中云网安
ZYPROTECT

AI 防护者用户手册

中云网安科技有限公司

Table of Contents

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-9.0.0-72.centos7.x86_64.rpm

备注：9.0.0-72 为版本号，会随着发版而变化

如图 1-1 所示：

```
[root@localhost Downloads]# rpm -ivh zyWAF-8.2.1-7406.centos7.x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:zyWAF-8.2.1-7406.centos7         ################################# [100%]
[root@localhost Downloads]#
```

图 1-1 安装信息

注意：AI 防护者管理界面使用 TCP 端口 8020。

注意：现在可以按照按照本手册第 2 节中的说明运行 快速设置。

1.2 Windows 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。

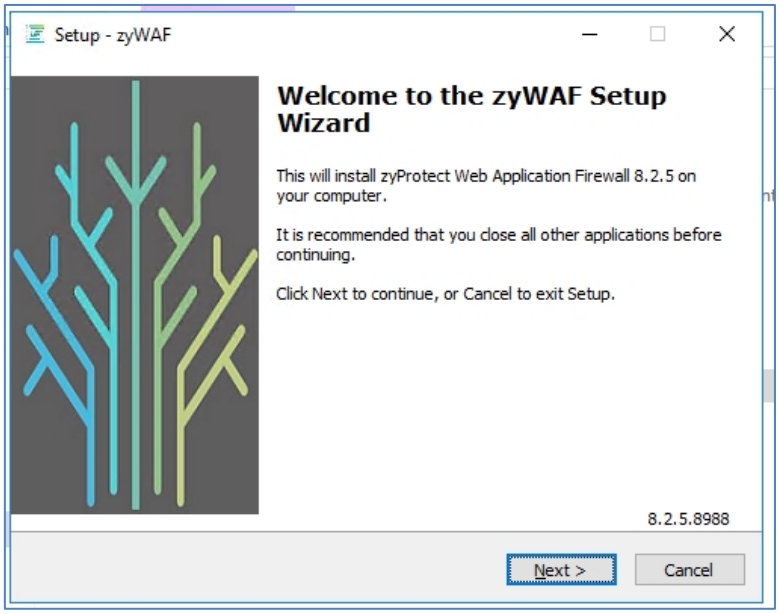

图 1-2 Windows 安装界面

此页面显示许可协议。（图 1-3）单击“下一步”接受协议并继续。

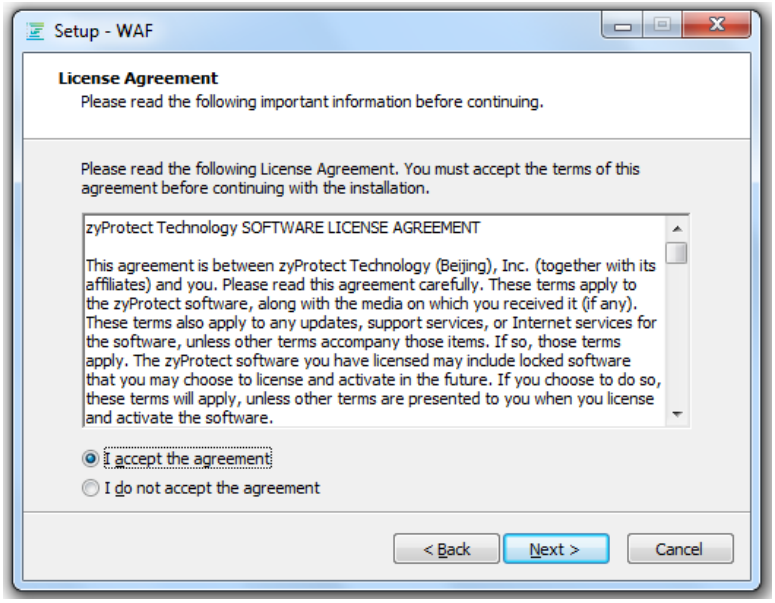

图 1-3 许可协议

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。

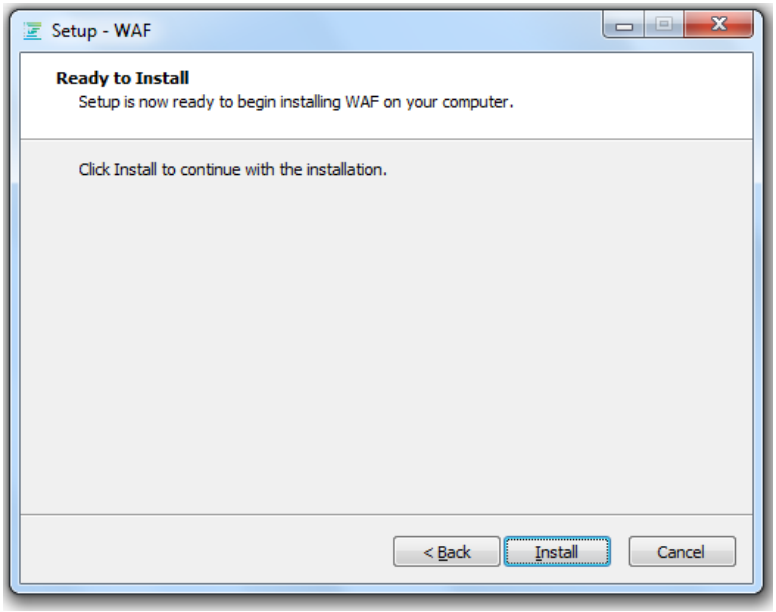

图 1-4 准备安装

进度条显示安装过程 (图 1-5)

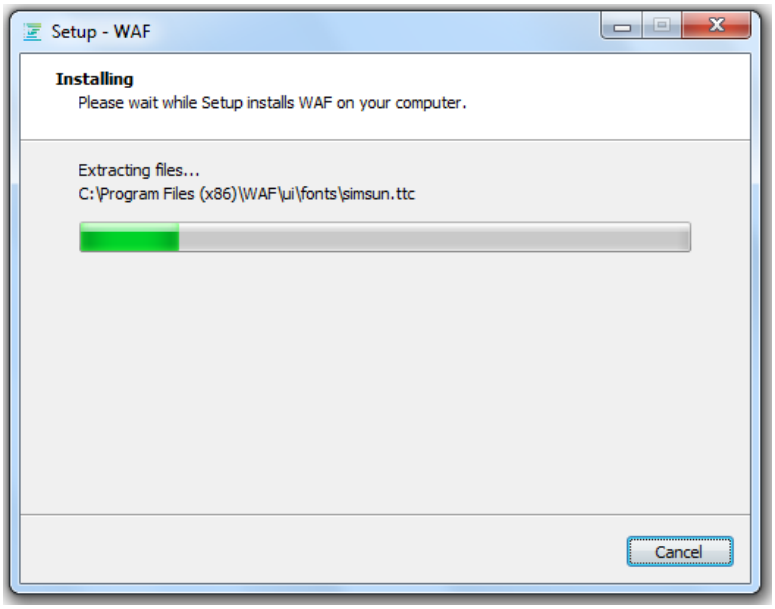

图 1-5 安装过程

在安装过程中，WAService 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）。

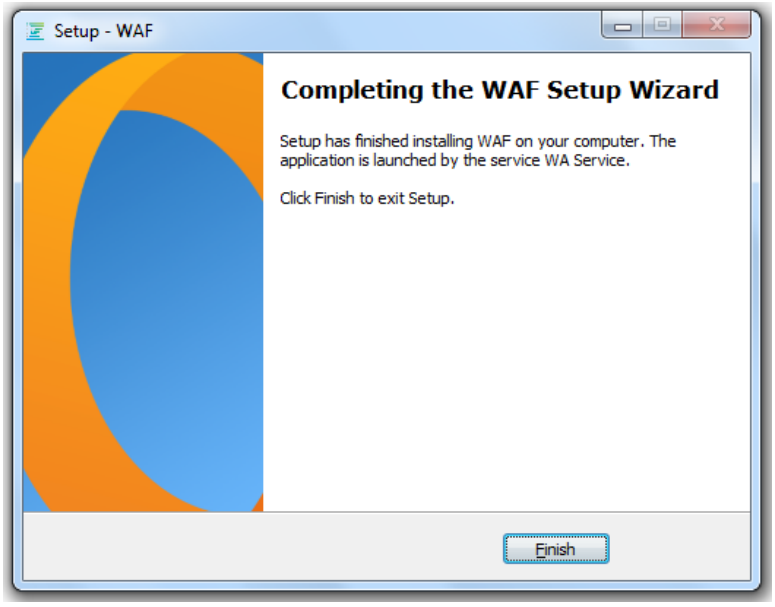

图 1-6 安装完成

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

注意：验证 WAService 是否正在运行：在 Windows 中，选择“搜索程序和文件”，键入服务，然后选择打开“Windows 服务”。应看到状态为“已启动”的服务“WA Service”。

（图 1-7）。

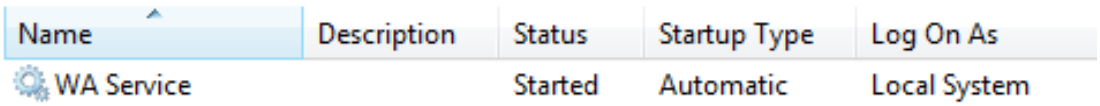

图 1-7 Windows 服务验证

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。

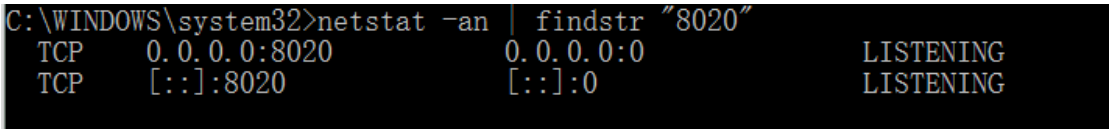

图 1-8 管理界面端口验证

注意：网站的 IP 将默认为 127.0.0.1 (localhost)。 如果 AI 防护者 和网站安装在同一台服务器上，只有一个网络接口，您必须更改网站的端口以避免端口冲突。 要更改您网站的“侦听”端口，请参阅您的网站服务器文档。

注意：现在可以按照按照本手册第 2 节中的说明运行 快速设置。

1.3开始和停止 AI 防护者进程

完成 AI 防护者 安装后会自动运行，无需手动启动。

但是，为方便起见，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

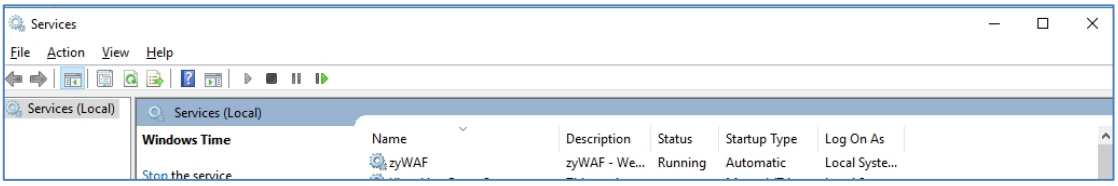

图 1-9 Windows 任务管理器

注意： 停止 AI 防护者 将阻止流量到达受保护的网站。在大多数情况下，最好将 AI 防护者 切换到旁路模式。旁路模式允许流量通过 AI 防护者（无需检查）到达网站。

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 才能与管理控制台一起使用。

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

完成首次登录密码修改后，AI 防护者默认运行快速设置，引导网站的设置和学习。您将看到快速设置对话框。图 2-3。也可以通过在 AI 防护者的左侧菜单中选择 系统设置>快速设置 手动访问快速设置。

注意：初次登录时，AI 防护者会提示您输入许可证密钥或允许您在试用模式下运行。另外，可以通过从左侧菜单中选择 系统设置>证书 手动输入许可证密钥。

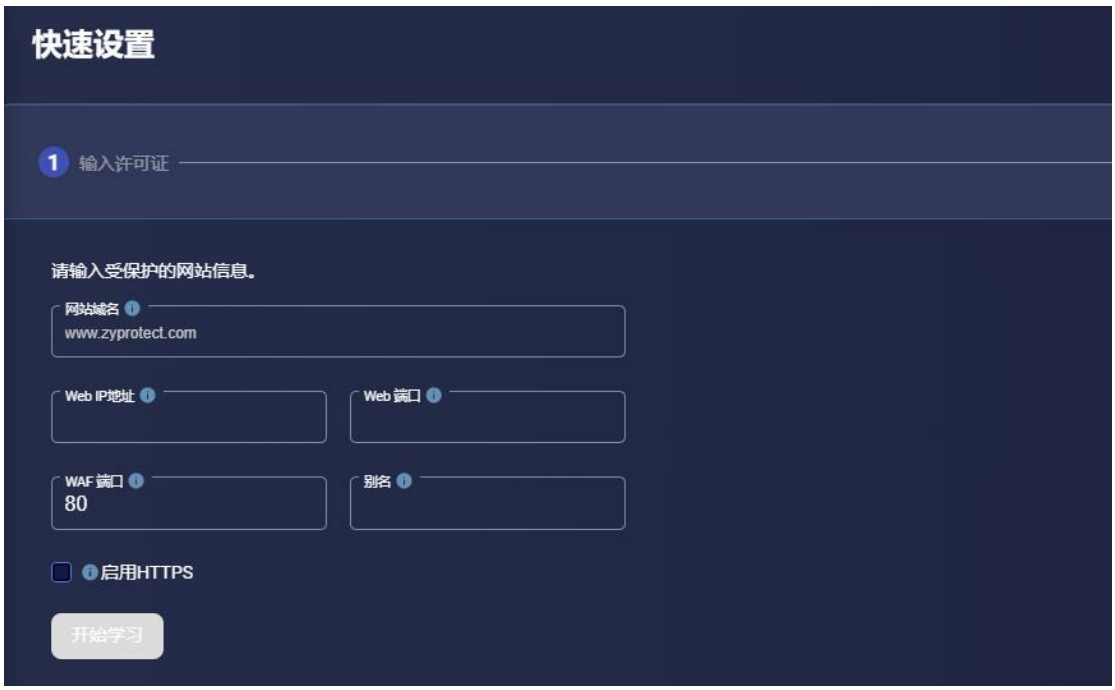

图 2-3 快速设置

在“快速设置”对话框中输入请求的信息，然后单击“开始学习”。AI 防护者开始安全发现网站的结构和内容。 此安全发现学习过程可能需要几分钟或几小时，具体取决于网站的复杂性。也可以通过从左侧菜单中选择学习>安全发现来手动访问安全发现。

安全发现学习过程不会从网站上学习所有内容。 某些动态内容无法通过“安全发现”进行学习。

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网站上的所有动态内容和所有受密码保护的内容。

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学习的网站资源。 如果发现任何遗漏，可以将用户定义属性 (UDP) 添

加到 AI 防护者，以允许流量访问这些网站资源。 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 UDP 按钮。

建议验证过程执行 7 天，或者直到没有发现需要添加 UDP 的进一步告警。 此时，AI 防护者可以切换到保护模式，并提供网站保护。

注意： 在保护模式运行时，AI 防护者将继续使用机器学习来学习网站。

3 设置

设置菜单允许配置基本的 AI 防护者操作参数。

注意：标准的 AI 防护者许可证允许保护一个网站。本章中的图显示了单个受保护网站许可证的数据输入对话框。如果要保护多个网站，则必须购买增强许可证。数据输入对话框的格式将与下图所示略有不同，但适用于要保护多个网站时输入数据的描述。

3.1 服务器设置

服务器设置面板显示当前在 AI 防护者中配置的 Web 服务器的状态。 它还允许添加新的 Web 服务器配置、编辑现有配置和删除现有配置。

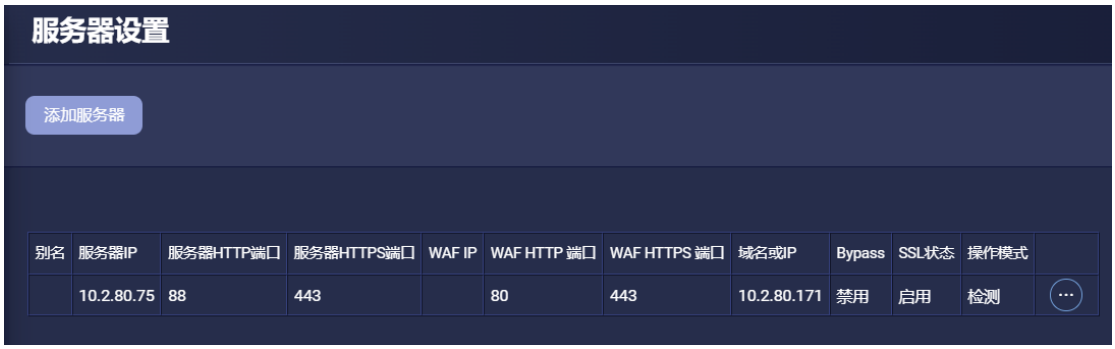

图 3-1--服务器设置

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 服务器的 IP 地址的 HTTP 端口号。HTTP 端口不加密传输的数据。

服务器 HTTPS 端口：受保护 Web 服务器的 IP 地址的 HTTPS 端口号。 HTTPS 端口对传

输的数据进行加密。

WAF IP：AI 防护者将在其上接收受保护 Web 服务器的传入浏览器请求的 IP 地址。如果留空，AI 防护者将接收来自所有 IP 地址的传入请求。

WAFHTTP 端口：IP 地址的 HTTP 端口号，AI 防护者将在其上接收受保护 Web 服务器的非加密传入浏览器请求。

WAF HTTPS 端口：AI 防护者将在其上接收受保护 Web 服务器的加密传入浏览器请求的 IP 地址的 HTTPS 端口号。

域名或 IP：受保护 Web 服务器的一个或多个完全限定的 Internet（外部）Web 服务器域名或受保护 Web 服务器的 IP 地址。

Bypass：如果值为“Enable”，则所有到 Web 服务器的流量都将通过 AI 防护者而不进行检查。正常 AI 防护者操作模式显示“禁用”值，表示 AI 防护者正在检查所有 Web 服务器流量。

SSL 状态：如果值为“启用”，AI 防护者将使用 SSL 连接。如果值为“禁用”，则使用非 SSL（安全性较低）连接。

操作模式：如果值为“保护”，则 AI 防护者正在积极保护网络服务器，并将阻止威胁。如果值为“Detection”，AI 防护者将检查流量并学习无威胁的 Web 服务器流量，并且不会阻止威胁。

添加服务器

服务器设置面板顶部的添加服务器按钮用于为 AI 防护者创建新的 Web 服务器配置。

图 3-2 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。

透明模式：选中后，流量将不经检查直接传递到 Web 服务器。 没有威胁记录或阻止。 默认值：禁用。

注意：在 Bypass 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，不会向浏览器或其他网站访问工具提供 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。 隐藏 Web 服务器身份对于防止横幅抓取攻击很有用。 默认值：启用

添加 X-Forwarded-Proto 标头：选中后，AI 防护者将使用源连接的原始协议添加 X-Forwarded-Proto 标头。这通常用于表示 AI 防护者将原始的 HTTPS 流量转换为 HTTP 流量。 默认值：禁用。

保护模式：此选项为面板中指定的 Web 服务器 IP 和 Web 服务器端口的网站选择当前的 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。
- **监测：**仅记录威胁。

注意：在主动模式和被动模式下运行的同时，AI 防护者将继续使用机器学习来学习网站。

Web IP：受保护的 Web 服务器的地址必须使用 IP 地址（推荐）或完全限定的 Internet Web 服务器域名输入。 默认值：空。

Web 端口：受保护网站侦听 HTTP 流量的传输控制协议 (TCP) 端口。 默认值：80。

WAF IP： AI 防护者接收传入流量的 IP 地址 Default： Empty.

WAF 端口：AI 防护者接收传入流量的 TCP 端口。 默认值：80。

注意：仅当 AI 防护者安装在单独的操作系统上时，AI 防护者端口分配可能与网站端口

相同。 如果网站安装了 AI 防护者，则保护端口和网站端口必须不同，以允许 AI 防护者处理的代理流量路由到网站。

绑定 IP：AI 防护者在连接 Web 服务器前会绑定的 IP 地址。 这允许将 AI 防护者配置为仅侦听来自特定网络接口的连接。 例如，如果安装了 AI 防护者的服务器中有两个网卡，那么您可以将 AI 防护者绑定到任一接口。 如果留空，操作系统将分配一个 IP 地址给 AI 防护者。 默认值：空。

客户端主机验证：启用后，AI 防护者将验证主机标头名称是否与 Web 服务器域名之一匹配。 默认值：启用。

域名或 IP 地址：AI 防护者正在保护的 Web 服务器的一个或多个完全限定的 Internet Web 服务器域名或 IP 地址。 默认值：空。

注意： *Web 服务器 IP 标识受 AI 防护者保护的网站以建立套接字连接，而 Web 服务器域名为 AI 防护者提供了一种方法来识别网站 HTML 内容中引用的全限定 URL。*

SSL 设置

加密到 Web 服务器：选中后，AI 防护者将重新加密流量并使用 HTTPS 传输到 Web 服务器。 当 AI 防护者和 Web 服务器都位于受保护的 DMZ（受防火墙保护的非军事区）内时，避免对 Web 服务器进行加密可能会提高性能，而不会对安全造成威胁。 默认值：启用。

将 HTTP 流量重定向到 HTTPS 端口：选中后，AI 防护者会将未加密的 HTTP 流量重定向到 HTTPS 端口。 例如，http：//www.myhost.com/index.html 将被重定向到 https：//www.myhost.com/index.html。 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。

注意：HTTP 端口（通常是端口 80）对于 HTTP 流量将保持活动状态。

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

证书文件：AI 防护者代表 Web 服务器使用的 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。 Microsoft ™ 约定 .crt 文件必须转换为 .pem 格式。 默认值：空。

Certificate Key File：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。Certificate 证书文件：证书的证书证书 (CA) 文件。 此文件还必须采用 ASCII PEM 编码 (Base64) 格式。默认值：空。

注意：证书文件、证书密钥文件和证书颁发机构文件都必须从网站所有者/管理员处获取，并放置在安装了 AI 防护者的操作系统上的适当目录中。

3.2高级功能

高级功能菜单面板允许配置高级 AI 防护者操作参数。

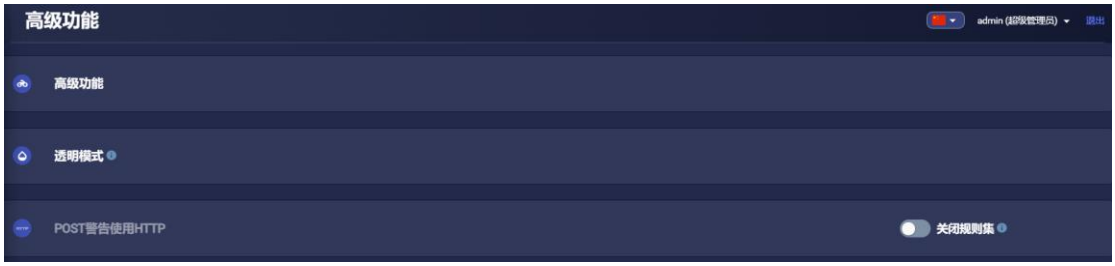

图 3-3 高级功能

3.2.1 高级功能

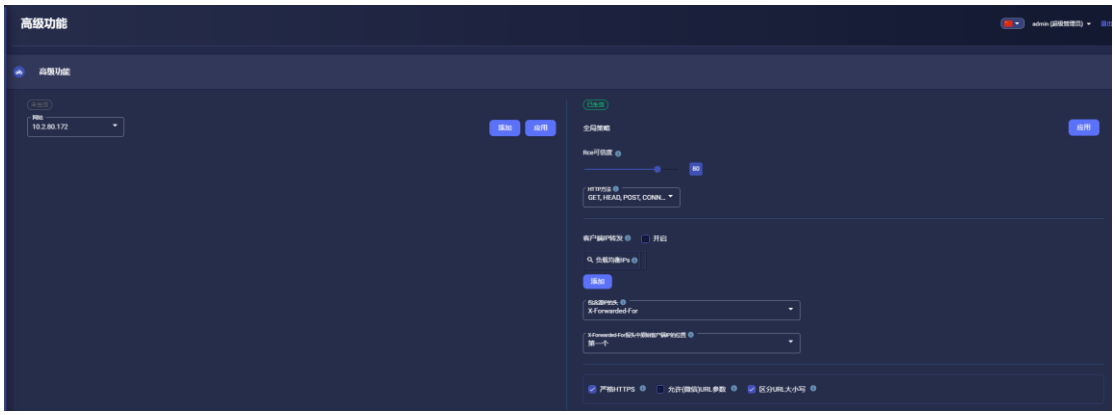

图 3-4 高级功能

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

RCE 置信度：Remove Command Execution 置信度介于 10 和 100 之间。值 10 提供的保护最少，值 100 提供最大的保护。 默认值：80。

HTTP 方法：AI 防护者允许的 HTTP 方法。 默认的 HTTP 方法将满足大多数网站的需求。仅应根据需要启用其他方法。 默认值：GET、HEAD、POST、CONNECT。

客户端 IP 转发启用：勾选后，AI 防护者将添加一个 X-Forwarded-For 标头与连接的源 IP。 默认值：禁用。

数据表

代理和负载均衡 IP：勾选 启用客户端 IP 转发 时，来自这些 IP 的请求将被视为已实现该协议的代理或负载均衡器。 默认值：空。

Header 包含源 IP：选择的 header 将用于标识请求的源 IP。 默认值：X-Forwarded-For。

X-Forwarded-For 标头中原始客户端 IP 的位置：AI 防护者期望源 IP 在 X-Header 中的位置。 默认值：第一个。

严格 HTTPS：选中并启用 HTTPS 协议时，将阻止基于相对 URL 的 HTTP 请求。 默认值：启用。

允许分析（微信）：选中后，微信分析参数将附加到客户端 URL。 默认值：禁用。

区分大小写的 URL：选中后，具有相同字符和不同大小写的 URL 将被视为不同的 URL。默认值：启用。

3.2.2 透明模式

图 3-5 透明模式

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。.

数据表

管理 IP 地址：来自这些 IP 地址的请求将被直接转发到网站，无需 AI 防护者检查。

3.2.3 Post 告警使用 HTTP

图 3-6 Post 告警使用 HTTP

开启规则集：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网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站设置的的所有网站。

告警原因：指定后，只会发送符合指定原因的告警。当未指定告警原因时，将发送所有告警。默认值：0 项已选。

服务器名称：将接收基于 HTTPPOST 的通知的服务器名称或 IP 地址。默认值：空。

服务器端口：将接收基于 HTTPPOST 的通知的服务器端口。默认值：80。

来自：用于指示基于 HTTPPOST 的通知的来源的说明文字（注释）。默认值：空。

URL：用于处理基于 HTTPPOST 的通知的 URL。默认值：空。

3.3规则设置

规则菜单面板允许配置高级 AI 防护者规则。.

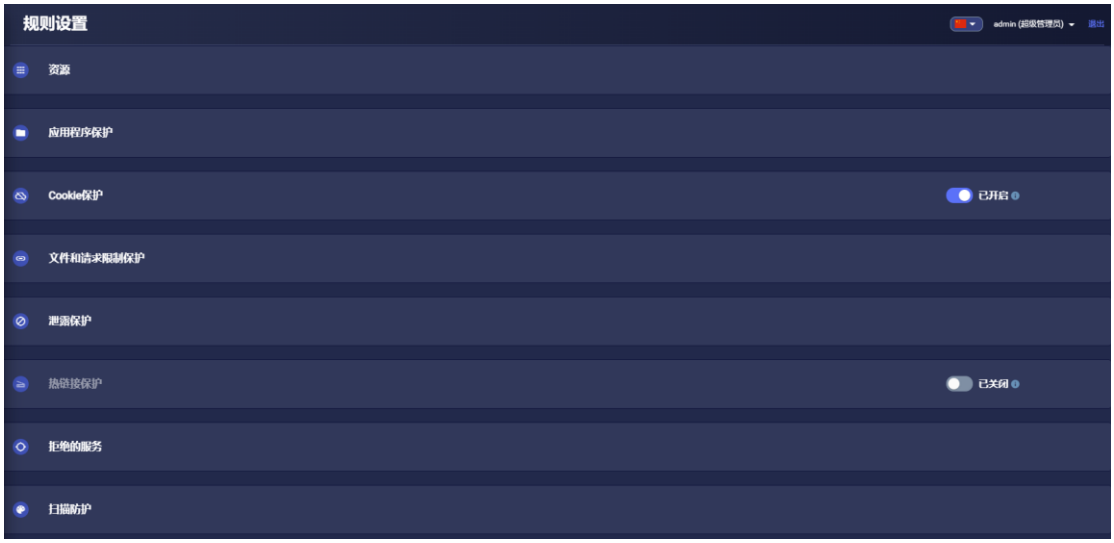

图 3-7 规则设置

3.3.1 资源

可以通过将受保护网站上的指定目录、文件指定为资源例外来允许访问它们（URL 白名单）。浏览器可以直接访问这些文件。

图 3-8 资源

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

数据表

URI 路径：一个或多个允许的文件 URI。默认：“ /”。

进入节点：为指定的文件 URL 路径启用或禁用。 默认值： “/”启用，其他禁用。

仅安全 (HTTPS)：选中后，仅允许 HTTPS 连接。 默认值：禁用。

区分大小写：选中后，AI 防护者将观察区分大小写的文件 URL 路径。 默认值：禁用。

正则表达式：启用后，文件 URL 路径可能是正则表达式。 有关示例，请参见下表。 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 3-9 使用正则表达式的文件路径 URL 示例

3.3.2 应用程序保护

可以在这些面板中配置 AI 防护者恶意代码注入保护的设置。

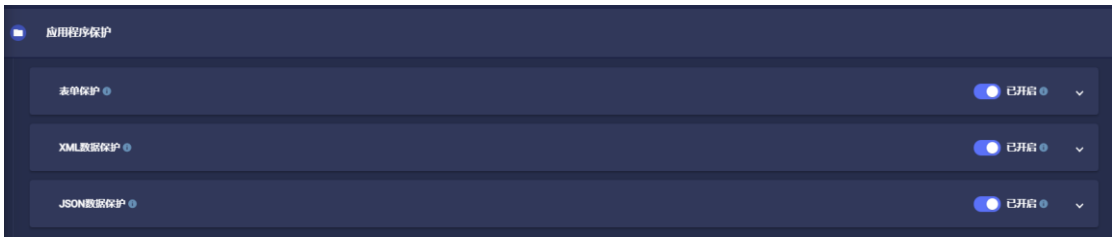

图 3-10 应用程序保护

表单防护

将使用表单验证以防止注入攻击。 开启“表单保护”面板底部的功能列表，可以允许对指定表单进行未经验证的表单输入。

图 3-11 表单防护

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

规则集开：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：TEXT、TEXTAREA 和 PASSWORD。

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**：当在文本输入表单上输入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，当在文本输入表单上输入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。

任何字段类型：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

将对请求正文中的应用程序数据进行验证，以防止注入攻击。 可以使用面板底部的表格来允许未经验证的输入，以列出无需验证的 URI。

图 3-12 XML 数据保护

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

规则集开：确定是否将执行 XML 数据威胁检测。默认值：启用。

告警：选中并检测到对 XML 数据的威胁时，将生成告警。默认值：启用

阻止：选中并检测到对 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

将对请求正文中的 JSON 数据进行验证，以防止注入攻击。 可以使用面板底部的表格来允许未经验证的输入，以列出无需验证的 URI。

图 3-13 JSON 数据保护

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

规则集开启：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。

3.3.3 Cookie 保护

图 3-14cookie 保护

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

规则集开启：确定是否将执行 cookie 验证。 默认值：启用。

行动：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）。在这些情况下，请求将显示为对网站的“新”请求。该网站将通过创建一个由客户端浏览器缓存的新 cookie 来响应。
- **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：最初启用 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**：未通过验证的 cookie 被阻止或剥离之后的天数和小时数。 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。

3.3.4 文件和请求限制保护

可以在这些面板中配置 AI 防护者文件保护的设置。

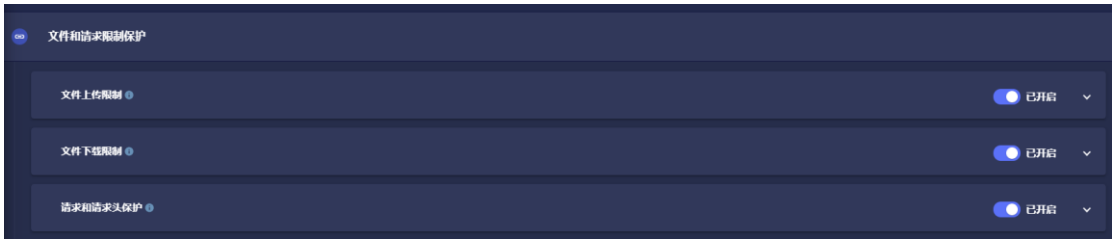

图 3-15 文件和请求限制保护

文件上传限制

图 3-16 文件上传限制

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

规则集开启：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，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。

注意： *可以启用允许的文件上传或拒绝的文件上传。 两者可能不会同时启用。*

选择允许的文件上传时，允许的文件上传列表表列表显示在数据表中。 选择拒绝文件上传时，将显示在数据表中的拒绝文件上传列表表。 每个列表都是独立的。

文件下载限制

图 3-17 文件下载限制

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

规则集打开：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。

Additional Allowed Special Characters：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数据表中。 选择文件下载黑名单时，文件下载黑名单列表显示在数据表中。 每个列表都是独立的。

请求和请求标头保护

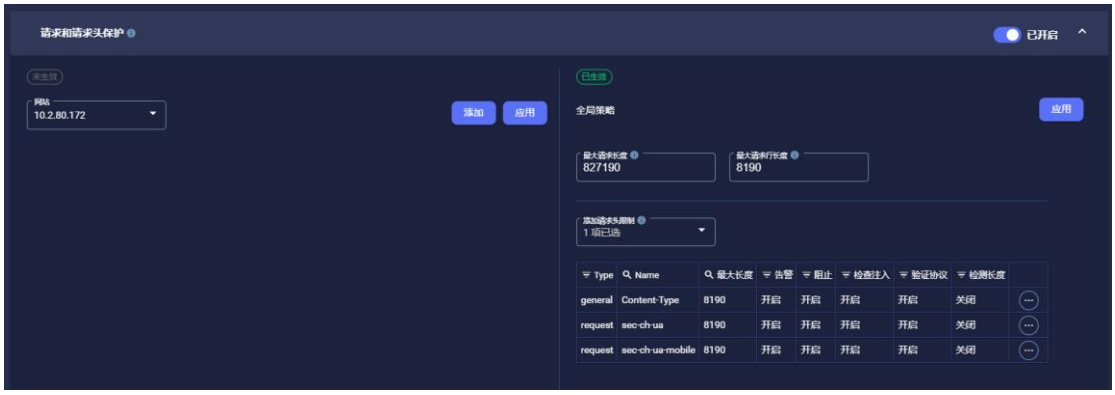

图 3-18 请求和请求标头保护

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设

置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

Ruleset On：确定文件请求和标头保护是否处于活动状态。 默认值：禁用。

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：请求标头中允许的最大字符数。 默认值：8190。

添加标头限制允许 HTTP 标头中允许的最大字符数由标头类型指定。 可以使用为每种类型设置的最大字符数来定义多种标题类型的限制。

数据表包含将受保护的请求和请求标头以及将应用的保护。

3.3.5 泄漏保护

AI 防护者数据泄露的设置 URL 泄露保护可以在这些面板中进行配置。

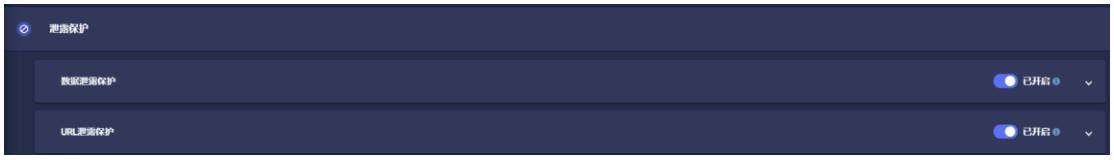

图 3-19 泄漏保护

数据泄露保护

图 3-20 数据泄露保护

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

Ruleset On：确定数据泄漏保护是否处于活动状态。 默认值：禁用。

数据表

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，名称和值条目将被评估为正则表达式。 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 3-21 URL 泄漏保护

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

已开启：确定 URL 泄漏保护是否处于活动状态。 默认值：禁用。

数据表

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，名称和值条目将被评估为正则表达式。 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。

3.3.6 热连接保护

图 3-22 热连接保护

网站： 此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

策略开启： 确定是否阻止带有源自远程网站域的链接的客户端请求，以获取具有受保护文件类型列表中列出的扩展名的文件。 允许的网站域列表中的网站域不会发生阻止。 默认值：禁用。

允许的热连接域名： 不会被阻止热链接到文件的网站域列表。 默认值：空。

受保护的文件类型：启用热链接限制时将防止热链接的文件扩展名列表。 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。

3.3.7 拒绝的服务

可以在这些面板中配置 AI 防护者拒绝的服务保护的设置。

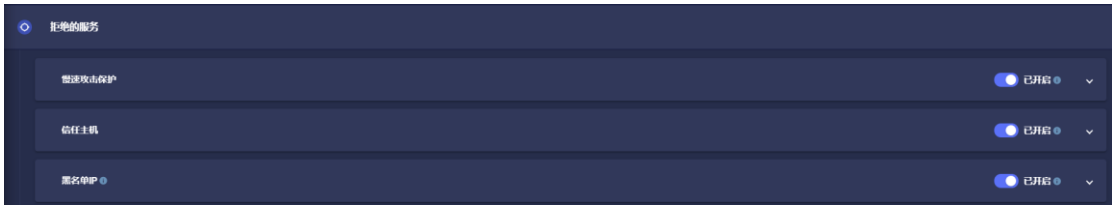

图 3-23 拒绝的服务

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 3-24 慢速攻击保护

网站： 此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局： 在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

策略开启： 确定慢速攻击保护是否处于活动状态，以及是否将对已达到 HTTP 消息阈值或 TCP 数据包间隔阈值中指定的超时的 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）：在执行所选操作之前 HTTP 事务必须经过的秒数。 默认值：60。

TCP 超时阈值（秒）：在执行所选操作之前，TCP 数据包必须经过的秒数。 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 3-25 信任主机

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

启用策略：确定是否会阻止来自受信任 IP 的恶意活动，但不会生成告警。 此功能旨在用于证书的渗透测试。 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 地址添加到此列表表中或从中删除。 默认值：127.0.0.1

IP 黑名单

图 3-26 IP 黑名单

网站：此下拉菜单用于选择一个网站，当单击“应用”按钮时，将应用在面板中输入的设置。

全局：在全局面板中输入的设置将应用于尚未使用网站下拉菜单定义的所有网站。

启用： 确定被阻止的 IP 设置是否处于生效状态。 默认值：禁用。

黑名单 IP： 将被阻止的 IP 地址列表。 默认值：空。

3.3.8 扫描防护

图 3-27 扫描防护

网站：此下拉菜单用于选择单击“应用”时面板中输入的数据将应用到的网站。

开启/关闭： 确定扫描仪保护是否处于活动状态。 默认值：禁用。

监控周期（秒）： 检查告警数据库以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。

监控时间范围（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。

监控周期（秒）： 将该 IP 添加到阻止 IP 列表所需的监控范围内 IP 的告警数量。 默认值：50。

3.4HTTP 响应页面

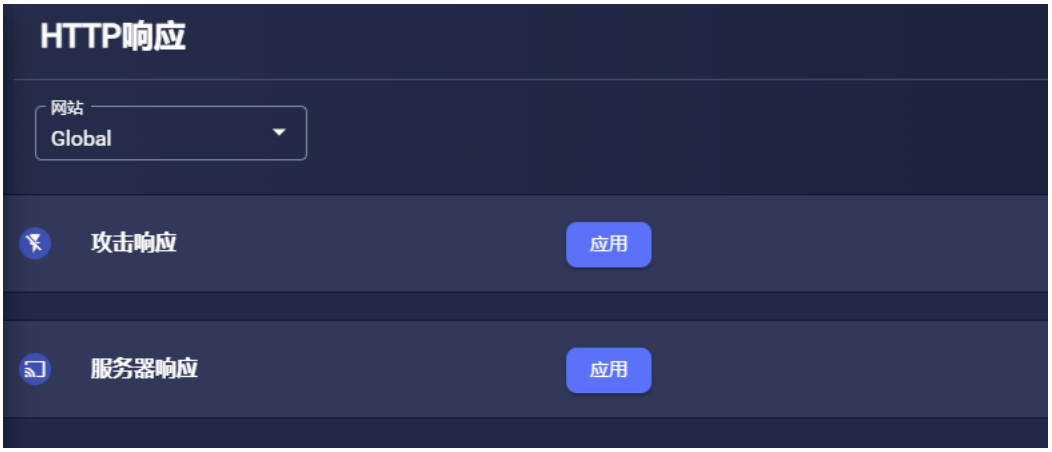

图 3-28 HTTP 响应页面

网站：此下拉菜单用于选择单击“应用”时面板中输入的数据将应用到的网站。 可用选项将包括所有单个网站和“Global”。 选择“Global”时，将在面板中输入的数据应用于所有单个网站。 默认值：Global。

攻击响应

图 3-29 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下面输入的 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： 确定当收到 403 错误时，客户端是否将重定向到下面输入的 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下面输入的 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

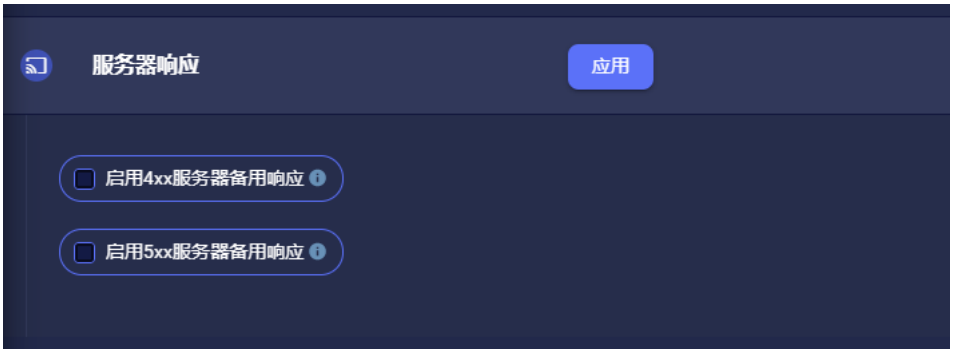

图 3-30 服务器响应页面

Enable 4xx 服务器备用响应

开启/关闭： 确定对于所有 4xx 错误响应，是否将仅包含状态代码和简单描述的替代响应返回给客户端。 默认值：禁用。

开启 5xx 服务器响应页面替换

开启/关闭： 确定对于所有 5xx 错误响应，是否将仅包含状态代码和简单描述的替代响应返回给客户端。 默认值：禁用。

4 告警

告警面板显示由 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。 所有可见告警都显示在表格中。

图 4-1 告警

网站： 来自所选网站的告警将显示在表格中。

时间范围： 只有在指定时间范围内发生的告警才会显示在表格中。

告警描述： 只有与指定字符串匹配的告警才会显示在表格中。

聚合： 告警可以按远程 IP 或 URL 在表中分组。 默认值：禁用。

状态 只有与所选状态匹配的告警才会显示在表格中。 默认值：可见。

自动刷新：在以指定的时间间隔查看表格时，新告警将添加到表格中。 默认值：关闭

更多过滤条件

图 4-2 更多过滤条件

更多过滤器面板用于进一步限制表中显示的告警。

告警原因： 只有与所选原因匹配的告警才会显示在表格中。

告警子原因：只有与所选告警子原因匹配的告警才会显示在表格中。

远程 IP： 只有与所选远程 IP 匹配的告警才会显示在表格中。

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。

告警

图 4-3 告警表单

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

搜索： 此按钮更新告警表的内容以匹配指定的搜索参数。

刷新： 此按钮使用当前记录的告警更新告警表的内容。

导出 CSV： 此按钮会将所有标记的告警导出到逗号分隔值格式的文件中。

隐藏：此按钮将隐藏所有标记的告警。

添加策略：此按钮将创建一个用户定义的策略（UDP），该策略将允许在所选告警中检测到的条件将来发生。

时间：发生告警的日期和时间。

远程 IP：触发告警的请求的远程（源）IP 地址。

国家：触发告警的请求的远程（源）IP 地址所在的国家/地区。

告警原因：告警的威胁类别。

Alert subReason：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。

WAFHTTP 代码：触发此告警时 WAF 返回的 HTTP 错误代码。

WAF 服务器 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面板，用于根据列中的条件限制表中显示的告警。

5 报告

立即报告按钮用于选择允许立即生成报告的面板。 Scheduled Reports 按钮用于选择允许在未来数据和时间自动生成报告的面板。

现在报告

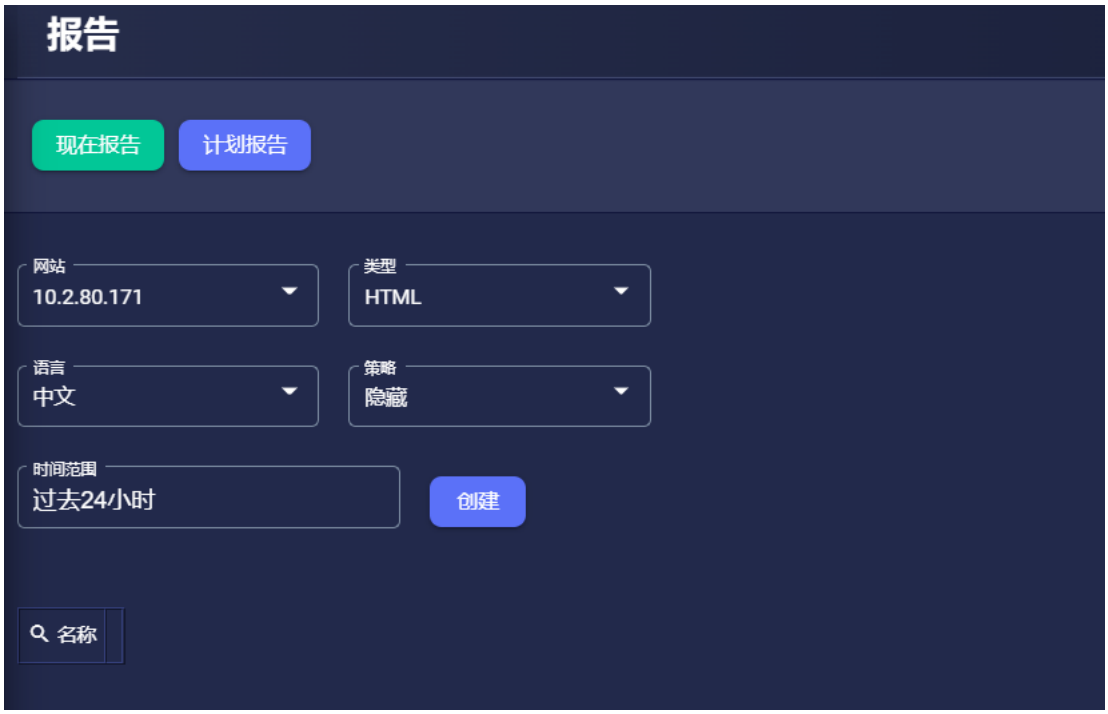

图 5-1 现在报告

网站：来自所选网站的数据将包含在报告中。

类型：这选择报告文件是 HTML 还是 PDF 格式。

语言：选择报告文件是英文还是中文。

策略：这选择是否将 AI 防护者策略（设置）包含在报告文件中。

时间范围：只有在指定时间范围内发生的告警才会包含在报告文件中。

名称：这是以前生成的报告的文件名，现在已保存并可供查看和下载。 文件名包括受保护网站的 IP 地址和端口； 报告中数据的时间范围； 报告的语言； 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 5-2 计划报告

添加计划：此按钮将启用新报告生成任务的创建。

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还是中文。

类型：这将选择计划的报告文件是 HTML 还是 PDF 格式。

报告时间：这将选择创建计划报告的时间。

报告频率： 这将选择创建计划报告的频率。

策略： 这将选择是否将 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，这将选择将创建计划报告的星期几或月份中的哪一天。

收件人：单击添加按钮允许输入将发送预定报告的电子邮件地址。 计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： 此按钮将启用电子邮件服务器设置的输入。

测试邮件按钮： 此按钮将立即使用当前电子邮件设置参数发送一封验证电子邮件。

主题： 用于标记要包含在电子邮件“主题”标题中的发件人的文本字符串。 默认值：AI 防护者。

安全邮件：选中后，将使用传输层安全性 (TLS) 发送电子邮件。 默认值：禁用。

服务器地址： 用于通过电子邮件发送报告的电子邮件服务器的 IP 地址。 默认值：空。

服务器端口：电子邮件服务器用于通过电子邮件发送报告的端口号。 默认值：25。

邮件地址：用于标识要包含在电子邮件消息中的发件人的电子邮件地址。 默认值：空。

邮件密码：用于通过电子邮件发送报告的电子邮件服务器的密码。 默认值：空。

证书文件：启用安全电子邮件时要使用的身份证书文件的位置和名称。 默认值：空。

证书 Key 文件：启用安全邮件 时要使用的身份证书对应的私钥的位置和名称。 默认

值：空。

计划的报告任务： 此表是所有先前创建的计划报告任务的列表。

名称：先前创建的计划报告的用户定义名称。

(...)：单击此按钮允许编辑和删除以前创建的计划报告任务。

计划报告任务的历史记录：此表是所有以前创建的已保存计划报告的列表。

名称： 用于创建报告文件的计划任务生成任务的用户定义名称。

时间：通过电子邮件发送此报告文件的日期和时间。

收件人：用于发送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。

6 学习

学习菜单用于启用机器学习和安全发现。

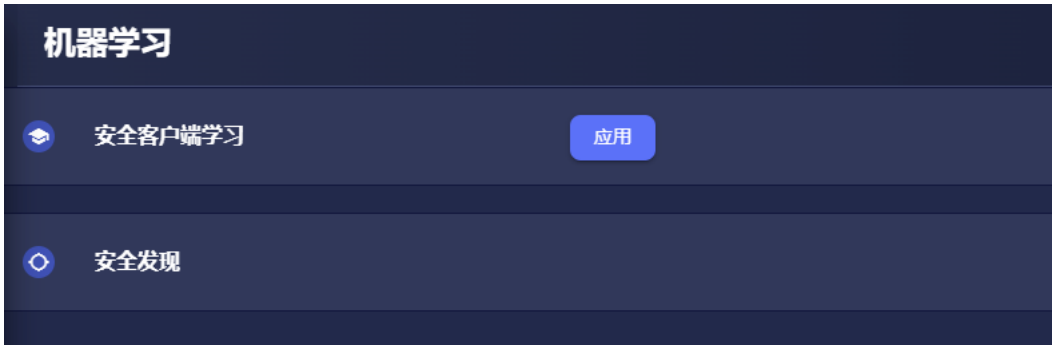

图 6-1 机器学习

6.1机器学习

6.1.1 安全客户端学习

安全客户端学习是机器学习的补充。在正常运行中，AI 防护者只会从网站的响应中不断学习网站的特点。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 请求中学习特征。 来自安全学习 IP 位置的所有 HTTP 查询都被学习为“可信的访问”。

图 6-2 安全客户端学习

安全学习开启/关闭： 确定安全客户端学习是否处于活动状态。 默认值：禁用。

安全学习 IP 地址： 一个 IP 地址列表，AI 防护者将从中“信任”网站请求是安全的并且会学习它们。 来自安全学习 IP 位置的所有客户端 HTTP 查询都被学习为“允许的活动”。一旦获悉，这些来自任何 IP 地址的请求都将被允许。 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。

6.1.2 安全发现

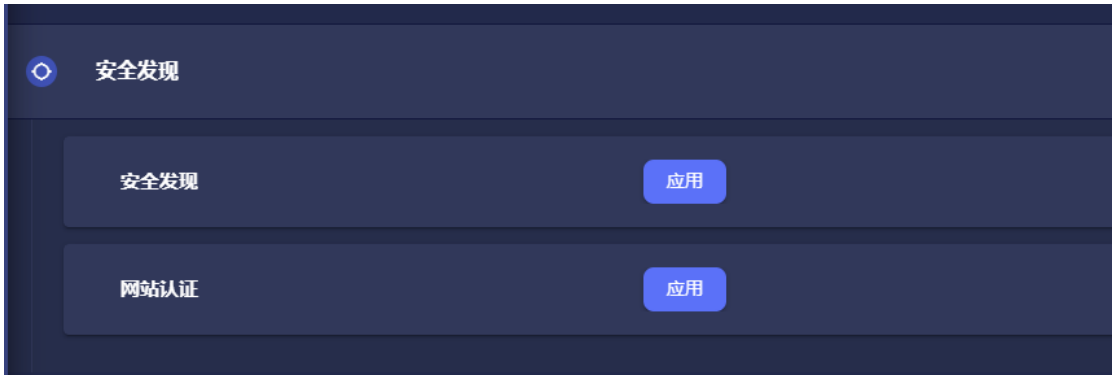

图 6-3 安全发现

安全发现

安全发现自动化机器学习。 在正常运行中，AI 防护者只会从网站的响应中不断学习网站的特点。 启用安全发现后，AI 防护者还将从 AI 防护者运行的网络爬虫的 HTTP 请求中学习特征。 来自 AI 防护者的网络爬虫的所有客户端 HTTP 查询都被学习为“允许的活动”。

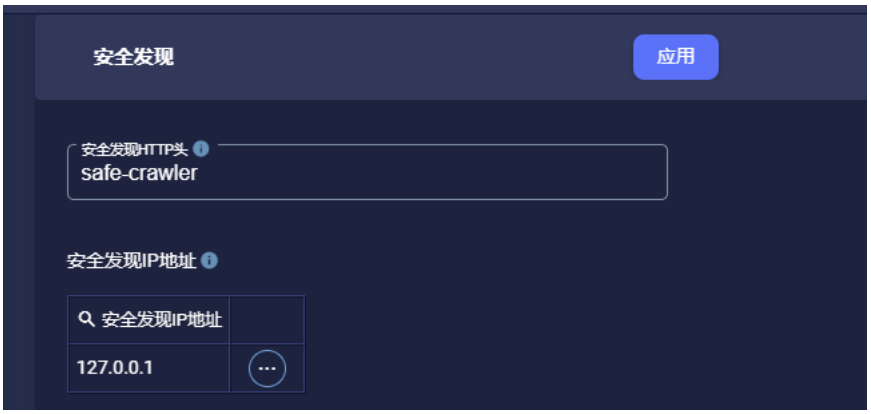

图 6-4 安全发现

应用按钮： 单击后，安全发现爬虫将开始递归发现受保护的网站。

安全发现 HTTP 标头： 安全发现爬虫将返回的标题文本。AI 防护者不会为带有此标头的流量生成告警。 默认值：安全爬虫。

安全学习 IP： 这将显示安全发现爬虫将使用的 IP 地址。AI 防护者不会为来自这些 IP 地址的流量生成告警。

(...)：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 6-5 网站验证

应用按钮： 点击后，安全发现爬虫将在开始递归发现受保护网站时使用提供的数据。

网站：此下拉菜单用于选择安全发现爬虫将开始递归发现的网站。

基本 URL 路径：这是安全发现爬虫将使用的网站的入口点。 默认： /

认证方式：当受保护网站需要证书凭证时，可选择认证方式并输入登录凭证。 默认值：无

6.2安全发现

安全发现状态面板显示安全发现爬虫在学习网站期间返回的数据。

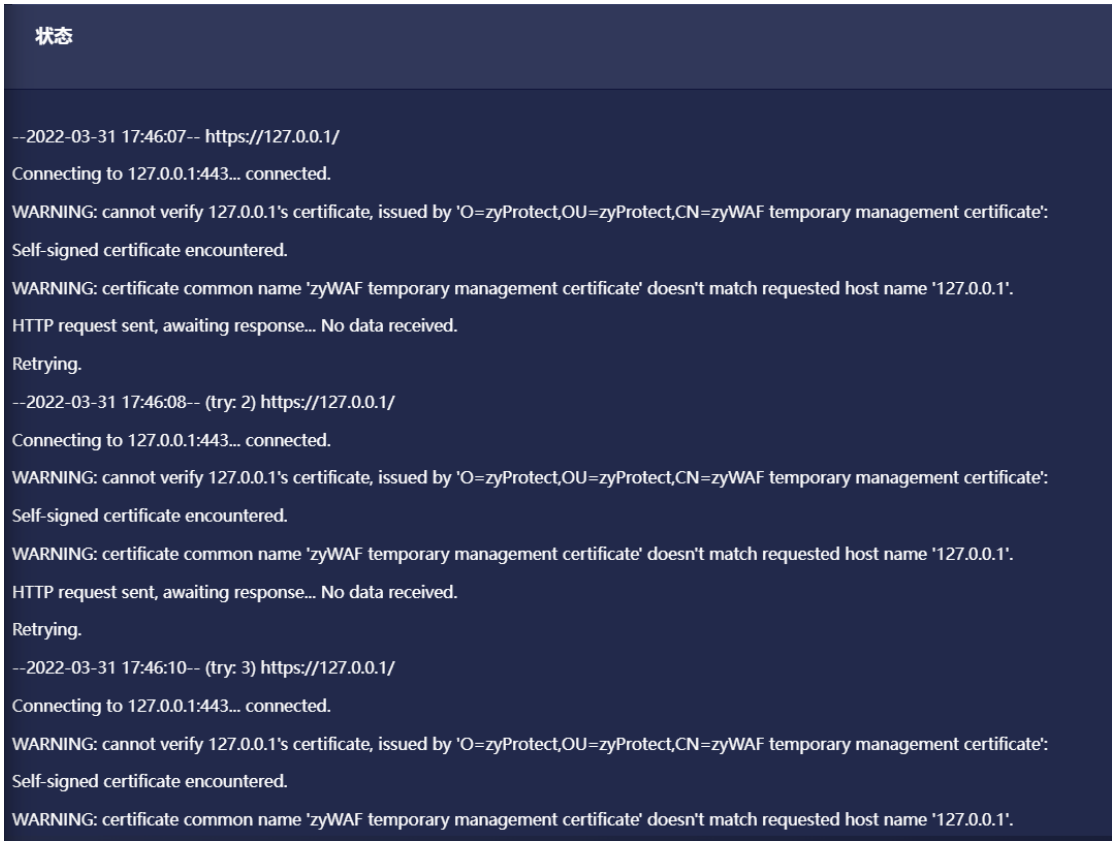

图 6-6 安全发现

网站：此下拉菜单用于选择安全发现爬虫将开始递归发现的网站。

开始：单击后，安全发现爬虫将开始递归发现所选网站。

安全爬虫参数：这将显示安全发现爬虫将使用的参数。

状态：这显示来自在爬行期间创建的安全发现爬虫的状态消息。

7 系统

系统菜单项提供对系统相关功能和设置的访问。

7.1 性能优化

性能调整菜单用于启用和配置性能调整、Cookie 保留、表单保留和资源保留的设置。

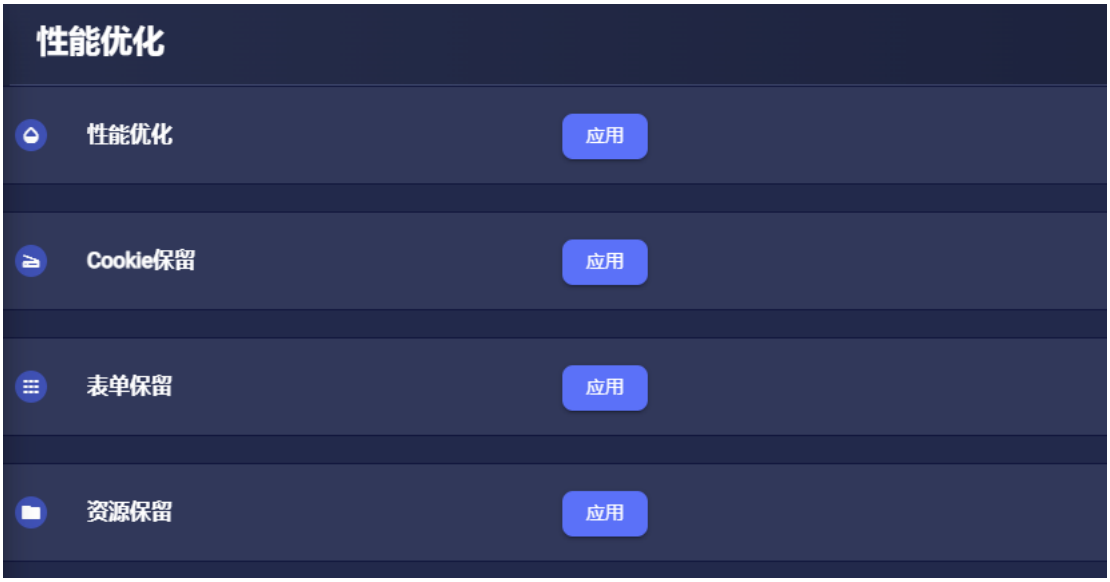

图 7-1 性能优化

7.1.1 性能优化

图 7-2 性能优化

最大连接数：将服务的最大同时请求数。 默认值：5000。

Keep-Alive 超时时间 (秒)：在关闭连接之前等待后续请求的秒数。 默认值：15。

性能因素：用于处理流量的线程数。 默认值：3。

连接缓存保留：保留连接尝试超时的 URL 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之间等待的秒数。 默认值：60。

7.1.2 Cookie 保留

图 7-3cookie 保留

开启/关闭：确定 cookie 是无限期保留（禁用时）还是在指定的日期和时间后删除（启用时）。 默认值：启用 / 15 / 0。

7.1.3 表单保留

图 7-4 保单保留

开启/关闭：确定表单是无限期保留（禁用时）还是在指定的日期和时间后删除（启用时）。默认值：启用 / 3 / 0。

7.1.4 资源保留

图 7-5 资源保留

开启/关闭： 确定资源是无限期保留（禁用时）还是在指定的天数和小时后删除（启用时）。 默认值：启用 / 30 / 0。

7.2仪表板参数

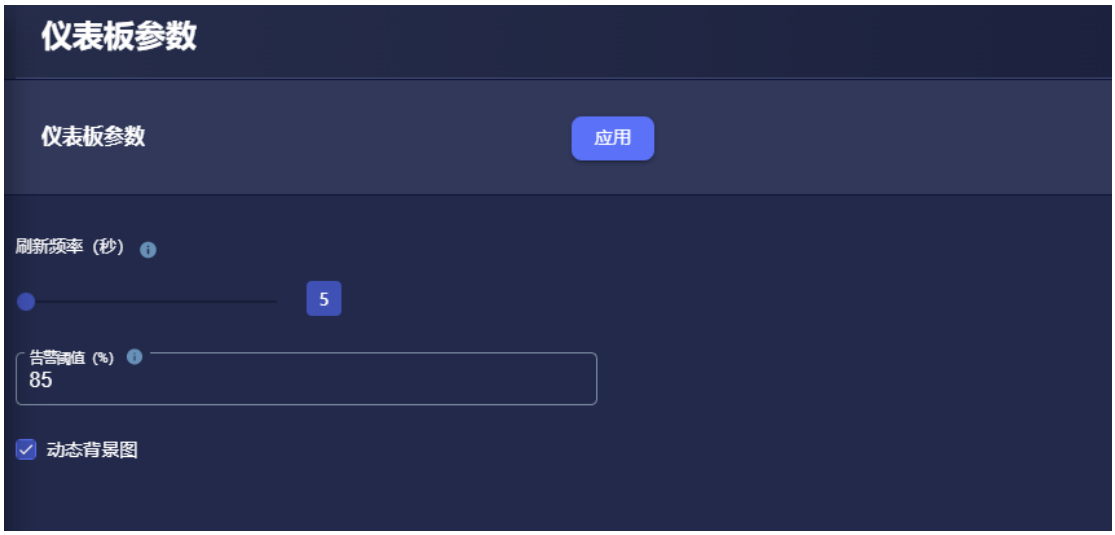

图 7-6 仪表板参数

利用率刷新频率（秒）： CPU、RAM 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。

利用率刷新 (%)：将在仪表板上显示告警的 CPU、RAM 和磁盘利用率百分比。 默认值：

85。

动态背景： 启用后，仪表板将显示动态背景。 默认值：启用。

7.3重启

图 7-7 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。

7.4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。AI 防护者的学习包含在两个文件中：用户定义策略 (UDP) 文件和预期使用指南 (IUG) 文件。 UDP 文件包含用户添加的所有策略。 IUG 文件包含由 AI 防护者自动创建的所有策略，包括监控持续的网站使用、监控安全客户端学习和监控安全发现学习。 备份会保存当前的 AI 防护者设置文件和学习模型。

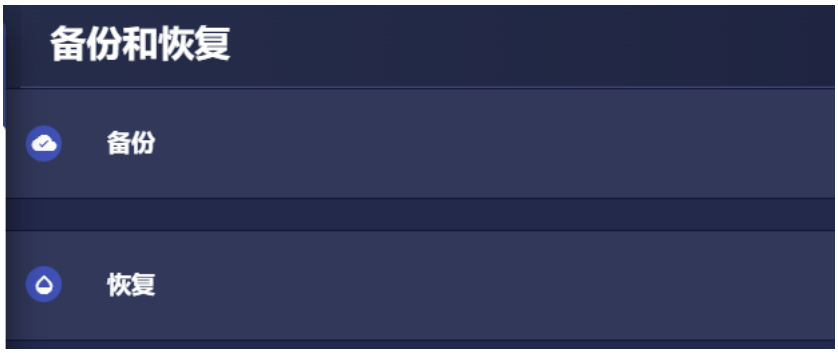

图 7-8 --备份和恢复

7.4.1 备份

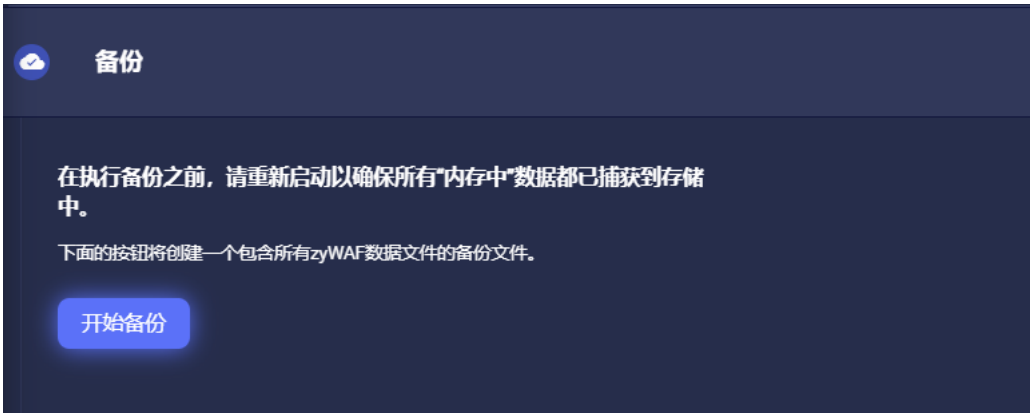

图 7-9 备份

点击 **开始备份** 创建并保存一组 AI 防护者备份文件。

7.4.2 恢复

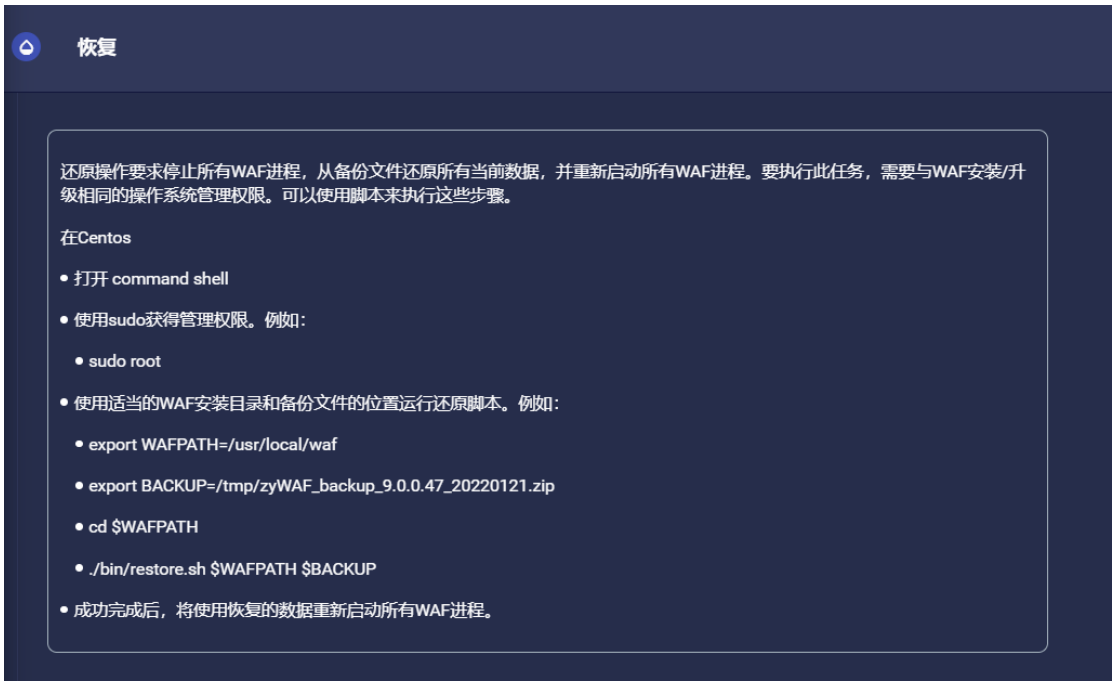

图 7-10 恢复

单击**选择文件并恢复**，将所有现有的 AI 防护者参数文件（设置、UDP 数据和 IUG 数据）替换为从选择框中选择的备份数据。

7.5健康检查

AI 防护者的设计保证了高可用性。 保障措施到位，以确保 AI 防护者的任何问题都不会阻止对网站的访问。 具体来说，有三项保障措施可确保 AI 防护者永远不会阻止流量到达网站：

1. AI 防护者作为服务安装，设置了操作标志，如果 AI 防护者服务停止，操作系统会自动重启 AI 防护者进程。 本次重启由操作系统完成，不依赖 AI 防护者。 这意味着只要操作系统在运行，AI 防护者服务就永远不会停止运行。

2. 在保护模式下运行时，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。 如果没有发生这种情况，健康检查会默认重启 AI 防护者。

3. 健康检查重启 AI 防护者 5 次（默认值）后，如果流量无法通过 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，无需检查。

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 7-11 健康检查

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。

禁用/启用：启用后，将以指定的指定时间间隔监控对选定网站的访问，如果该网站不可用，将采取指定的失败操作。默认值：启用。

健康检查间隔（秒）：这是健康检查检查网站可访问性的频率（以秒为单位）。默认值：60。

失败阈值：这是在健康检查将采取指定的失败操作之前网站必须连续无法访问的次数。默认值：3。

失败操作：这是当指定网站无法访问时，健康检查将采取的操作。默认值：重启 WAF。

重启失败阈值：当失败操作设置为重启时，这是健康检查将重启 AI 防护者以尝试恢复网站

可访问性的次数。在这个数字之后，AI 防护者将被切换到 Bypass 以便恢复网站访问。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：这是运行状况检查用来确定网站可访问性的 HTTP 返回代码。默认值：200。

方法：这是运行状况检查检查网站可访问性的 HTTP 方法。默认值：头。

URL：这是健康检查将检查网站可访问性的网站 URL。默认： /。

7.6用户管理

在初始安装 AI 防护者时，定义了一个用户：“admin”。 “admin”用户是内置的，拥有所有权限。 “admin”用户不能被删除。 建议在安装后定义至少两个新用户：一个具有“管理型用户”角色，另一个具有“审计用户”角色。 通过这种方式，您可以提供职责分离，以确保 AI 防护者得到适当的审计，并且审计日志不会被修改。

图 7-12 用户管理

用户管理列表显示了所有定义的 AI 防护者用户，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 AI 防护者用户。

用户名：这是创建用户帐户时为此用户创建的用户定义名称。

角色：这是创建用户帐户时分配给该用户的用户指定角色。 可用的角色有：General、System、Security 和 Audit。

这些角色具有以下权限：

系统管理员 - 此角色允许访问以下 AI 防护者菜单项：

- 仪表板
- 快速入门
- 系统
- 学习
- 帮助

安全管理员 - 此角色允许访问以下 AI 防护者菜单项：

- 仪表板
- 设置
- 告警
- 帮助

管理员 - 此角色允许所有功能，除了：

- 添加和删除用户
- 导出或重置审核日志

审计员 - 此角色允许“只读”功能。 审核角色不得更改 AI 防护者策略或重新启动 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：这是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。

7.7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 7-13 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：单击将清除所有审核日志条目。

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。

7.8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。

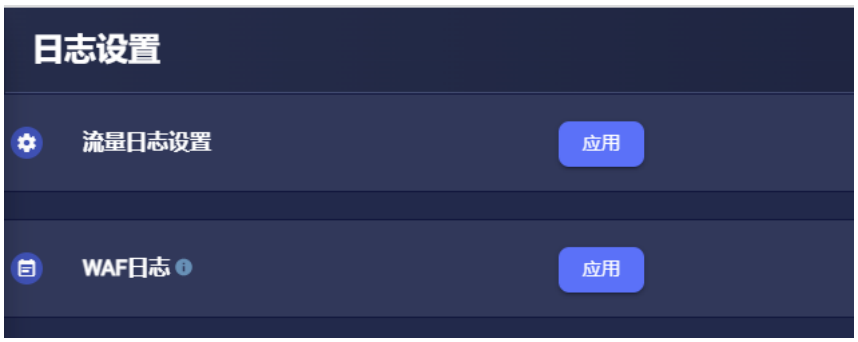

图 7-14 流量日志

7.8.1 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 7-15 流量日志设置

网站：此下拉菜单选择将记录流量的网站。

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：这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。 默认标签页

存档保留期。 这指定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。

7.8.2 WAF 日志

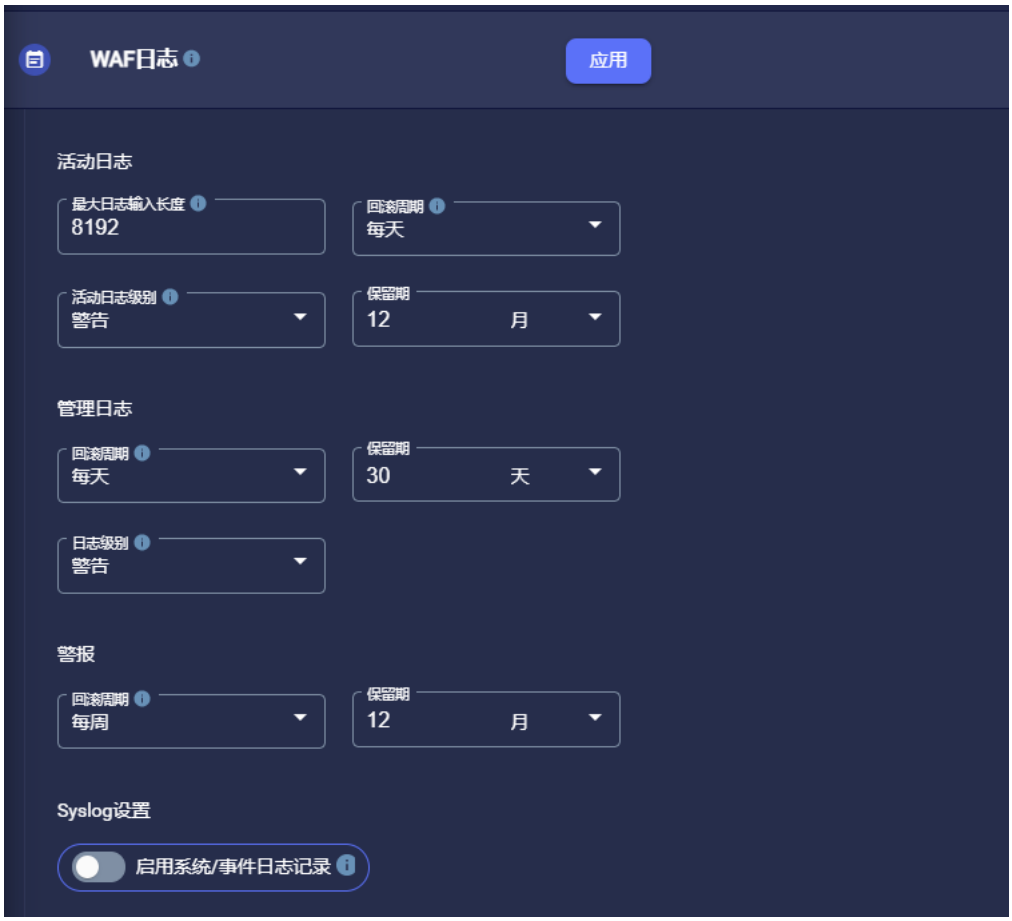

图 7-16 WAF 日志

活动日志

最大日志条目长度：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。

翻转期：这指定活动日志将关闭、重命名并启动新活动日志的月数、周数或天数。 默认值：每天。

活动记录级别：将记录的消息的最低严重性 [调试、信息、警告、错误]。 具有较小严重性的消息将不会记录在活动日志中。 默认值：警告。

存档保留期。 这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

滚动周期：这指定管理日志将关闭、重命名并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：这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 [调试、信息、警告、错误]。 具有出租人严重性的消息将不会记录在管理日志中。 默认值：警告。

告警日志

滚动周期：这指定告警日志将关闭、重命名并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：这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。

7.9日志文件管理

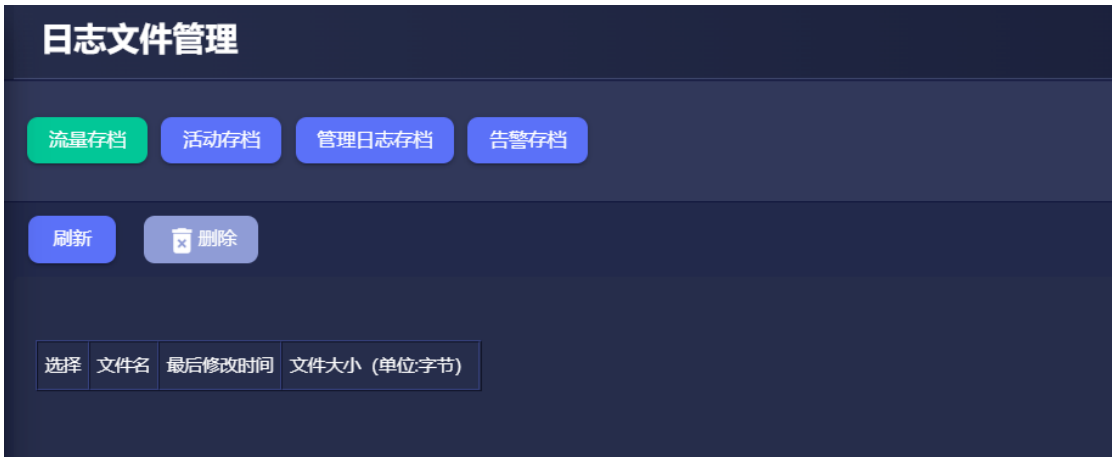

图 7-17 日志存档

流量日志存档

横幅右侧的数字是表格中流量归档文件的数量。

刷新按钮将更新表格的内容。

“删除”按钮将删除表格中已使用“选择”列中的复选框选中的所有文件。

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。

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

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。

WAF 活动日志存档

刷新按钮将更新表格的内容。

“删除”按钮将删除表格中已使用“选择”列中的复选框选中的所有文件。

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。

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

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。

WAF 管理日志存档

刷新按钮将更新表格的内容。

“删除”按钮将删除表格中已使用“选择”列中的复选框选中的所有文件。

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。

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

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。

告警存档

刷新按钮将更新表格的内容。

“删除”按钮将删除表格中已使用“选择”列中的复选框选中的所有文件。

RESTORE 按钮将文件中的告警恢复到当前告警表，该表使用告警菜单项查看。

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

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。

7.10 远程访问

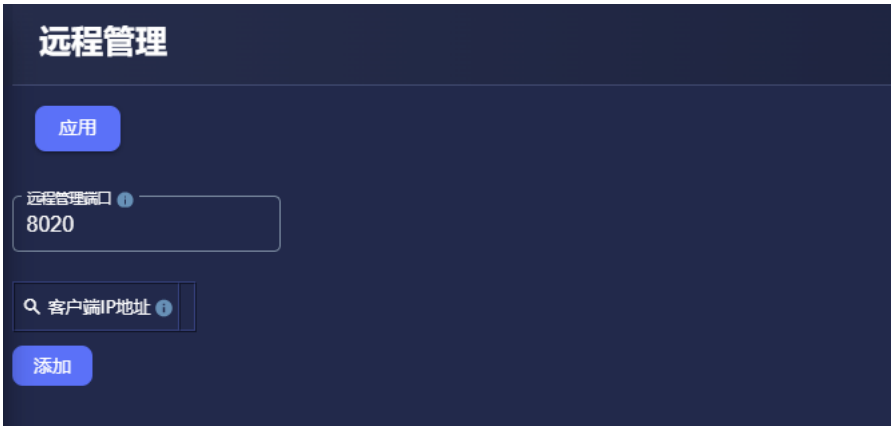

图 7-18 远程访问

远程管理端口：用于 AI 防护者管理控制台的 TCP 端口（本用户指南中描述的接口）。 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。

7.11 证书

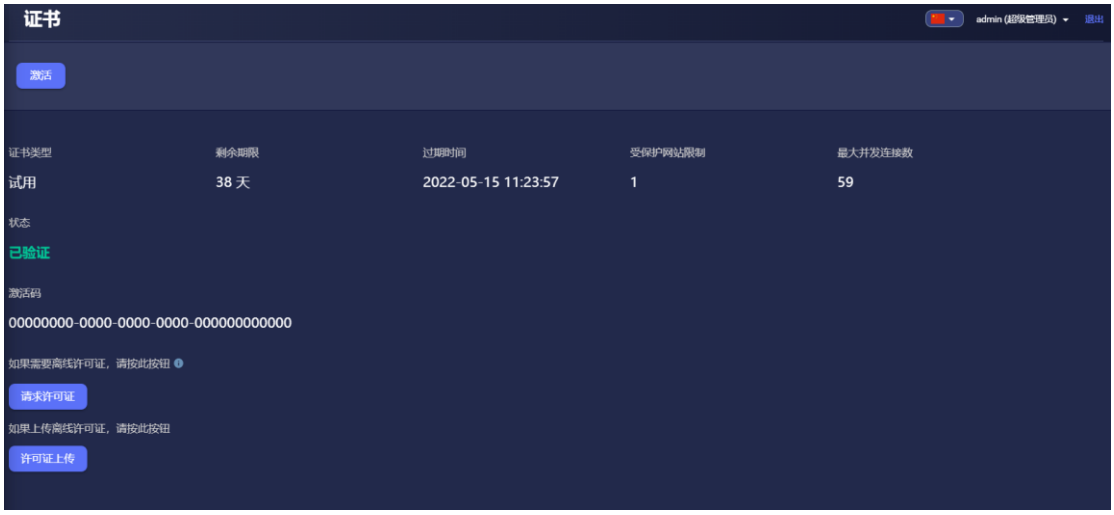

图 7-19 证书

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。将需要有效的许可证密钥才能将试用许可证替换为永久许可证。 颁发的永久许可证具有特定的到期日期和最大并发连接数。 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。 然后在新安装上重新激活许可证。*

许可证类型：当前使用的许可证类型。默认：试用

剩余许可证持续时间：许可证到期前的天数。 （值 -1 表示许可证已过期。值 0 表示许可证永不过期。） 默认值：45 天。

到期日期：许可证到期的日期和时间。默认值：45 天。

受保护网站的限制：可以受当前许可证保护的网站的最大数量。默认值：1。

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。）默认值：59

状态：许可证的状态 - 已验证、已过期。

激活密钥：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。

8 仪表盘使用

仪表板可从屏幕左侧的 AI 防护者左侧菜单访问。（图 3 1） 左侧菜单可以通过在没有文本的区域单击展开或折叠。

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。

8.1受保护网站

图 3-2 受保护网站

受保护的网站选择下拉菜单用于指定仪表板显示的数据。单击下拉列表会显示受 AI 防护者保护的所有网站的列表。

8.2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仪表板显示的数据。

注意： “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。

8.3检测到的威胁

检测到的威胁面板显示有关网站和 AI 防护者的摘要信息。

检测到的威胁：这是 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。

- **零日攻击**：AI 防护者在选定时间范围内为受保护网站检测到的威胁总数，这些威胁被归类为使用传统 Web 应用程序防火墙中发现的威胁签名不太可能检测到的威

胁总数 .

- **其他攻击**：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，这些威胁被归类为可能使用传统 Web 应用程序防火墙中发现的威胁签名进行检测.

8.4威胁历史

威胁历史面板显示在选定时间范围内 AI 防护者检测到的受保护网站的威胁数量。 威胁历史以柱状图显示。 每个柱状图的高度表示在 x 轴上指示的时间内检测到的威胁总数。每个柱都用颜色编码以显示零日威胁和传统威胁。

每个栏提供的信息是：

- **零日威胁**：AI 防护者在时间范围内为受保护网站检测到的威胁总数，这些威胁被归类为使用传统（无人工智能）Web 应用程序防火墙中发现的威胁签名不太可能检测到的威胁总数.

- **其他威胁**：AI 防护者在时间范围内检测到的受保护网站的威胁总数，这些威胁被归类为可能使用传统（无人工智能）Web 应用程序防火墙中发现的威胁签名进行检测。

8.5威胁国家

“按国家/地区划分的威胁源”面板显示 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。

8.6按 IP 地址阻止的 IP 请求

“按 IP 地址划分的威胁源”面板显示 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。

8.7按浏览器列出的威胁

按浏览器系列划分的威胁面板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。

8.8威胁统计-周

按周统计的威胁面板显示 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。

8.9威胁统计-天

按周统计的威胁面板显示 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。

8.10 威胁统计-过去 120 分钟

最近 120 分钟检测到的威胁面板显示最近 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。

8.11 当前状态

受保护网站状态：这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%。

一键恢复-单击按钮将用于消除状态为“高”的选项。

8.12 TCP 连接

TCP 连接面板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。

8.13 受保护的网站

受保护的网站面板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。

    - **监测**：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。

8.14 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。

8.15 威胁源 – IP 地址

威胁源-IP 地址面板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。

8.16 威胁源 - URL

威胁源 - URL 面板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 的左侧是针对该 URL 检测到的威胁计数。

8.17 系统资源使用 -CPU 使用率

系统资源使用 –CPU 使用率面板显示 AI 防护者应用程序和运行 AI 防护者应用程序的计算机系统的资源使用情况。

- **WAF**：此图显示了以百分比衡量的 AI 防护者的 CPU 使用率。
- 系统： 此图显示了运行 AI 防护者的计算机系统的 CPU 使用率（以百分比衡量）。

8.18 系统资源使用-内存使用率

系统资源使用 - 内存使用面板显示 AI 防护者应用程序和运行 AI 防护者应用程序的计算机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 防护者的计算机系统的内存使用率，以百分比显示。

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，其中将显示《AI 防护者用户手册》。

9.2提交诊断

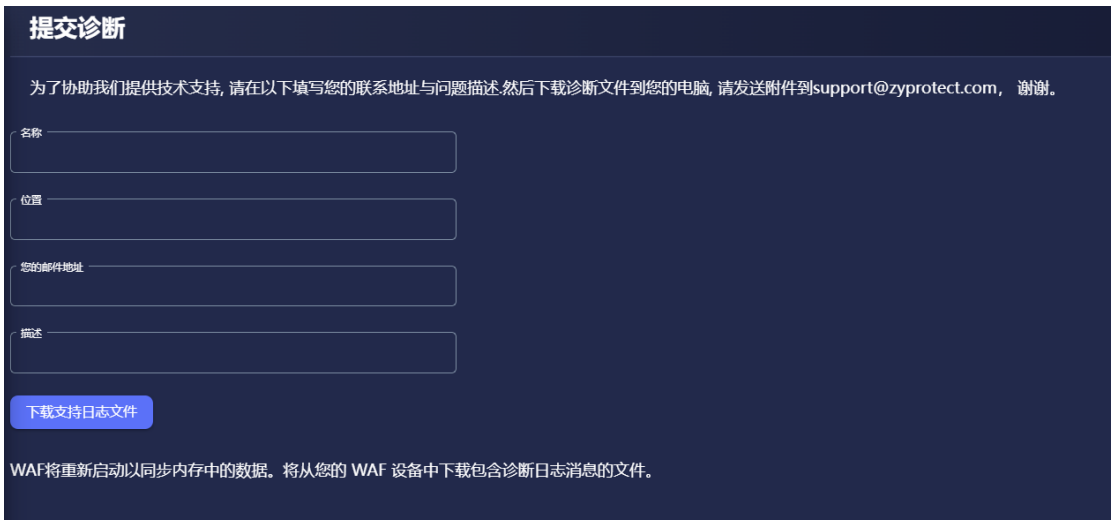

图 9-1 提交诊断

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。 单击此页面底部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。