将文件扩展名添加到显示的列表中或从中删除。 这种白名单方法是使用文件下

载限制时的推荐策略。 默认值：启用。

文件下载黑名单：选择后，“拒绝文件类型”列表定义被阻止的文件扩展名。 通过单击“(...)”按钮，可以将文件扩展名添加到显示的列表中或从中删除。 使用文件上传限制时，不建议使用这种应用文件上传限制的黑名单方法。 默认值：禁用。

选择文件下载白名单时，文件下载白名单列表显示在显示列表中。 选择文件下载黑名单时，文件下载黑名单列表显示在显示列表中。 每个列表都是独立的。

请求和请求头保护

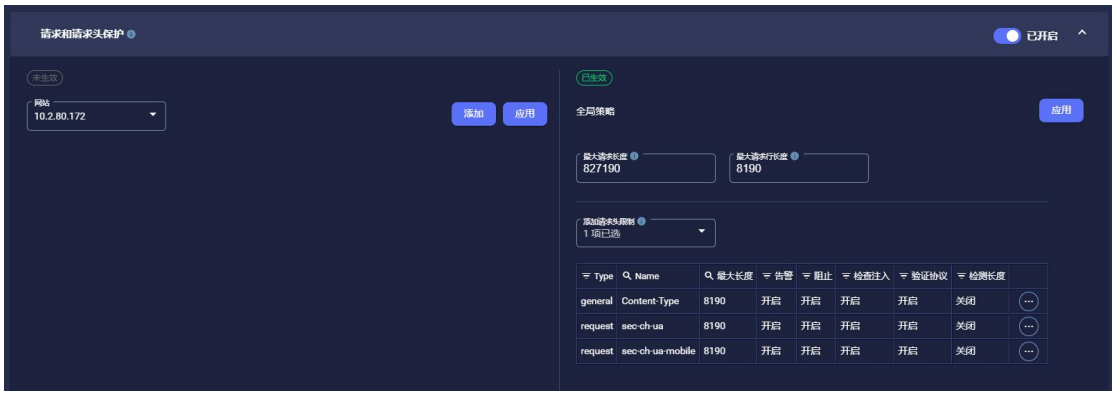

图 4-18 请求和请求头保护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

全局策略开启：确定文件请求和头保护是否处于活动状态。 默认值：启用。

最大请求长度：请求中允许的最大字符数。 默认值：827190。

最大请求行长度：请求头中允许的最大字符数。 默认值：8190。

添加头限制，HTTP 头中允许的最大字符数由头类型指定。 可以使用为每种类型设置

的最大字符数来定义多种头字段类型的限制。

显示列表包含将受保护的请求配置。

4.3.5 泄漏保护

AI 防护者数据泄露、URL 泄露保护可以在这些页面中进行配置。

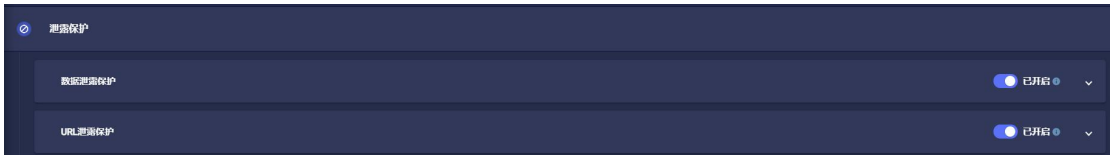

图 4-19 泄漏保护

数据泄露保护

图 4-20 数据泄露保护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

全局策略开启：确定数据泄漏保护是否处于活动状态。 默认值：禁用。

显示列表

名称和值：用于输入数据泄漏保护将匹配的数据。 默认值：空

告警：选中后，数据泄漏将生成告警。 默认值：禁用。

阻止：选中后，将阻止数据泄漏。 默认值：禁用。

区分大小写：选中后，将使用区分大小写的匹配来检测数据泄漏。 默认值：禁用。

正则表达式：选中后，值的内容将按照正则表达式识别。 默认值：禁用。

点击测试 按钮将测试正则表达式内容是否可以匹配上数据。

URL 泄漏保护

图 4-21 URL 泄漏保护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

已开启：确定 URL 泄漏保护是否处于活动状态。 默认值：禁用。

显示列表

名称和值用于输入 URL 泄漏保护将匹配的数据。 默认值：空

告警：选中后，URI 泄漏将生成告警。 默认值：启用。

阻止：选中后，将阻止 URL 泄漏。 默认值：启用。

区分大小写：选中后，将使用区分大小写的匹配来检测 URL 泄漏。 默认值：禁用。

正则表达式：选中后，值的内容将按照正则表达式识别。 默认值：禁用。

点击测试 按钮将测试正则表达式内容是否可以匹配上数据。

4.3.6 热连接保护

图 4-22 热连接保护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

策略开启： 确定是否阻止跨域的客户端请求。允许的网站域列表中的网站域不会被阻止。

默认值：禁用。

允许的热连接域名： 不会被阻止热链接到受保护 Web 应用的网站域列表。 默认值：空。

受保护的文件类型：启用热链接文件保护，禁止其他网站的跨域热连接文件类型。 通过单击 (...) 按钮，可以在此列表中添加和删除文件扩展名。 只有此列表中的文件扩展名会受到保护，以免被盗链。

4.3.7 拒绝的服务

可以在这些页面中配置 AI 防护者拒绝的服务保护的设置。

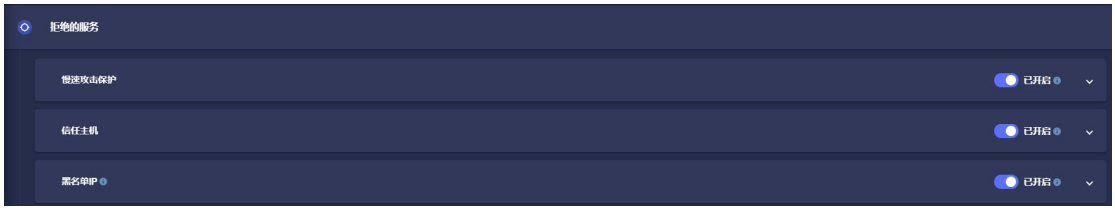

图 4-23 拒绝的服务

慢速攻击保护

慢速攻击涉及看似合法的流量以非常慢的速度到达。这是一种拒绝服务攻击。

图 4-24 慢速攻击保护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

策略开启： 确定慢速攻击保护是否处于开启状态，以及是否将对已达到阈值的源 IP 地址采取选定的操作。 默认值：启用。

策略动作： 如果达到 HTTP 超时阈值或数据包超时阈值，将对源 IP 地址执行所选操作。默认值：阻止。

HTTP 超时阈值（秒）：HTTP 超时计算周期。 默认值：60。

TCP 超时阈值（秒）：TCP 数据包超时计算周期。 默认值：7。

监控周期（秒）：检查 HTTP 事务或 TCP 数据包是否已达到超时阈值的频率。 默认值：

100。

信任主机

图 4-25 信任主机

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

启用策略：会阻止来自受信任 IP 的恶意活动，但不会生成告警。 此功能旨在用于授权的渗透测试。 默认值：禁用。

信任 IP： 受信任主机的一个或多个 IP 地址。 通过单击 (...) 按钮，可以将受信任的 IP 地址添加到此列表中或从中删除。 默认值：127.0.0.1

IP 黑名单

图 4-26 IP 黑名单

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

全局策略：在全局策略页面中输入的设置将应用于所有受保护网站。

黑名单 IP： 将被阻止的 IP 地址列表。 默认值：空。

注意：IP 黑名单可以通过扫描防护自动添加也可以通过管理员手工添加（开启扫描防护功能后，同时需要开启 IP 黑名单功能）。

4.3.8 扫描防护

图 4-27 扫描防护

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

开启/关闭：确定扫描仪保护是否处于活动状态。 默认值：禁用。

计时周期（秒）：查找正在运行渗透或漏洞扫描的可疑 IP 的频率（以秒为单位）。 默认：300。

探测时间范围（秒）：检查疑似运行渗透或漏洞扫描的 IP 的告警时间范围（以秒为单位）。默认值：300。

告警频率：计时周期内，一个 IP 产生告警频率的阈值。 默认值：50。

注意：达到告警频率阈值的 IP 将被自动的添加到 IP 黑名单中。

4.4HTTP 响应页面

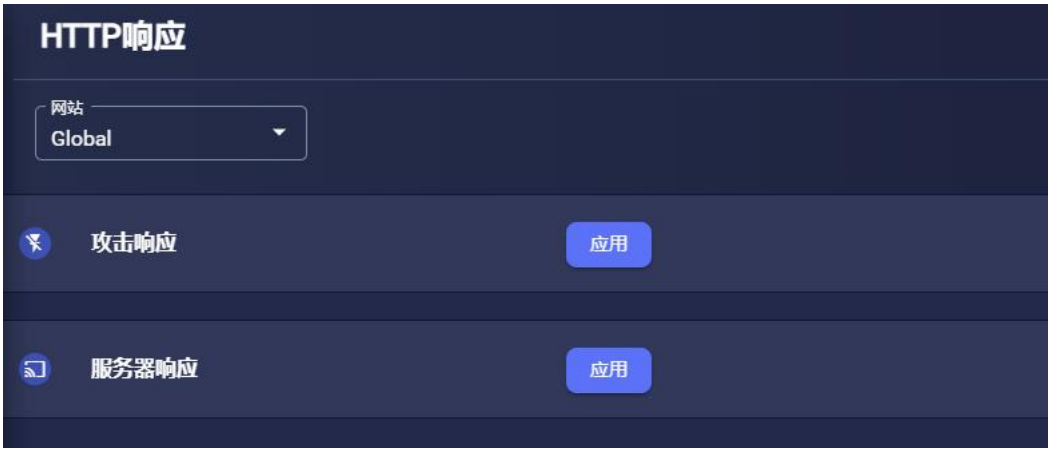

图 4-28 HTTP 响应页面

网站：此下拉菜单用于选择一个受保护网站，配置的策略仅对选择的网站生效。

攻击响应

图 4-29 攻击响应

400 错误的请求

开启/关闭：当收到 400 错误时，客户端是否将重定向到指定的 URI。 默认值：禁用。

URI： 400 错误的自定义页面的 URI。 默认值：空

403 禁用错误

开启/关闭：当收到 403 错误时，客户端是否将重定向到指定的 URI。 默认值：禁用。

URI： 403 错误的自定义页面的 URI。 默认值：空。

405 方法不允许

开启/关闭：确定当收到 405 错误时，客户端是否将重定向到指定的 URI。 默认值：禁用。

URI： 405 错误的自定义页面的 URI。 默认值：空。

服务器响应页面

图 4-30 服务器响应页面

启用 4xx 服务器备用响应

开启/关闭：所有 4xx 错误响应，AI 防护者仅返回状态代码和简单描述给客户端（防止敏感信息泄漏）。 默认值：禁用。

开启 5xx 服务器备用响应

开启/关闭： 确定对于所有 5xx 错误响应，AI 防护者仅返回状态代码和简单描述给客户端（防止敏感信息泄漏）。 默认值：禁用。

5 告警

告警页面显示由 AI 防护者生成的告警。

告警可能是可见的或隐藏的。 默认情况下，所有告警都是可见的，直到被用户标记为隐藏。默认所有可见状态的告警都显示在表格中。

图 5-1 告警

网站： 来自所选网站的告警将显示在表格中。

时间范围：指定查询告警的时间范围。

告警描述：过滤告警详情中的关键字。

分组：告警可以按远程 IP 或 URL 去重后进行分组。 默认值：禁用。

状态：过滤告警状态，默认为可见。 默认值：可见。

自动刷新：设置告警刷新时间，新告警将添加到列表中。 默认值：关闭

国家： 只有与触发告警的请求的远程（源）IP 地址所在国家/地区相匹配的告警才会显示在表格中。

远程 IP：按远程 IP 过滤告警。

更多过滤条件

图 5-2 更多过滤条件

更多过滤器页面用于进一步筛选告警。

告警原因：从攻击分类中筛选告警原因。

告警子原因：从攻击分类中筛选告警子原因。

请求 URI：通过 URI 筛选告警，点击正则表达式按钮，将允许使用正则表达式进行过滤。

告警

图 5-3 告警表单

注意：单击列标题将按列的内容对列表进行排序。 再次单击将在升序和降序值之间切换排序顺序。

刷新：重置筛选条件，更新显示告警的内容。

导出 CSV：此按钮会将所有勾选的告警导出到 CSV 文件中，并自动通过浏览器下载。

隐藏：此按钮将隐藏所勾选的告警。

添加策略：此按钮将根据告警创建 UDP（白名单）。

时间：告警产生的日期和时间。

远程 IP：触发告警请求的远程（源）IP 地址。

国家：触发告警请求的远程（源）IP 地址所在的国家/地区。

告警原因：告警的威胁类别。

告警子原因：告警的威胁子类别。

请求 URI：触发告警时请求的网站 URI。

告警描述：告警的描述。

WAF HTTP 状态码：触发此告警时 WAF 返回的 HTTP 错误代码。

WAF 服务 HTTP 代码：触发此告警时 Web 服务器返回的 HTTP 错误代码。

搜索： 此按钮用于显示搜索页面，用于根据列中的条件限制表中显示的告警。

6 报告

现在报告按钮用于进入立即生成报告的页面。计划报告按钮用于进入按计生成报告的页面。

现在报告

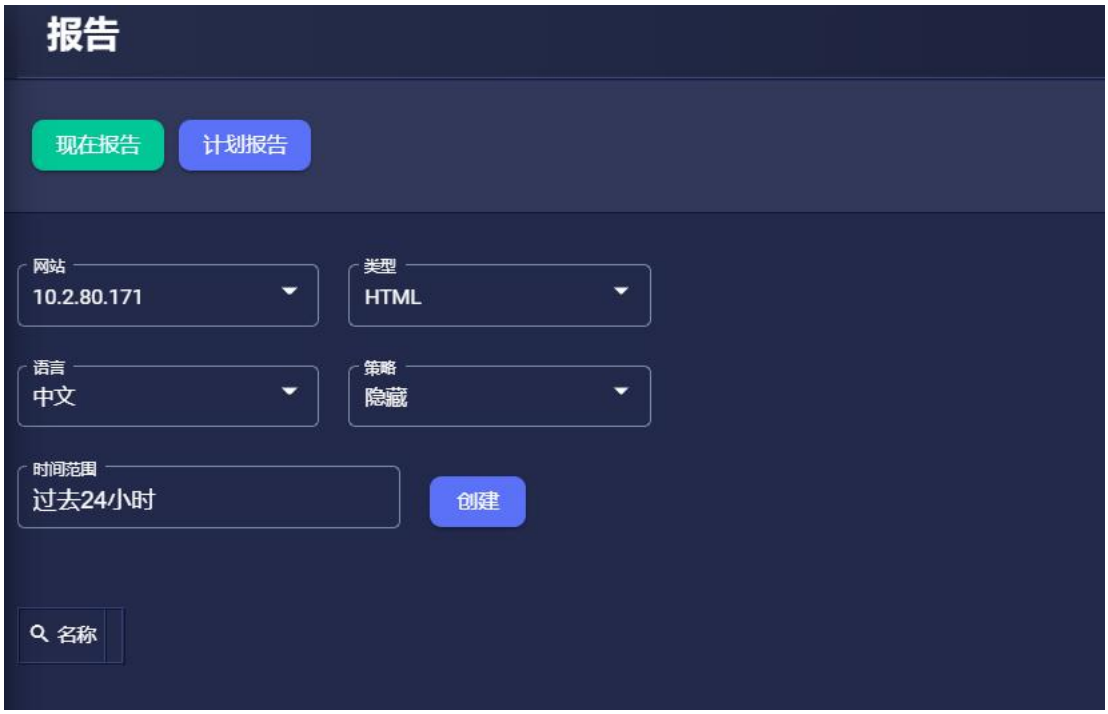

图 6-1 现在报告

网站：所选网站的数据用于生成报告。

类型：选择报告文件是 HTML 或 PDF 格式。

语言：选择报告内容是英文还是中文。

策略：选择是否将 AI 防护者策略（设置）包含在报告文件中。

时间范围：选择指定时间范围的告警用于生成报告。

名称：已生成的报告的文件名，可供查看和下载。（文件名包括受保护网站的 IP 地址和端口+报告生成的时间+报告使用的语言+和报告格式。）

(...)：单击此按钮并选择“删除”将删除报告。

计划报告

图 6-2 计划报告

添加计划：此按钮将创建报告生成计划。

名称：计划报告的用户定义名称。

网站：来自所选网站的数据将包含在预定报告中。

语言：此按钮选择预定报告文件是英文或中文。

类型：选择计划的报告文件是 HTML 或 PDF 格式。

报告时间：选择创建计划报告的时间。

报告频率：选择创建计划报告的频率。

策略：选择是否将 AI 防护者策略（设置）包含在计划报告中。

星期/日：当报告频率设置为每周或每月时，将选择某个固定时间生成报告。

收件人：单击添加按钮允许添加收件人电子邮件地址。划报告的副本被保留并显示在计划报告的历史记录表中。

邮件设置：设置电子邮件服务器相关配置。

测试邮件按钮：此按钮将立即发送一封验证电子邮件。

主题：设置计划报告邮件的主题 默认值：zyWAF。

安全邮件：选中后，将使用加密协议发送电子邮件。 默认值：禁用。

服务器地址：邮件服务器的 IP 地址。 默认值：空。

服务器端口：邮件服务器端口。 默认值：25。

邮件地址：发件人的电子邮件地址。 默认值：空。

邮件密码：发件人的电子邮件服务器的密码。 默认值：空。

证书文件：使用安全电子邮件时要使用的证书文件。 默认值：空。

证书 Key 文件：启用安全邮件 时要使用的证书对应的私钥。 默认值：空。

计划列表： 此表是已创建的计划报告任务的列表。

名称：已创建的计划报告的自定义名称。

(...)：单击此按钮允许编辑和删除以前创建的计划报告任务。

生成报告历史：此表是所有已生成计划报告的列表。

名称：已生成报告的自定义名称。

时间：通过电子邮件发送此报告文件的日期和时间。

收件人：用于接收此报告文件的电子邮件地址。

状态：　此报告文件的电子邮件发送操作的状态。

(...)：单击此按钮并选择“删除”将删除此报告文件。

7 学习

学习菜单用于启用机器学习和安全发现。

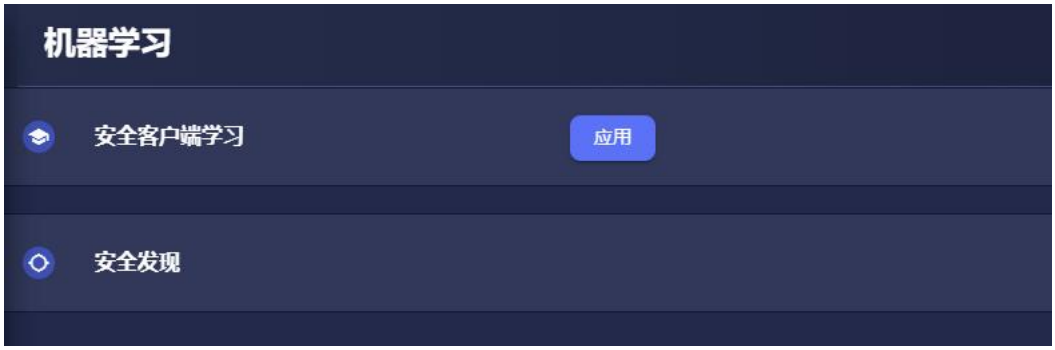

图 7-1 机器学习

7.1机器学习

7.1.1 安全客户端学习

安全客户端学习功能是无监督学习的补充。在正常运行中，AI 防护者从受保护 Web 应用的响应中不断学习网站的逻辑。启用安全客户端学习后，AI 防护者也会从指定安全学习 IP 地址的 HTTP 请求中学习网站的逻辑。 来自安全学习 IP 的所有 HTTP 请求都被认为是可信请求。

图 7-2 安全客户端学习

安全学习开启/关闭：确定安全客户端学习的状态。 默认值：关闭。

安全学习 IP 地址：可信 IP 地址列表。 默认值：127.0.0.1。

注意：*无法删除默认的安全学习 IP127.0.0.1。*

(...)：单击此按钮将从列表中添加或删除 IP 地址。

7.1.2 安全发现

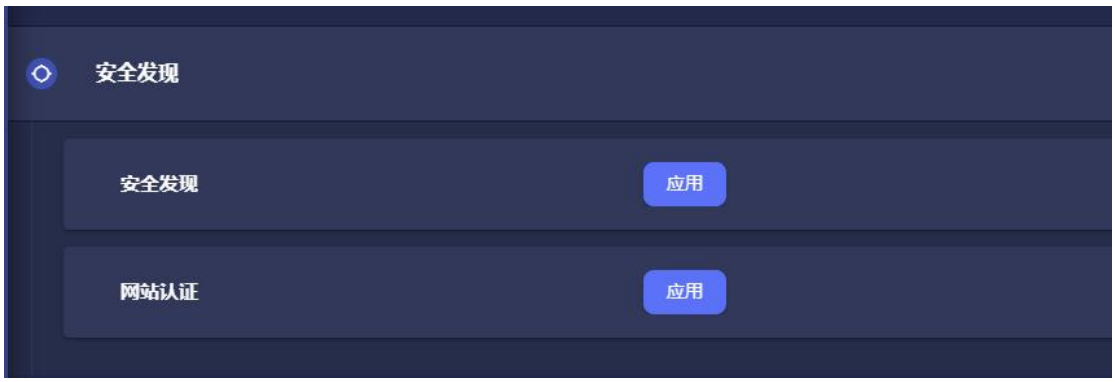

图 7-3 安全发现

安全发现

安全发现是自动化机器学习功能。启用安全发现后，AI 防护者还将从内置网络爬虫的 HTTP 请求中学习网站的逻辑。

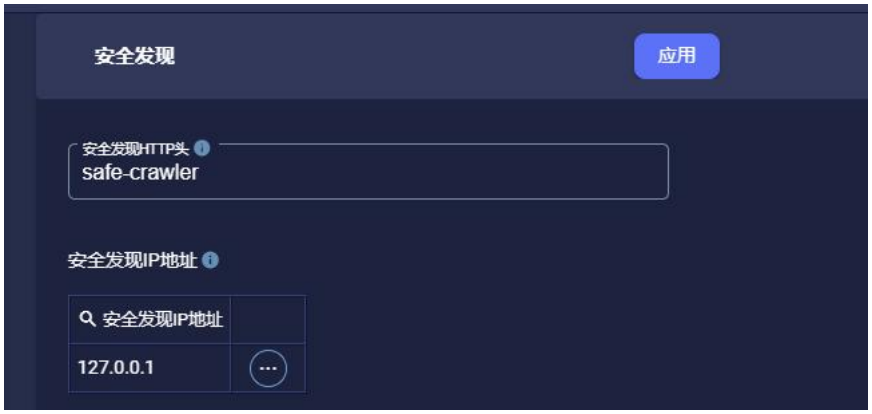

图 7-4 安全发现

安全发现 HTTP 头：安全发现爬虫使用的标识 ID。AI 防护者不会为带有此标识的流量生成告警。 默认值：safe-crawler。

安全学习 IP：安全发现爬虫将使用的 IP 地址。这些 IP 地址的流量不会生成告警。

(...)：单击此按钮将从列表中添加或删除安全发现 IP 地址。

网站验证

图 7-5 网站验证

网站：此下拉菜单用于选择安全发现爬虫将开始爬取的网站。

基本 URL 路径：安全发现爬虫将使用的网站的起始 URL 路径。 默认： /

认证方式：当受保护网站需要凭证时，可选择认证方式和输入登录凭证。 默认值：无

7.2安全发现

安全发现状态页面显示安全发现爬虫在学习网站期间返回的数据。

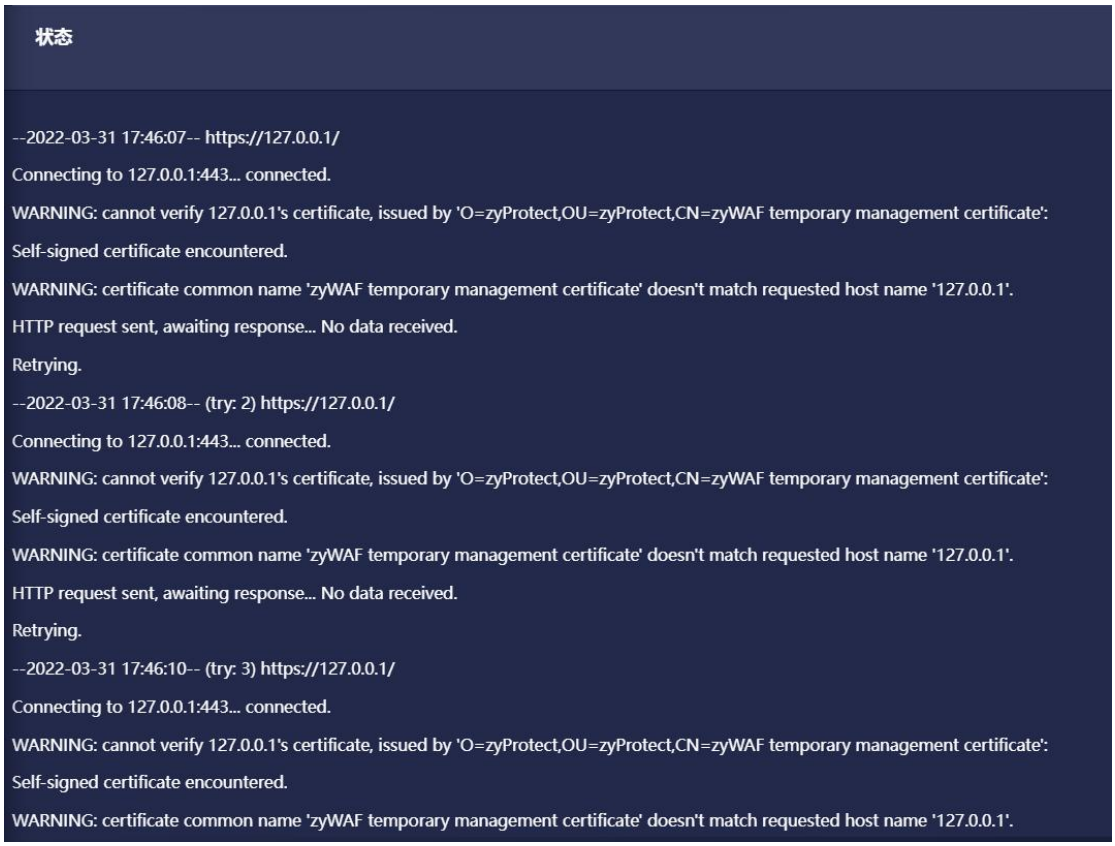

图 7-6 安全发现

网站：此下拉菜单用于选择安全发现爬虫将开始爬取的网站。

开始：单击后，安全发现爬虫将开始重新爬取所选网站。

安全爬虫参数：将显示安全发现爬虫将使用的参数。

状态：显示来自在爬行期间创建的安全发现爬虫的状态消息。

8 系统

系统菜单项提供系统相关功能的设置。

8.1 性能优化

性能调整菜单用于配置性能优化、Cookie 保留、表单保留和资源保留的参数设置。

图 8-1 性能优化

8.1.1 性能优化

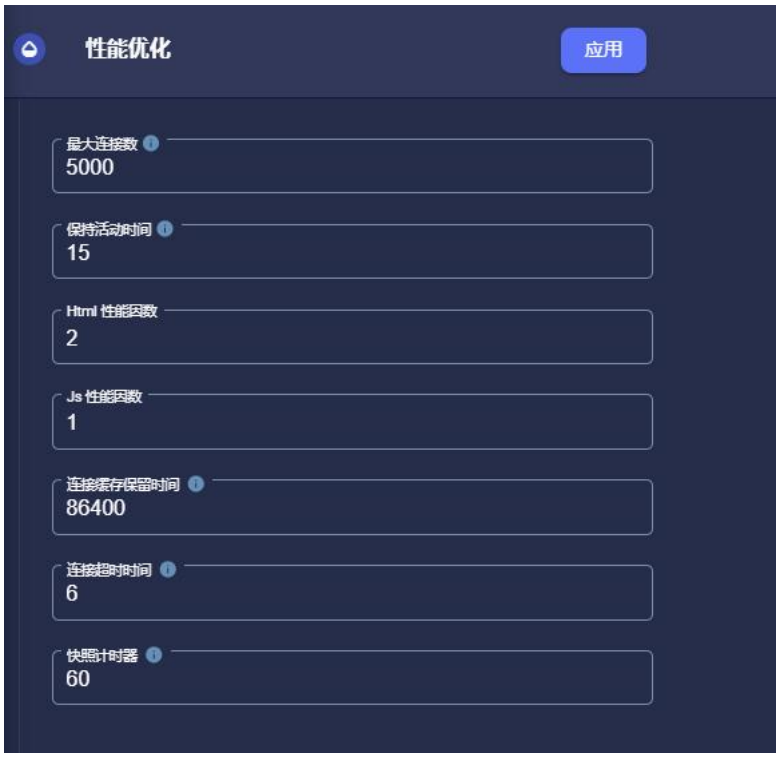

图 8-2 性能优化

最大连接数：允许的最大同时请求数。 默认值：5000。

保持活动时间 （秒）：在关闭连接之前等待后续请求的秒数。 默认值：15。

Html 性能因数：用于处理流量的线程数。 默认值：2。

Js 性能因数：用于处理 js 的线程数。 默认值：2

连接缓存保留时间：保留超时 http 连接缓存的秒数。 默认值：86400。

连接超时：等待建立连接的秒数。 默认值：6。

快照计时器：将内存中的学习数据保存到磁盘的周期（秒）。 默认值：60。

8.1.2 Cookie 保留

图 8-3cookie 保留

开启/关闭：确定 cookie 保留时间（启用时）。 默认值：启用 / 15 天 / 0 小时。

8.1.3 表单保留

图 8-4 保单保留

开启/关闭：确定表单保留时间（启用时）。 默认值：启用 / 3 天 / 0 小时。

8.1.4 资源保留

图 8-5 资源保留

开启/关闭： 确定资源保留时间（启用时）。 默认值：启用 / 30 天 / 0。

8.2仪表板参数

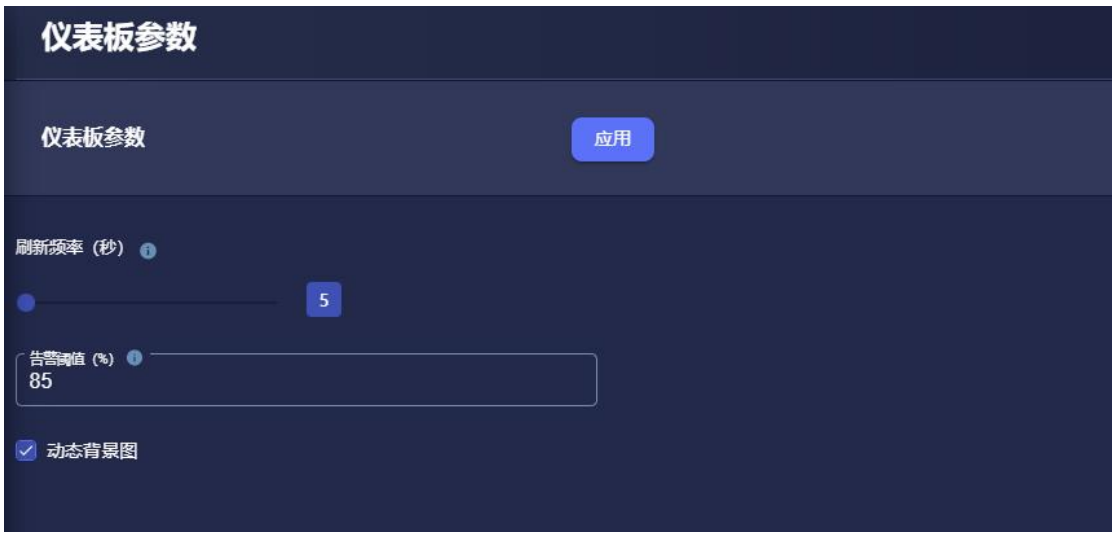

图 8-6 仪表板参数

利用率刷新频率（秒）： CPU、内存和磁盘利用率数据在仪表板上更新的频率（以秒为单位）。 默认值：5。

告警阈值 (%)：仪表板上显示 CPU、内存和磁盘利用率告警的阈值。 默认值：85。

动态背景图： 启用后，仪表板将显示动态背景。 默认值：启用。

8.3重启

图 8-7 重启

点击**确定**重启 AI 防护者。 单击**取消**退出对话框而不重新启动。

8.4备份还原

备份和恢复提供了一种将一个 AI 防护者节点的设置和网站学习转移到另一个 AI 防护者节点的方法。 它还可以用于为存档目的进行备份。

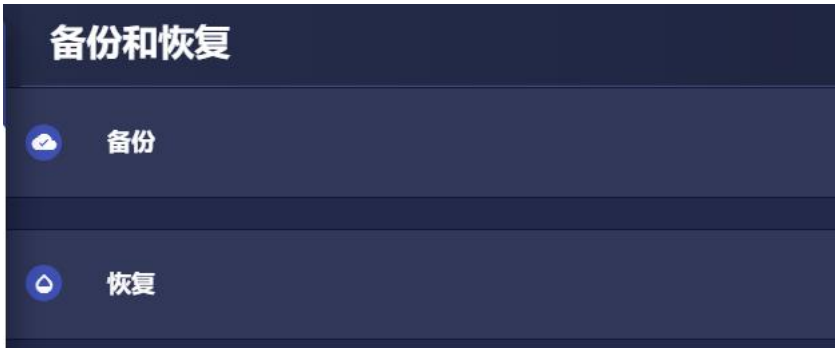

图 8-8 --备份和恢复

8.4.1 备份

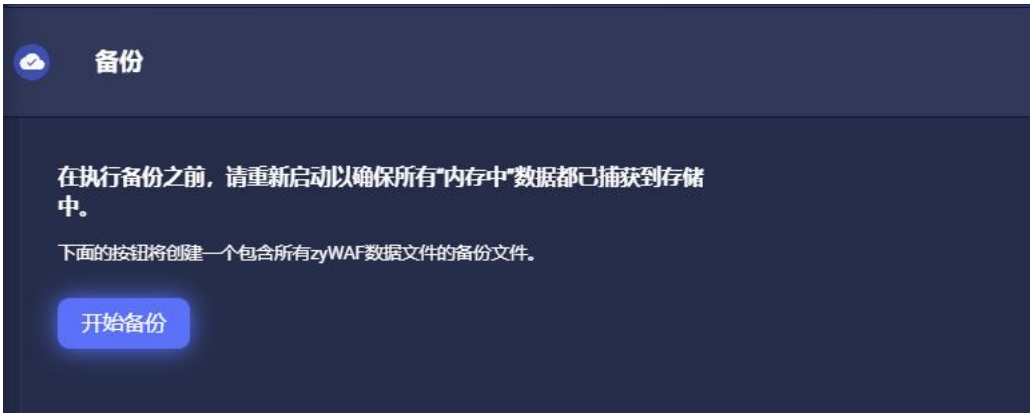

图 8-9 备份

点击 **开始备份** 创建并保存一组 AI 防护者备份文件。

8.4.2 恢复

图 8-10 恢复

按照恢复提示进行操作。

8.5健康检查

AI 防护者的设计保证了高可用性，以确保 AI 防护者不会因为自身问题阻止对网站的访问。

1. AI 防护者默认启用健康检查。健康检查 每分钟检查一次流量是否通过 AI 防护者到网站，以及从网站通过 AI 防护者返回流量给客户端。如果检测不通过，AI 防护者会自动重启。

2. AI 防护者因为健康检查失败重启 5 次后，如果流量仍然无法通过 AI 防护者进出网站，健康检查会将 AI 防护者切换到透明模式。在透明模式下，AI 防护者不对流量

进行处理，直接转发给受保护 Web 服务器。

这些保障措施确保 AI 防护者的意外问题不会干扰网站的流量。

图 8-11 健康检查

网站：此下拉菜单用于选择健康检查将监控的网站。

开启：启用后，将以指定周期检测通过 AI 防护者后网站是否可访问，如果通过 AI 防护者后网站不可访问，AI 防护者将重启。默认值：启用。

健康检查间隔（秒）：检查网站可访问性的频率（以秒为单位）。默认值：60。

失败阈值：网站连续无法访问的次数。默认值：3。

失败行动：健康检查失败后将采取的操作。默认值：重启 WAF。

重启失败阈值：超过失败次数阈值后，AI 防护者将被切换到透明模式。默认值：5。

网站：此下拉菜单用于选择健康检查将监控的可访问性网站。

HTTP 代码：检查可访问性请求的 HTTP 返回代码。默认值：200。

方法：检查可访问性的 HTTP 方法。默认值：HEAD。

URL：检查可访问性的网站 URL。默认： /。

8.6用户管理

在初始安装 AI 防护者时，默认定义了一个用户： “admin” 。

“admin”用户是内置的，拥有所有权限并且不能被删除。

图 8-12 用户管理

用户管理列表显示了所有用户，包括默认的“admin”用户。可以查看、添加和删除用户。

添加用户：单击此按钮允许创建新的用户。

用户名：创建的帐户名。

角色：创建账户的角色。可用的角色有：管理型用户、系统用户、安全用户和审计用户。

这些角色具有以下权限：

系统用户 - 此角色允许访问以下菜单项：

- 仪表板
- 快速入门
- 系统
- 学习
- 帮助

安全用户 - 此角色允许访问以下菜单项：

- 仪表板
- 设置
- 告警
- 帮助

管理型用户 - 此角色允许除一下功能外的所有功能：

- 添加和删除用户
- 导出或重置审核日志

审计用户 - 此角色允许“只读”功能。 审核角色不得更改策略和重新启动 AI 防护者。

该角色允许：

- 导出审核日志
- 重置审核日志

登录失败模式：用户登录失败时采取的操作。

活动：显示用户当前的登录状态。

(...)：单击此按钮将删除选定的用户。

8.7审计日志

审计日志记录所有重要的管理事件，包括：

- 设置更改
- 成功的登录/注销活动
- 登录尝试失败
- 用户管理功能
- WAF 重启

图 8-13 审计日志

导出 CSV 按钮：单击会将审核日志导出为 CSV 文件。

重置按钮：单击将清除所有审计日志条目。

刷新按钮：单击会将任何新的日志条目添加到审核日志表中。

快速搜索：输入文本并按 Enter 搜索审计日志表中的所有字段。

审核日志提供以下信息：

日期时间：记录事件的日期和时间。

级别：记录事件的级别。

用户：执行记录事件的用户。

远程 IP：执行记录事件的用户的 IP 地址。

API：导致记录事件的 API。

内容：记录事件的描述。

8.8日志设置

日志设置菜单用于启用和配置流量日志设置和 WAF 日志的参数。

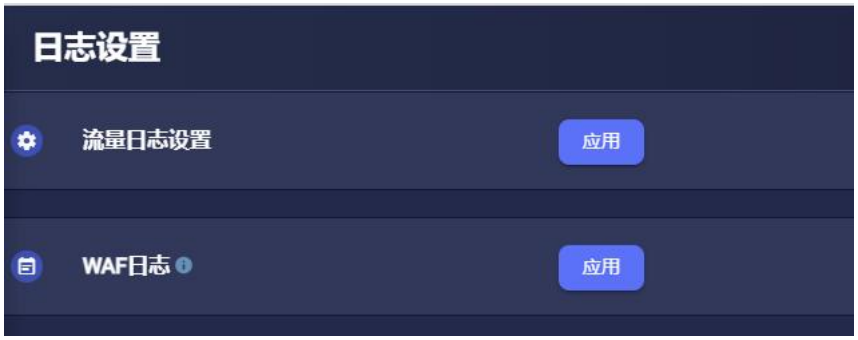

图 8-14 流量日志

8.8.1 流量日志设置

流量日志设置记录受保护网站的所有流量。

图 8-15 流量日志设置

网站：此下拉菜单选择设置受保护网站日志参数。

启用/禁用：启用后，将为所选网站启用流量记录。 默认值：禁用。

字段：此处选择要包含在流量日志文件中的字段。 默认值：日期、时间、c-ip、cs-method、cs-uri、cs-uri-stem、cs-uri-query、s-status、sc-bytes。

周期：指定了流量日志关闭、重命名和开始新流量日志的时间段 [每月、每周、每天、每小时]。 默认值：每天。

分隔符：在流量日志中用作分隔符的字符。 默认值：制表符

存档保留期。要保留流量日志的月数、周数或天数。 超出指定时间段的交通日志数据将被删除。 默认值：12 个月。

8.8.2 WAF 日志

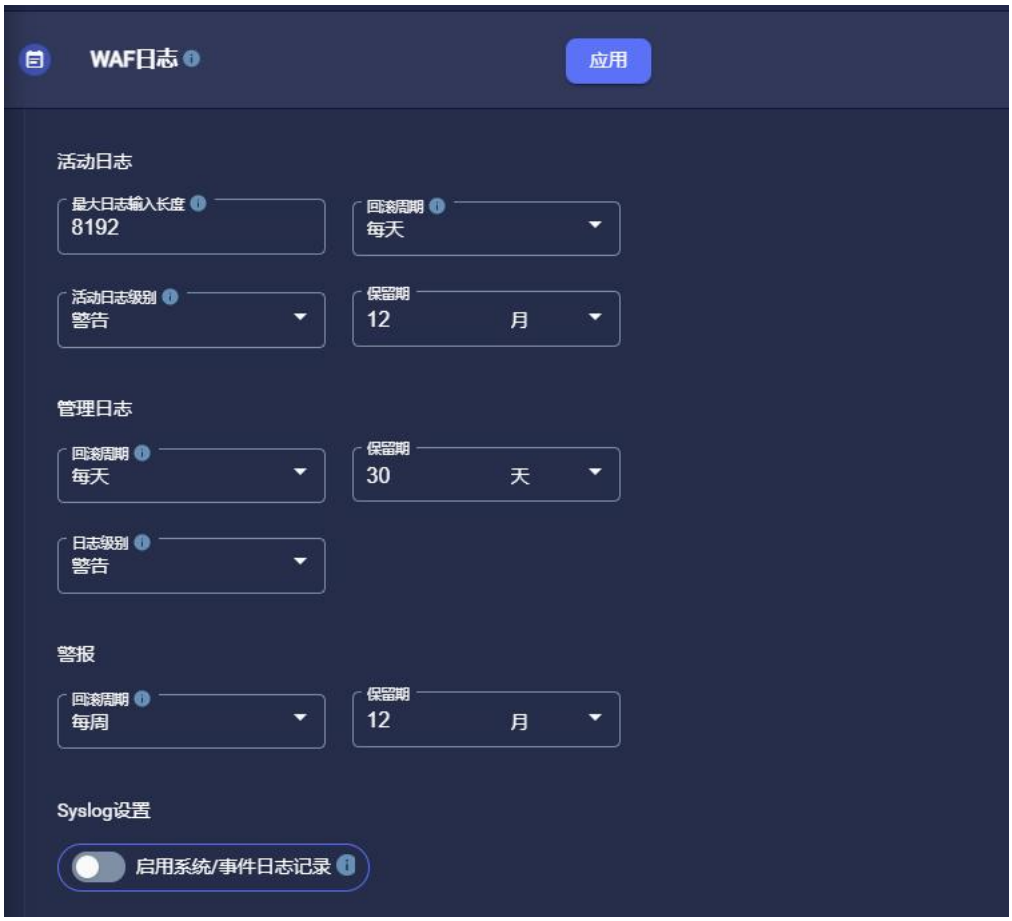

图 8-16 WAF 日志

活动日志

最大日志输入长度：活动日志条目中允许的最大字符数。 超过此长度的字符将从活动日志条目中截断。 默认值：8192。

回滚周期：指定活动日志将重命名保存和启动新活动日志的月数、周数或天数。 默认值：每天。

活动日志级别：将记录的消息的级别 [错误、警告、正常、调试、超级]。超过所选级别的消息将不会记录在活动日志中。 默认值：警告。

保留期。 指定要保留活动日志的月数、周数或天数。 指定期间以外的活动日志数据将被删除。 默认值：12 个月。

管理日志

回滚周期：指定管理日志将重命名保存和启动新管理日志的月数、周数或天数。 默认值：每天。

存档保留期：指定要保留管理日志的月数、周数或天数。 超出指定期限的管理日志将被删除。 默认值：30 天。

日志记录级别：将记录的消息的最低严重性 [正常、错误、警告、调试]。超过所选级别的消息将不会记录在活动日志中。 默认值：警告。

告警日志

回滚周期：指定告警日志将重命名保存和启动新告警日志的月数、周数或天数。 默认值：每周。

存档保留期：指定要保留告警日志的月数、周数或天数。 超出指定时间段的告警日志将被删除。 默认值：12 个月。

系统日志设置

启用系统/事件日志：选中后，系统/事件日志将被启用。 默认值：禁用。

8.9日志文件管理

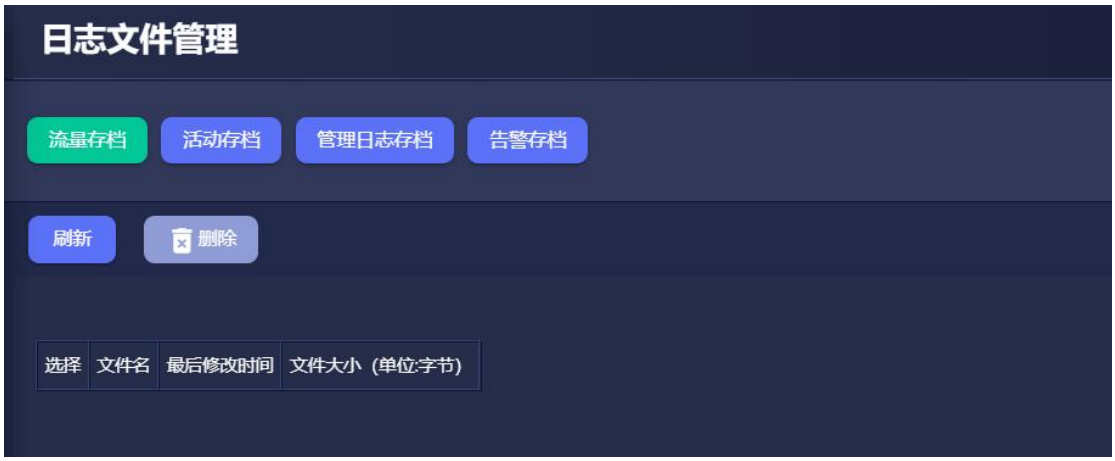

图 8-17 日志存档

流量日志存档

刷新：更新列表的内容。

选择：选中此复选框时，单击顶部的删除按钮将删除相应的文件。

删除：按钮将删除表格中已勾选的所有文件。

文件名：包含流量存档数据的文件的名称。

上次修改时间：上次修改流量存档文件的时间。

文件大小（单位：字节）：流量存档文件的大小。

注意：单击列标题将按列的内容对表条目进行排序。 再次单击将切换排序顺序。

WAF 活动日志存档

刷新：更新表格的内容。

选择：选中此复选框时，单击顶部的删除按钮将删除相应的文件。

删除：按钮将删除表格中已勾选的所有文件。

文件名：包含 WAF 活动日志存档数据的文件的名称。

上次修改时间：上次修改 WAF 活动日志存档文件的时间。

文件大小（单位：字节）：WAF 活动日志存档文件的大小。

注意：单击列标题将按列的内容对表条目进行排序。 再次单击切换排序顺序。

WAF 管理日志存档

刷新：更新表格的内容。

删除：按钮将删除表格中已勾选的所有文件。

选择：选中此复选框时，单击顶部的删除按钮将删除相应的文件。

文件名：包含 WAF 管理日志存档数据的文件的名称。

上次修改时间：上次修改 WAF 管理日志存档文件的时间。

文件大小（单位：字节）：WAF 管理日志存档文件的大小。

注意：单击列标题将按列的内容对表条目进行排序。 再次单击将切换排序顺序。

告警存档

刷新：更新表格的内容。

删除：删除表格中已勾选的所有文件。

还原：将文件中的告警恢复到当前告警列表中。

文件名：包含告警存档数据的文件的名称。

上次修改时间：上次修改告警存档文件的时间。

文件大小（单位：字节）：告警存档文件的大小。

注意：单击列标题将按列的内容对表条目进行排序。再次单击将切换排序顺序。

8.10 远程访问

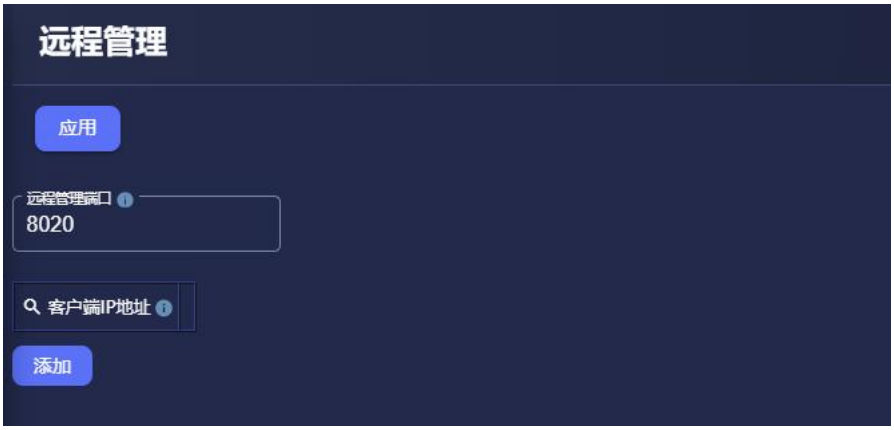

图 8-18 远程访问

远程管理端口：用于 AI 防护者管理控制台的 TCP 端口。 默认值：8020。

客户端 IP：可用于访问 AI 防护者管理控制台的 IP 地址列表。 如果列表为空，则允许所有 IP 地址访问。 默认值：空。

8.11 证书

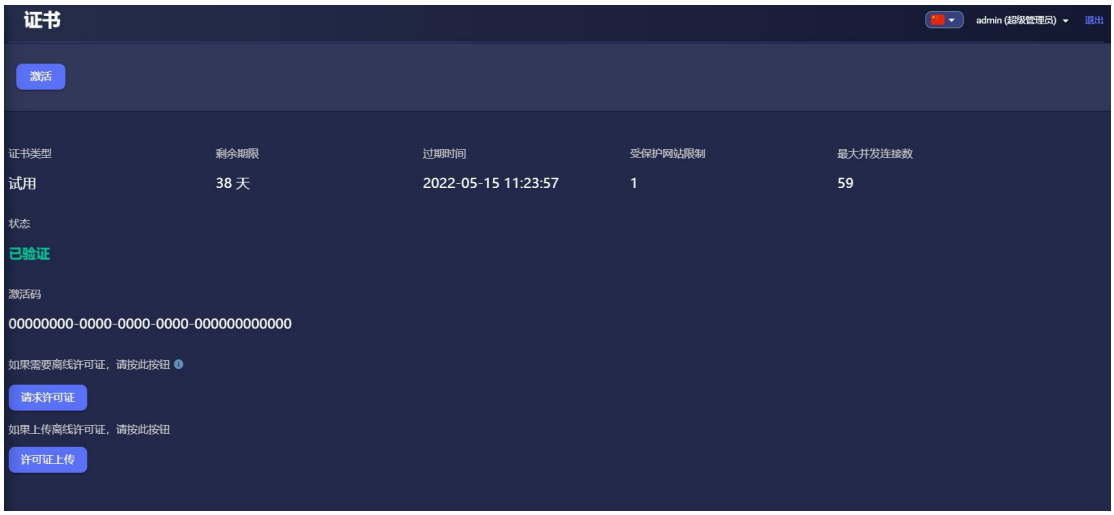

图 8-19 证书

AI 防护者安装后提供 45 天试用期。 在试用期间，最大并发连接数为 59。

如果需要正式授权的许可证，通过 sales@zyprotect.com 联系中云网安了解更多信息。

注意：删除已安装的 AI 防护者目录时，许可证将被销毁。 为避免此问题并继续使用许可证，请在删除已安装的 AI 防护者目录之前停用许可证。然后在新安装的 AI 防护者重新激活许可证。

许可证类型：当前使用的许可证类型。默认：试用

剩余期限：许可证到期的剩余天数。

过期时间：许可证到期的日期。

受保护网站的限制：当前许可证允许保护网站的最大数量。

最大并发连接数：当前许可证允许的最大并发连接数。 （值 0 表示无限制。）

状态：许可证的状态。

激活：用于激活当前许可证的代码。

许可证请求/许可证上传：使用离线许可证时使用这些按钮。许可证请求将创建一个唯一的代码，该代码可以通过电子邮件发送给 zyProtect，请求离线许可证。当收到来自 zyProtect 的离线激活码时，使用“许可证上传”按钮进行安装。

9 帮助

9.1用户手册

单击此菜单项可打开一个浏览器窗口，将自动下载并显示《AI 防护者用户手册》。

9.2提交诊断

图 9-1 提交诊断

如果在运行 AI 防护者时出现问题，您可以通过 support@zyprotect.com 向 AI 防护者支持团队发送反馈。 单击此页面的下载支持日志文件以下载中云网安 zyProtect 技术人员可用于分析问题的支持 zip 文件。 支持文件包括 AI 防护者的所有策略配置（在此处记录的管理界面中指定）、内部日志和内部机器学习策略。