TITANSEC

天泰 WEB 应用防火墙

用户管理手册(虚拟 WAF)

目录

图表索引

前言

文档范围

本手册将列出天泰WEB应用防火墙在云环境下（下文简称“vWAF”）有关的基本信息，并以云产品为例详细介绍WEB管理登录管理的所有功能的特点和使用方法。

期望读者

期望了解本产品主要技术特性和使用方法的用户、系统管理员、网络管理员等。本文假设您对下面的知识有一定的了解：

- 系统管理
- Linux 和 Windows 操作系统
- TCP/IP 协议
- HTTP 协议基础

格式约定

表示方式	表示结果
“粗体”	表示某一个功能菜单
“粗体”—“粗体”	连续性的菜单选择
粗体	表示必须注意
XXX	表示提示
XXX	表示技巧类提示

使用版本

本手册的适用版本：3.3.3版本及以上。

获得帮助

如需获取天泰 WEB 应用防火墙相关资料，请访问我公司官网：

http://www.titansec.com.cn

如需获取更为详尽、安全、专业的服务信息、商务信息，您可通过如下方式与我们联系：

客户服务热线：400-678-6569（手机和固定电话均可拨打）

Email：support@titansec.com.cn

一. 产品概述

1.1 概述

随着云计算的发展，企业和消费者都在利用云在新兴技术方面的优势。越来越多的用户采用了云服务商提供的云服务。但云上的威胁态势愈演愈烈，信息系统的攻击和破坏已经成为每日头条，企业希望能够防御新型威胁、风险和漏洞。云服务提供商正在通过参与网络安全信息共享来提升应对威胁的能力，企业也需要评估同云服务迁移、配置和采纳有关的风险因素，共建云安全。在云时代，企业需要建立新的网络安全体系。

在云计算环境中，位于 SaaS 层的应用服务依旧存在敏感信息被盗取和篡改的风险，使用云 WEB 应用防火墙（云 WAF）是确保 WEB 应用系统安全的唯一途径。云 WAF 同样拥有传统 WAF 所具有的功能，它通过非常细粒度的安全策略来保证 WEB 应用系统自身以及系统数据免遭各种攻击，可有效保护云服务器受到攻击、入侵，拦截 SQL 注入、XSS 跨站、文件注入、网站挂马等常规攻击，覆盖所有 WEB 安全攻击类型，防范恶意扫描，可根据应用灵活自定义安全规则。实时分析访问数据，快速发现黑客攻击行为，压缩优化 HTML、JS、CSS 等静态文件，降低带宽开销。云 WAF 是一种新型的可以保护 WEB 系统免遭攻击的信息安全设备。用户无需在自己的网络中安装软件程序或部属硬件设备，即可对网站实施安全防护。

1.2 典型部署

天泰云 WEB 应用防火墙可直接以虚拟机或服务的方式部署在私有云/公有云中，满足应用安全保证的可扩展性、性能弹性和管理维护的灵活性。虚拟化平台支持 VMWare、Hyper-V、Xen、OpenStack 等,部署灵活、便捷。

部署云 WAF，即把 WEB 服务器域名解析到 Web 应用防火墙提供的虚拟地址上，并配置被保护的服务器 IP；所有公网流量都会经过 Web 应用防火墙，过滤并处置恶意攻击流量，将正常流量返回给服务器 IP，从而确保应用服务的安全稳定可用。

图 1：网络部署示意图

二. WEB 界面管理

2.1 概述

WEB 管理界面为用户提供了更直观的人机交互方式，用户通过 WEB 管理系统实现对天泰 WAF 的管理和配置。

2.2 登录系统

登陆天泰 WEB 应用防火墙的 WEB 管理系统的步骤如下：

步骤 1：在阿里镜像市场申请天泰云 WAF 后阿里云会自动分配一个 IP 地址。

步骤 2：打开 IE 浏览器，用 HTTPS 方式访问：http://ip:8088。

步骤 3：在如图 2 所示的登录界面中，输入正确的用户名和密码（初始用户名 admin，密码 titan1qaz），并单击【登录】，即可进入 WEB 管理系统。

图 2：WEB 登录界面

登录系统注意事项：

- **建议使用 IE6.0 以上版本的浏览器，屏幕分辨率最好设置为 1024×768 及以上。**
- **初次使用本系统时可用默认用户登录（有关默认用户的初始账号，请参见附录 A2.1）。**
- **登录失败的原因有可能是：①用户名输入错误 ②密码输入错误 ③没区分大小写。**
- **登录本系统之前，请检查浏览器是否设置了禁止弹出窗口属性；如果是，请撤销此设置。**

2.3 页面布局

用户成功登录以后，进入系统当前运行的页面为概览页面，主要由以下几个部分组成：

2.3.1 导航栏

天泰 WEB 应用防火墙主要模块的菜单导航，通过其子链接可直接进入每个模块的功能菜单。

2.3.2 快捷功能栏

快捷工具栏包含了 WAF 当前用户登录账号、系统时间、用户登录注销等。点击其连接可分别进入详细配置页面。

点击时间，会出现修改日期时间窗口，修改后点击【确认】就修改完毕

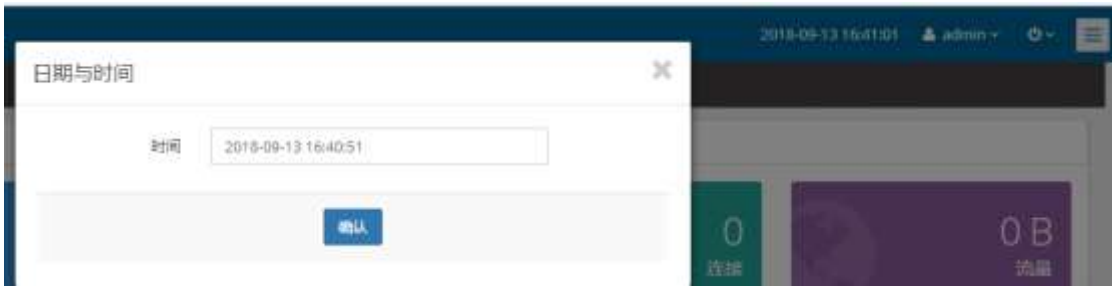


图 3 时间更改

点击登录账户，会出现三个菜单，分别为账户信息，更改密码和保存配置

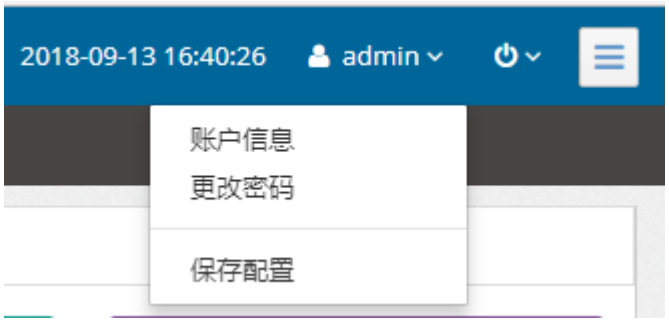


图 4 账户信息

点击账户信息，可以查看当前登录的账户信息

图 5 当前登录账号信息

点击更改密码，可以更改当前登录账户的密码

图 6 账号密码更改

点击保存配置可保存当前应用配置

图 4 中导航栏上  为：

退出登录：WAF 当前用户退出登录；

关机、重启：WAF 设备的重启、关机的快捷功能；

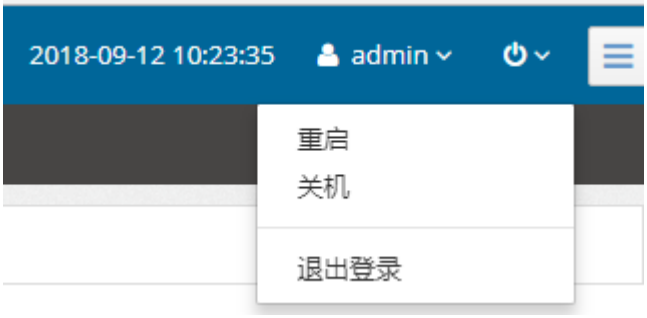


图 7：快捷工具栏

系统页面布局中的主菜单、子菜单和工作区会因用户权限不同，显示的内容不同；但在系统信息显示区和快捷按键操作区，所有用户的显示信息和操作权限都是相同的。

2.4 系统用户

天泰 WEB 应用防火墙(见下表 1)包括如下三类用户：

- 管理员：具有对系统的 WEB 界面进行管理、配置的权限，admin 为系统自带的缺省管理员。
- 审计员：具有查看系统审计日志的权限。
- 操作员：具有对系统的 WEB 界面进行管理、配置的部分权限。

表 1：系统用户信息

用户		权限
管理员	新建管理员 （由管理员创建）	具有除创建管理员和修改 admin 用户信息外的所有管理员权限
审计员	新建审计员 （由管理员创建）	只有查看审计日志和管理审计用户的权限
操作员	新建操作员 （由管理员创建）	只有查看及配置功能的权限

通过图 4 快捷功能栏处点击当前登录账号，可以对账号原始密码进行修改，admin 账号只能在该处修改。修改口令必须输入正确的旧密码，如果旧密码输入错误，则不允许修改口令。修改口令成功后，将在下次登陆时要求输入新的口令。

三. 系统状态

3.1 状态概览

状态概览实时记录了系统各部分信息的运行情况，包括**连接数**和**请求数**的近一小时变化趋势，**应用访问流量**和**安全事件**，**安全事件**趋势，**请求趋势**等信息。通过菜单可以快速的查看系统当前运行情况。

图 8 状态栏信息

3.2 系统概览

登入设备后，点击**概览**显示设备系统的概览页面。系统概览显示设备获取到的重要信息，包括：**安全事件**、**系统负载**和**接口流量**。

3.2.1 安全态势

安全态势分别展示设备运行以来各种威胁的统计图。安全事件主要对**攻击源 IP 数量**、**受攻击 IP 数量**、**受攻击域名**、**受攻击路径**、**触发安全规则**、**事件威胁等级**六个部分的信息进行统计。

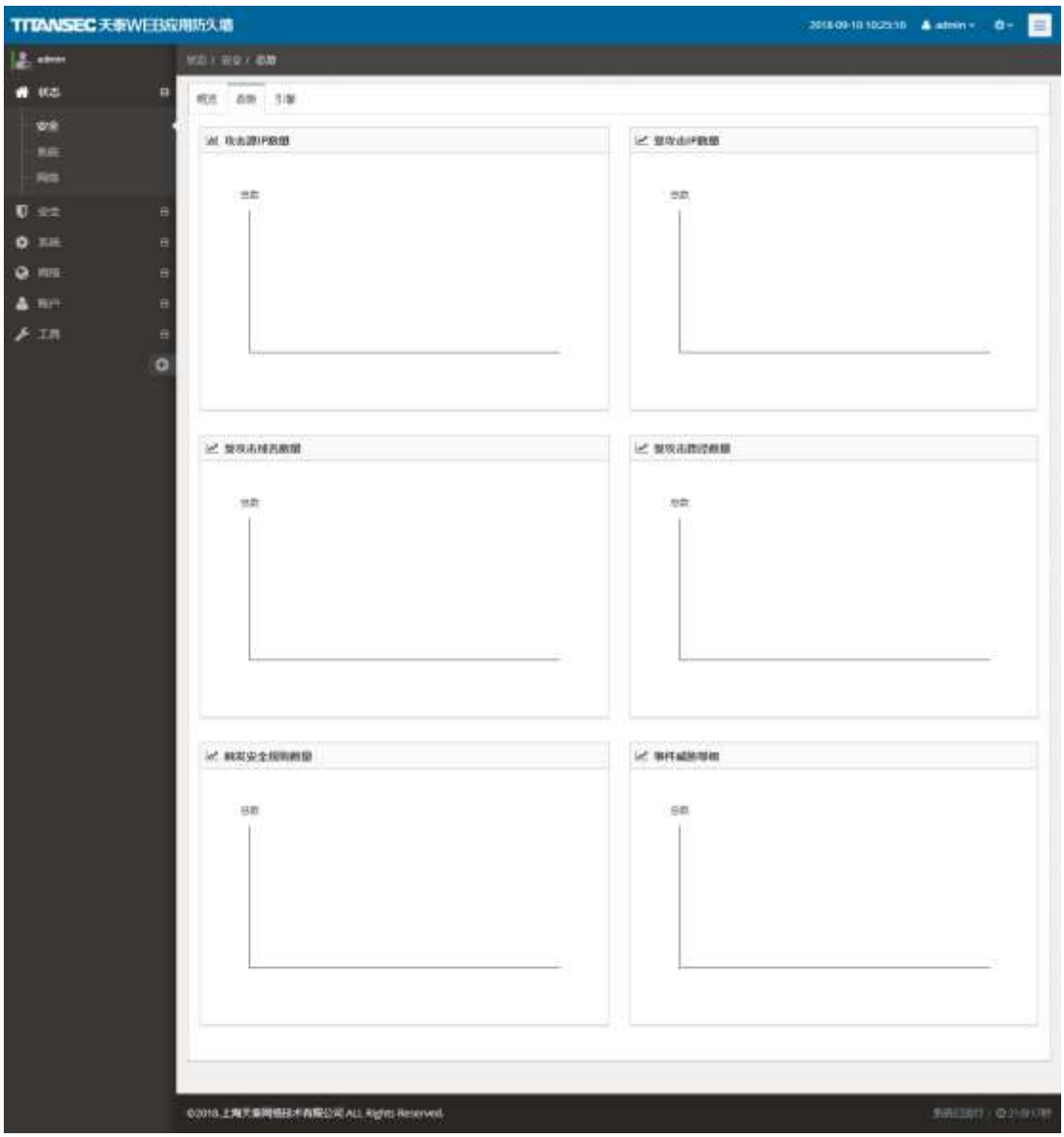


图 9 安全态势概览

3.2.2 引擎状态

引擎状态展示用户指定时间内设备网络连接情况，包括活动连接数，连接数/请求数、客户端响应码、服务端响应码、引擎流量（客户端）、引擎流量（服务器）它能记录设备当前时间段内设备的负载情况。

图 10 引擎信息概览

3.3 系统负载

资源部分包含了 CPU 和内存的使用率，防火墙连接数和系统负载。其数值均是实时显示当前设备的信息。**负载**是系统内设备的压力情况，通常按照 CPU 内核数来显示（例：双核 CPU 在负载超过 1 时，设备负载相应较大。该数值无单位）

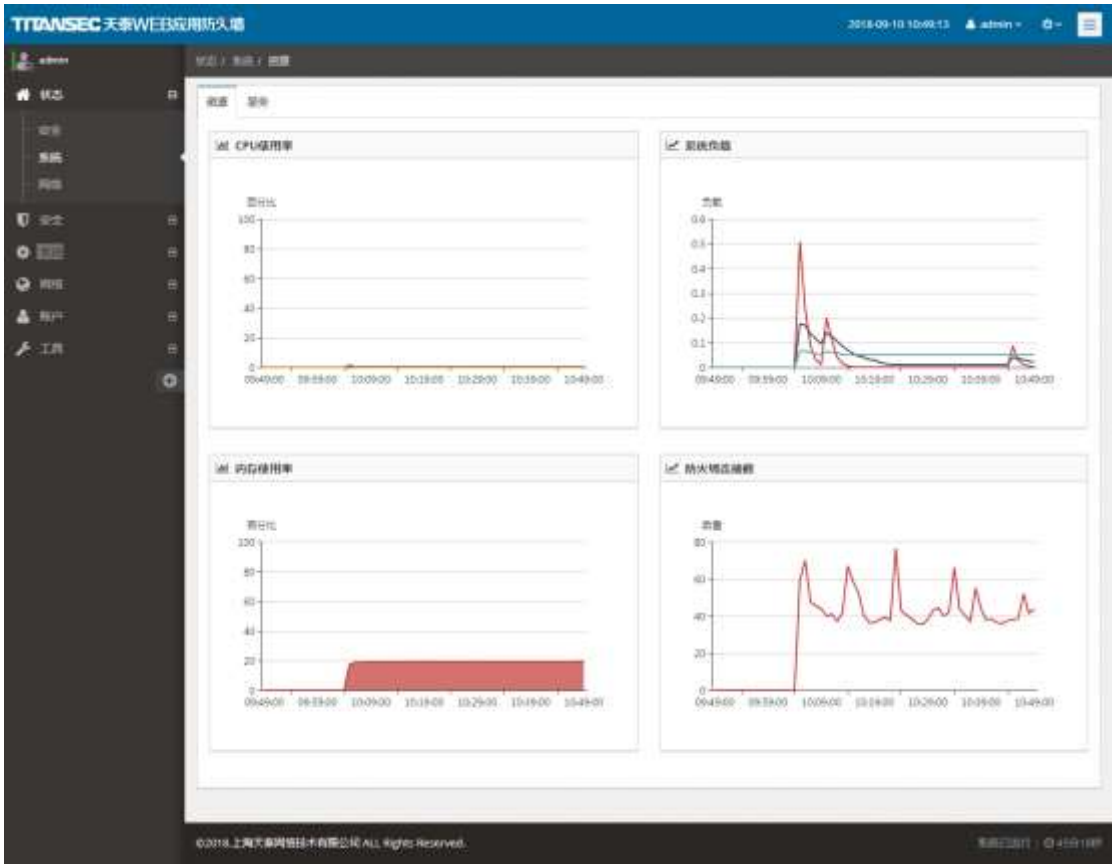


图 11：连接数和系统负载

部分低端型号设备不会显示磁盘和 CPU 的温度信息。

3.3.1 服务状态概览

查看各服务模块运行状态是否正常

图 12 服务状态概览

3.4 网络接口

系统概览页在网络部分会显示设备的所有物理网络接口的数量、介质、工作状态和速率等信息。发送（Byte）和接收（Byte）分别为该接口的发送流量和接收流量，该流量为设备累计叠加的数据流量，包括了非 HTTP 的流量如：FTP、视频等，也可以点击右侧 图标查看某接口实时的流量

图 13：网络接口

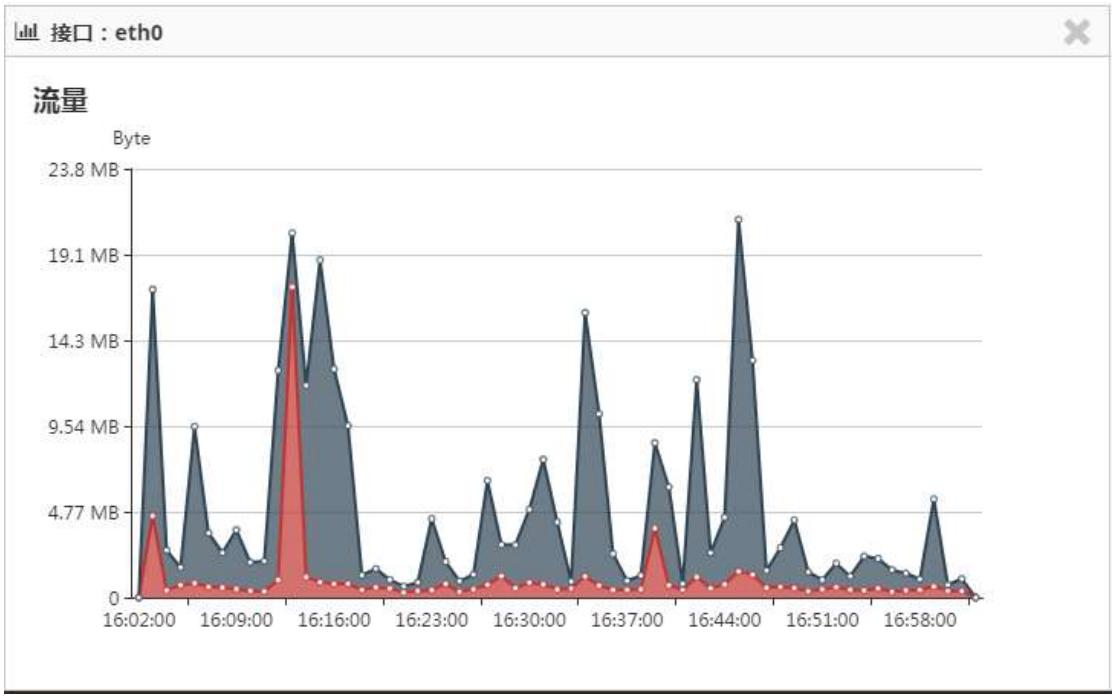


图 14 接口实时流量

3.4.1 ARP

ARP 记录显示设备获取到网络中所有设备的 MAC 地址和 IP 地址以及其所在的网络接口。

图 15 ARP 状态

3.4.2 路由

路由记录显示设备所有接口的接口地址和下一跳地址以及其所在的网络接口和目的网络。

图 16 接口路由状态

四. 应用配置

4.1 概述

应用配置模块为用户提供当前系统所有网站应用的配置，用户可以通过调整应用的安全防护、应用交付的各项参数，为用户提供全方位的防护。还为用户提供了添加、编辑等功能选项，方便用户对应用进行各项操作。

本章节介绍了应用的详细信息，包括控制台的运行状态、如何发布应用、设置安全防护、设置应用交付等功能的详细配置。

4.2 服务配置

登录设备以后，点击导航栏的**【安全】-【服务】**界面默认将进入到应用配置（WEB 站点列表），系统默认应用列表为空，添加新应用参见 4.4 章节。

若系统已存在站点应用，可以查看当前站点的基本配置、应用状态、以及服务器配置。如图所示：

图 17：WEB 应用列表

4.3 发布应用

发布应用之前，需要先确认 WAF 的部署模式，配置好网络接口和线路。

网络接口详细配置可以参考第六章节网络配置

线路详细配置可以参考 6.6 章节

在默认透明代理部署的情况下，你只要将被防护的站点进行添加配置即可，其他站点可直接放行不会对其造成影响。站点的添加可全新**添加**的配置这种方式实现。

如图所示为站点的添加功能。

4.3.1 添加 http 站点

点击【安全】-【服务】-【添加】添加 http 站点，具体详细配置见常规站点参数表。

图 18 添加 http 站点

4.3.2 添加 https 站点

点击【安全】-【服务】-【添加】添加 https 站点，具体详细配置见常规站点参数表

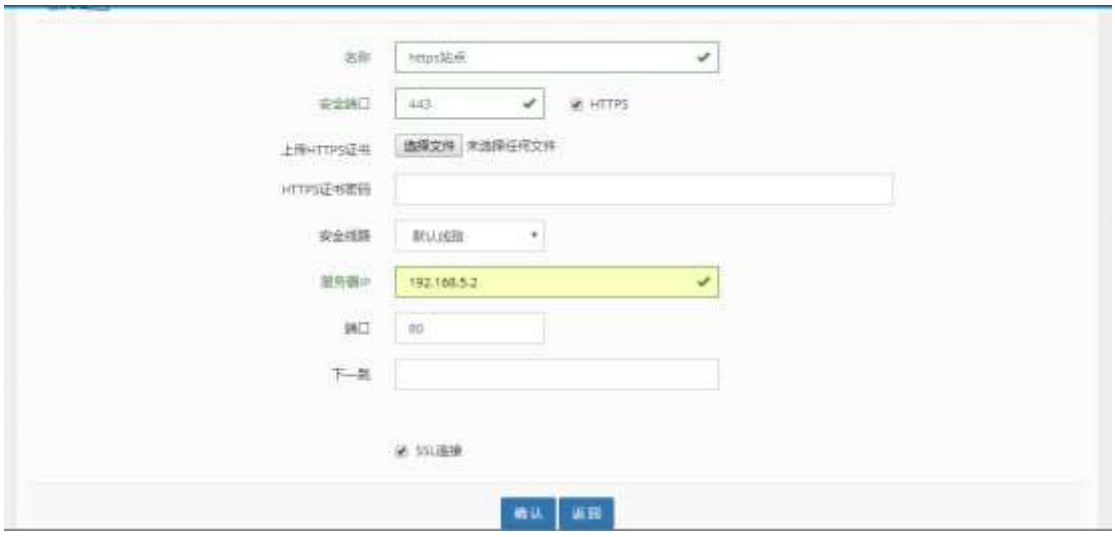


图 19：添加 https 站点

添加站点页面详细参数说明见下表 2：

表 2 常规站点参数

参数	说明
名称	站点名称，支持中英文
安全端口	Web 发布的访问端口
是否 HTTPS	是否是 HTTPS 网站
上传 HTTPS 证书	将服务器证书上传到 waf
HTTPS 证书密码	证书私钥密码
安全线路	服务经过 waf 哪条线路
域名	该站点可访问到的域名，包含 私网 IP 和公网 IP 地址
服务器 IP	后台真实服务器 IP 地址
端口	该站点访问端口
下一跳	WAF 发送数据包至下一个网络设备的地址
是否 ssl 连接	访问网站是否要 ssl 认证

添加完站点后页面如图所示：

图 20 站点添加

图 20 左侧为服务器的属性配置

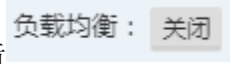
在*服务器*配置界面点击 可对后台服务器参数进行调整。

图 21 服务器参数设置

具体参数如下表 3 所示：

表 3 后台服务器参数

参数	说明
IP	后台服务器真实 IP
端口	服务器发布的端口
类型	服务器的类型
权重	当前服务器的权重，数字越高权重越高
最大连接数	后台服务器最大可用的连接数，通常默认，在后台服务器负载较高时可调低
下一跳	数据包至下一个网络设备的地址

点击 

按钮可以开启服务器的负载均衡配置如图

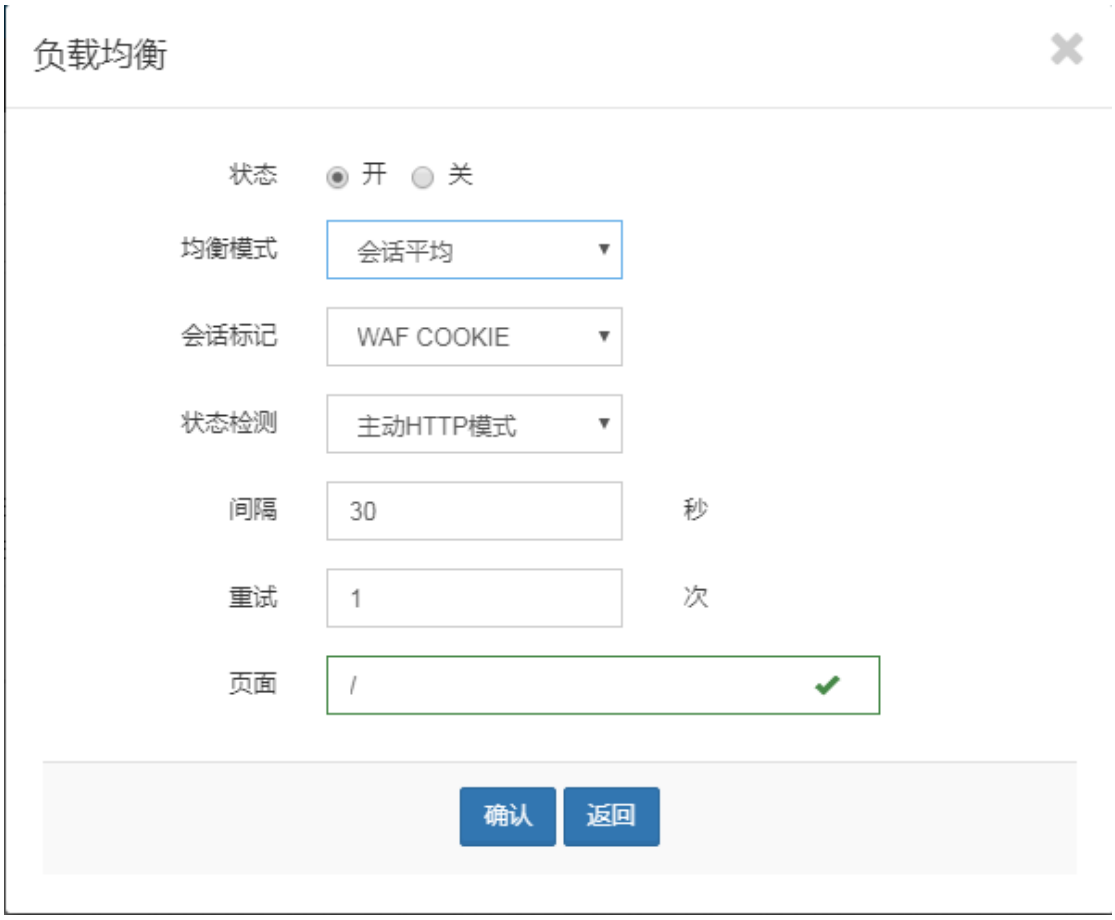


图 22 服务器负载均衡设置

表 4 服务器负载均衡参数

参数	说明
状态	负载均衡配置的开启或关闭
均衡模式	请求平均：按照请求数平均分配给后台服务器 客户端 IP 平均：按照客户端 IP 数量，平均分配后台服务器 会话平均：按照会话保持的方式分配给之前响应的服务器 服务器权重：按照服务器的权重大小来分配请求 服务器压力：按照服务器压力大小来分配请求
状态检测	TCP tcp 连接，如果连接成功，就说明后端正常 HTTP 发送 HTTP 请求，通过后端的回复包的状态来判断后端是否存活
间隔	间隔多久状态检测一次
重试	重复多少次认定不在线
页面	热备影响的路径
会话标记	会话标记来源 默认是 waf cookie

中间为站点信息配置点击 和 分别能够添加站点配置和编辑站点配置，点击 可以删除已有站点配置

图 23 添加站点

表 5 添加站点参数

参数	说明
域名	该站点可访问到的域名，包含 私网 IP 和公网 IP 地址
路径	网站访问的路径
路径区分大小写	是否区分路径的大小写
策略	防护策略选择
上传 HTTPS 证书	将服务器证书上传到 waf
HTTPS 证书密码	证书私钥密码

图 20 右侧为对服务的操作区域，可执行编辑、删除等操作，而 四个按钮功能分别为服务移至最上、服务向上移一位、服务向下移一位、服务移至最下，

 按钮可以暂停或开启服务（绿色表示开启服务，灰色表示暂停）

4.4 缺省防护

缺省防护是系统默认的防护策略，简单配置即能防护

图 24 缺省防护

表 6 缺省防护参数

参数	说明
状态	缺省防护开启或关闭
线路	服务经过 waf 哪条线路
策略	选择防护策略
服务器配置	要防护服务器的 IP 地址和端口
下一跳	数据包至下一个网络设备的地址

4.5 策略配置

1. 内置策略

内置策略包含默认模式、bypass 模式、审计模式。

默认模式：将基本防护开启，对攻击行为做出拦截。（具体防护参考本章节 4.5.1-4.5.13）

bypass 模式：将 waf 打通，不做流量拦截，直接通过

审计模式：对流量做行为审计后放行

2. 新建策略与复制策略

点击【添加】输入策略名称，即能新建策略，点击新建策略的【编辑】可对策略内部的防护选项做进一步配置。

点击【复制】输入策略名称（与已有策略名称不同）即可复制相同防护选项的策略，复制的策略也可对内部防护选项做进一步配置

可以通过建立不同的策略，分别针对不同的网站不同的安全需求进行防护

图 25 策略设置

4.5.1 攻击防护

天泰 WEB 应用防火墙通过内建过滤规则对 HTTP 数据包进行过滤检测，对已检测触发的攻击威胁将自动响应拦截该 HTTP 请求，保护网站不被受到攻击。天泰 WEB 应用安全防火墙可自定义防护路径，可以实现不同路径使用不同的安全策略和功能。

图 26 攻击防护

根据攻击防护参数表来根据需要配置

表 7：攻击防护参数

参数	说明
状态	攻击防护功能的开启与关闭
防护级别	关键防护：对网站的关键路径和关键文件进行防护 均衡防护：对网站的部分路径和文件进行防护，兼考虑访问速度与误报率 全面防护：对网站各个路径和所有文件进行防护
仿真模式	开启仿真模式后，waf 会识别记录所有攻击，但不会拦截
检测项	智能行为检测，基于异常评分对攻击行为进行智能检测
安全处理加速	安全处理加速功能的开启与关闭
HTTP 流加速	安全优先：访问速度会略微降低 速度优先：访问速度较快，安全检测项会少
动作	对触发规则的 HTTP 请求处理方式： **拦截并发送响应码**：阻止该次 HTTP 请求，发送错误码 **重定向**：触发操作规则以后重定向至指定页面或 URL **连接重置**：重新进行 HTTP 请求

	放行：降低严格过滤的等级大部分请求只记录不阻止，建议与告警配合使用
忽略异常请求	是否忽略异常请求
检测 cookie 中是否包含攻击内容	是否检测 cookie 中是否包含攻击内容
检测请求体中是否包含攻击内容	是否检测请求体中是否包含攻击内容
请求体检测阈值	检测文件的大小 不超过 999999KB

4.5.2 上传防护

为防止合法的用户上传了非法、恶意的文件，网站管理员账号密码泄露导致攻击者上传后门木马等文件，天泰 WEB 应用防火墙提供了上传防护功能，包括了用户上传行为的审计和 SHELL 脚本（动态页面脚本、CGI 脚本、服务器端 VBScript、伪装的 JPG 木马等）的检测，两个功能可独立使用。

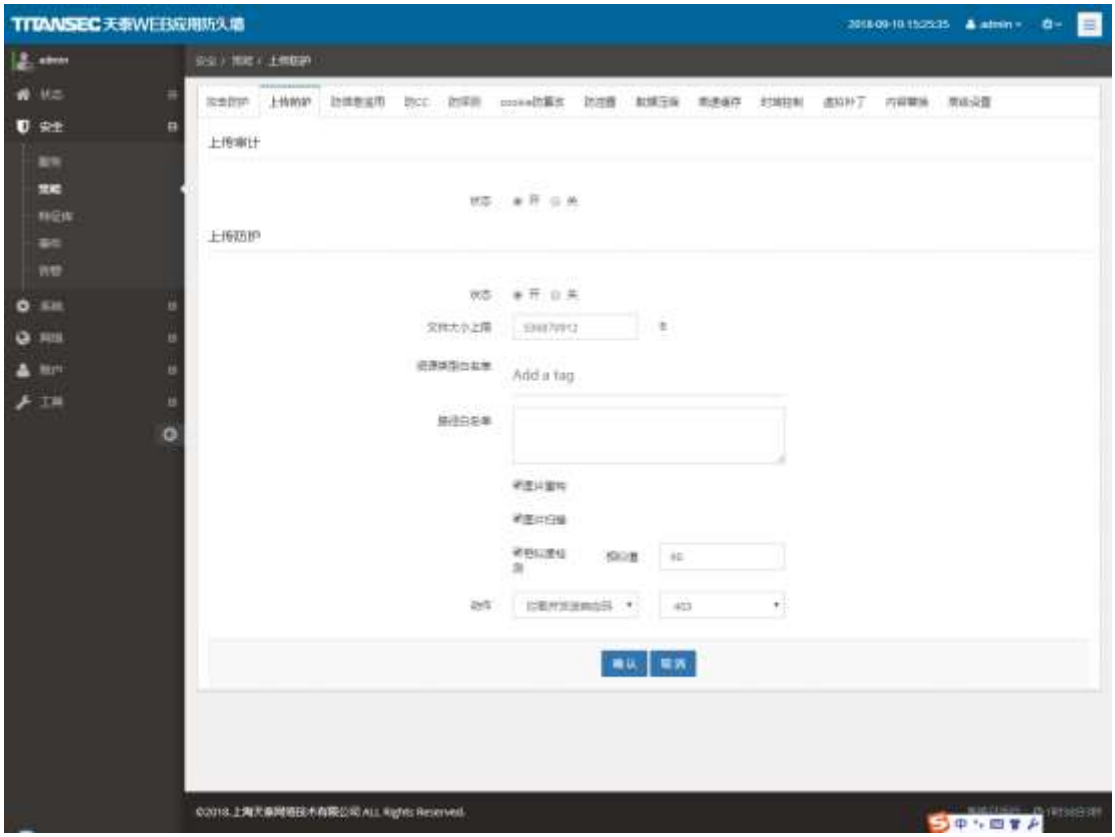


图 27 上传防护

图 32 所示，上传审计开启后可审计所有上传的文件，并对其进行记录。

上传防护参数见下表：

表 8：上传防护检测参数

参数	说明
状态	开启或关闭上传防护
文件大小上限	当上传文件超过这以大小后将不检查，适用于视频、音频等文件
资源类型白名单	添加白名单资源,一般指文件后缀名，例如：”txt”, “docx”, “jpeg”
路径白名单	添加上传路径的白名单，例如：”/”, “/admin/”, “/dashboard/how-to.jsp”
图片重构 图片扫描 相似度检查	开启或关闭功能，相似度可自定义
动作	对触发规则的 HTTP 请求处理方式： **拦截并发送响应码**：阻止该次 HTTP 请求，发送错误码 **重定向**：触发操作规则以后重定向至指定页面或 URL **连接重置**：重新进行 HTTP 请求 **放行**：降低严格过滤的等级大部分请求只记录不阻止，建议与告警配合使用

4.5.3 防信息滥用

WEB 盗链能够使服务器硬件资源、网络带宽资源严重消耗，但并不会增加被盗链站点的访问量，严重影响了被盗链网站的正常运行，天泰 WAF 通过检查 Referer 和 Cookie 两种方法来检测盗链的行为。

1）下载审计

下载审计开启后可审计所有下载的文件，并对其进行记录

2）防信息滥用

防信息滥用可防止外链盗取网站信息

3）点击劫持

可阻止或允许哪些能够被嵌入到 frame

4）自定义响应头

可添加 HTTP 响应头

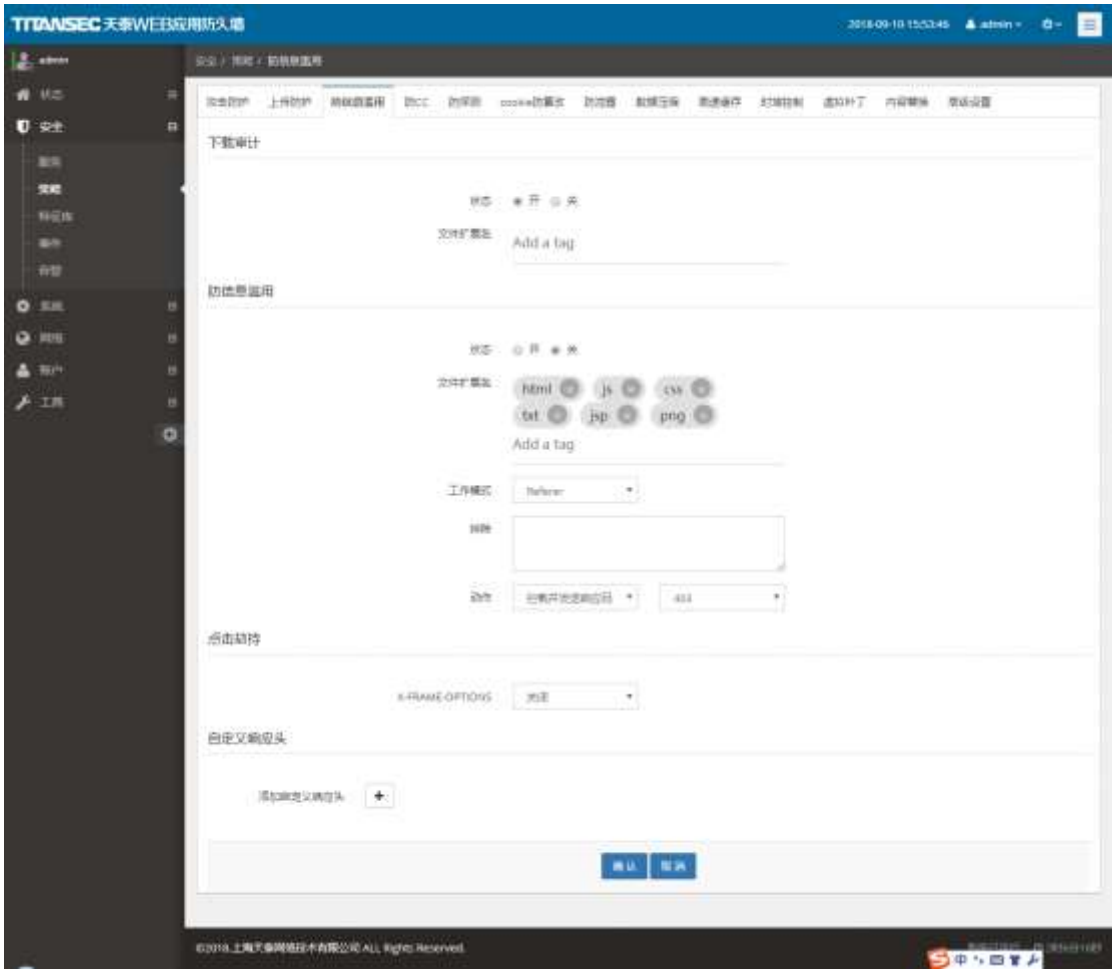


图 28 防信息滥用

表 9：防盗链参数

参数	说明
状态	开启或关闭防信息滥用
文件扩展名	文件扩展类型如 html、js、等
工作模式	**Referer**：针对 HTTP 应答中的 referer 字段进行检查，对迅雷等下载工具、视频、FLASH 无效

	Cookie：针对 HTTP 应答中 cookie 字段，无该站点 Cookie 的请求将被禁止访问
排除	盗链方式选 **Referer**，排除必须为正确的域名格式为 www.xxxx.com 盗链方式选 **cookie**，入口处填写访问入口路径，访问时不是从此路径访问的页面会触发规则，根路径是缺省值
动作	对触发规则的 HTTP 请求处理方式： **拦截并发送响应码**：阻止该次 HTTP 请求，发送错误码 **重定向**：触发操作规则以后重定向至指定页面或 URL **连接重置**：重新进行 HTTP 请求 **放行**：降低严格过滤的等级大部分请求只记录不阻止，建议与告警配合使用
点击劫持	X-FRAME-OPTIONS 关闭、拒绝任何域加载、允许同源域加载、自定义允许加载
自定义响应头	通过添加 HTTP 头来达到某些特定的效果

4.5.4 CC 防护

应用层 CC 攻击是当前对互联网应用的一个重要的危害。传统 DOS 攻击主要针对网络层，如 ICMP flooding，SYN flooding 等。然而针对应用层协议（如 HTTP）上的 CC 攻击，传统网络防火墙难以抵御。其攻击的主要目的除了消除带宽资源外，还将消耗主机资源等等。

针对这种应用层 CC 攻击，天泰 WEB 应用防火墙通过配置应用层 CC 攻击防护模块，能够极大缓解 CC 的攻击。

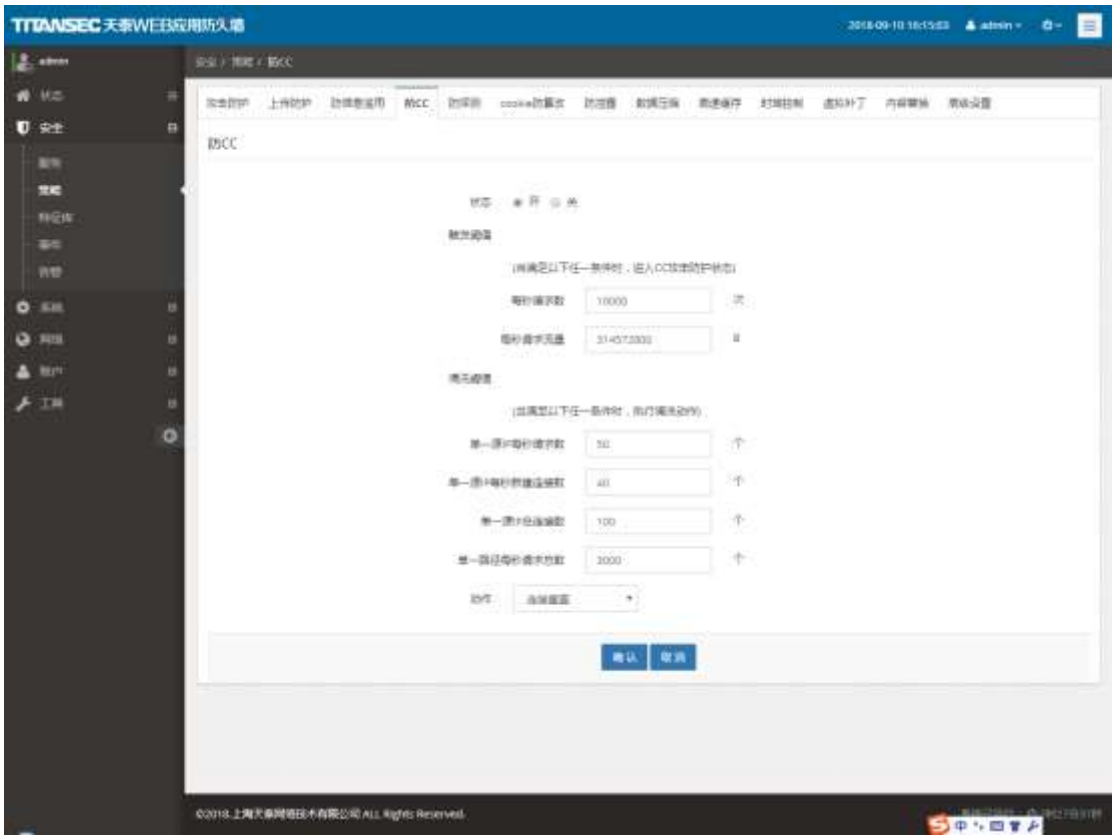


图 29 防 CC

CC 防护配置参数见下表

表 10：CC 防护参数

参数	说明
状态	开启或关闭 CC 防护
触发阈值	设置每秒请求数或每秒请求流量的阈值，超过即进入防 C C 状态
清洗阈值	设置单一源 IP 每秒请求数 单一源 IP 每秒新建连接数 单一源 IP 总连接数 单一路径每秒请求总数 任意一条超过即清洗阈值
动作	对触发规则的 HTTP 请求处理方式： **拦截并发送响应码**：阻止该次 HTTP 请求，发送错误码 **重定向**：触发操作规则以后重定向至指定页面或 URL **连接重置**：重新进行 HTTP 请求 **放行**：降低严格过滤的等级大部分请求只记录不阻止，建议与告警配合使用

	人机识别：只有当开启人机识别功能时生效。人机识别功能的使用请参考 4.5.5 章节

4.5.5 防探测

天泰 WEB 应用防火墙人机识别功能，可以针对那些没有完全实现浏览器功能的简单 HTTP 客户端，如扫描工具，爬虫等工具攻击网站时做出处理

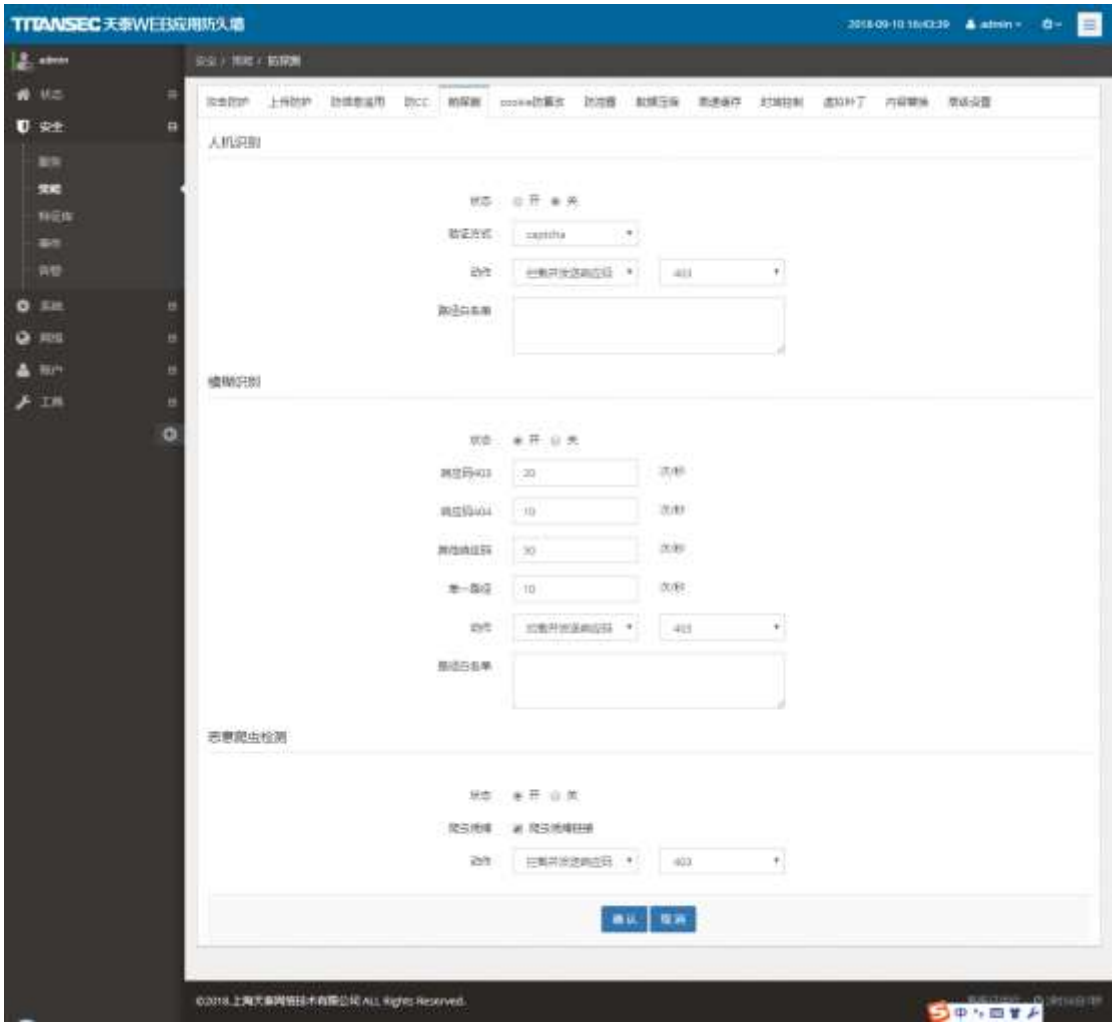


图 30 防探测

1）人机识别

可以通过验证码或 JS 方式，判断访问者是人还是工具扫描

表 11：人机识别参数

人机识别参数	说明
状态	开启或关闭人机识别，只作用于当前路径下
验证方式	Captcha(验证码)或 js
动作	拦截并发送验证码、重定向、重新连接、放行
路径白名单	设置白名单路径不检测

2）模糊识别

用现有识别的数据去和自己的设置去进行匹配，然后根据最大隶属度原则进行归类识别

表 12 模糊识别参数

模糊识别参数	说明
状态	开启或关闭模糊识别，只作用于当前路径下
响应码	403、404 次数，其他响应码次数
单一路径	探测路径的次数
动作	拦截并发送验证码、重定向、重新连接、放行
路径白名单	放行探测的路径

3）恶意爬虫检测

检测是否有恶意爬虫对网站安全造成损害

配置参数见表 13。

表 13 恶意爬虫检测参数

恶意爬虫检测参数	说明
状态	开启或关闭恶意爬虫检测
爬虫诱捕链接	开启或关闭爬虫诱捕链接
动作	拦截并发送验证码、重定向、重新连接、放行

图 31：人机识别

4.5.6 COOKIE 防篡改

针对 Cookie 安全要求较高的站点，天泰 WEB 应用防火墙可以使用 Cookie 防篡改来实现防止客户端 Cookie 被篡改的威胁。

图 32：Cookie 防篡改

表 14：Cookie 防篡改参数

参数	说明
状态	开启或关闭 Cookie 防篡改
模式	后缀模式或签名模式
排除 cookie	排除信任的 cookie 文件
动作	拦截并发送验证码、重定向、重新连接、放行
加密	开启或关闭加密 cookie 选项

4.5.7 防泄漏

服务器在异常状态下，可能会暴露版本信息，可以隐藏相关配置项

图 33 防泄漏

表 15 防泄漏配置参数

参数	说明
显示阻断信息开关	开启或关闭显示阻断信息
隐藏应用程序和版本标识	隐藏应用程序和服务器的版本号
隐藏服务器类型	隐藏服务器类型开关

4.5.8 数据压缩

当部分 WEB 站点响应的内容过大时，可使用 WAF 的页面数据压缩，以节省带宽，提高传递效率。

图 34 数据压缩

数据压缩配置参数见表 22：

表 16：数据参数配置

参数	说明
状态	开启或关闭数据压缩功能
文件大小下限	低于该数值的数据流将不被压缩
性能	WAF 对文本页面的压缩率 正常、平衡、最佳三选项
压缩类型	指定被压缩数据的类型，压缩类型为 Content-Type 参数的值，一般文本压缩率最大，包含 text/html, text/xml, text/css 等

4.5.9 高速缓存

在应用触发设定的高速缓存规则时，系统会自动缓存一些页面和文件，之后用户访问这些页面时会自动显示已缓存的页面内容，加快访问 WEB 应用的速度。同时使用高速缓存可以在应用的某些页面出错后让用户访问出错前的正常页面，用户感觉不到页面出错，使应用页面出错的影响降低。

本功能可在根路径及指定路径下生效，参数信息见下表

表 17：高速缓存常规参数

参数	说明
状态	开启或关闭高速缓存
更新时间	缓存更新的时间间隔
缓存前请求	缓存之前请求的次数，到达这个数值以后开始缓存
请求文件扩展名	请求文件扩展名一般为文件后缀名，例如：html, txt 等
响应资源扩展名	响应资源扩展名为 Content-Type 参数的值，例如：text/html, image/png 等
排除路径	将不需要进行缓存处理的路径，加入排除路径列表

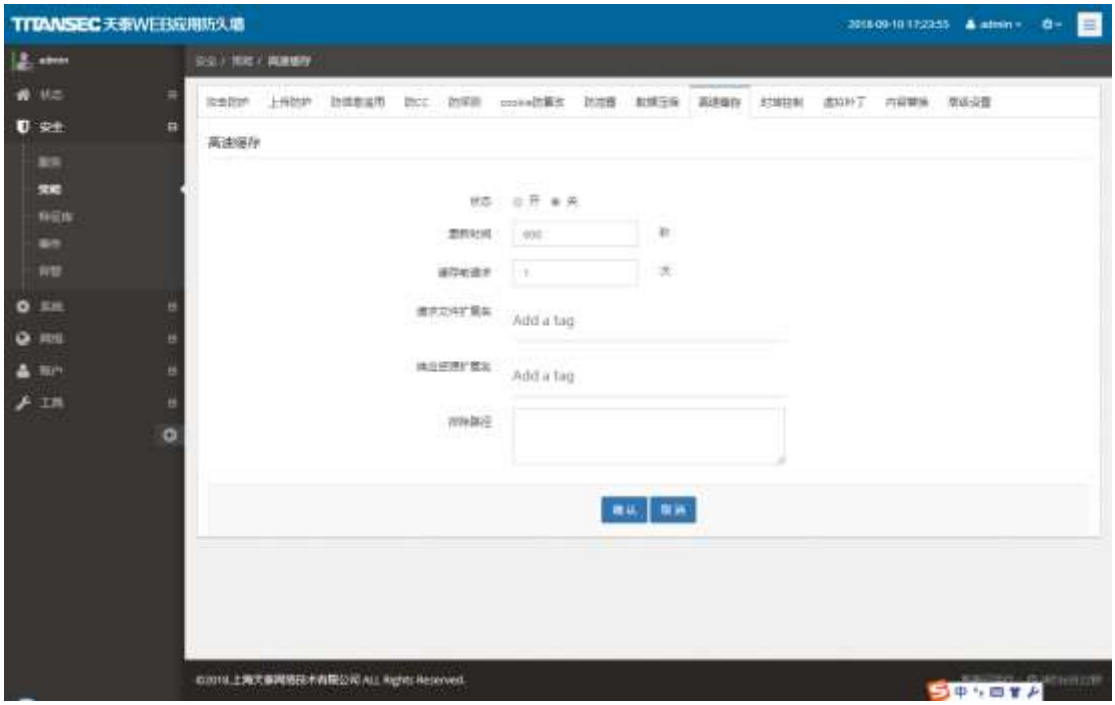


图 35：高速缓存常规配置

4.5.10 时域控制

天泰 WAF 时域控制通过控制来源 IP 地址，在指定时间内访问网站或自定义访问区域的特定路径的权限，如放行、阻止、信任等功能。

点击【添加】可添加时域控制策略

图 36 添加时域控制

如图 31 所示，添加新时域控制内容，需要指定区域对象，区域对象的详参数配置见下表 17:

表 18：时域控制参数

参数	说明
区域	选择需要控制的用户，自定义可指定 IP 段地址 ，也可取反值

	例如 192.168.0.0-192.168.255.255
时间	选择控制时间
取反	仅仅对当前的区域对象行为选择反向控制
动作	对触发规则的 HTTP 请求处理方式： **拦截并发送响应码**：阻止该次 HTTP 请求，发送错误码 **重定向**：触发操作规则以后重定向至指定页面或 URL **连接重置**：重新进行 HTTP 请求 **放行**：降低严格过滤的等级大部分请求只记录不阻止，建议与告警配合使用
域名	需要控制的网站域名
路径	需要控制的网站路径
请求方法	可选择 GET、POST、PATCH、DELETE、PUT 等五种请求方法

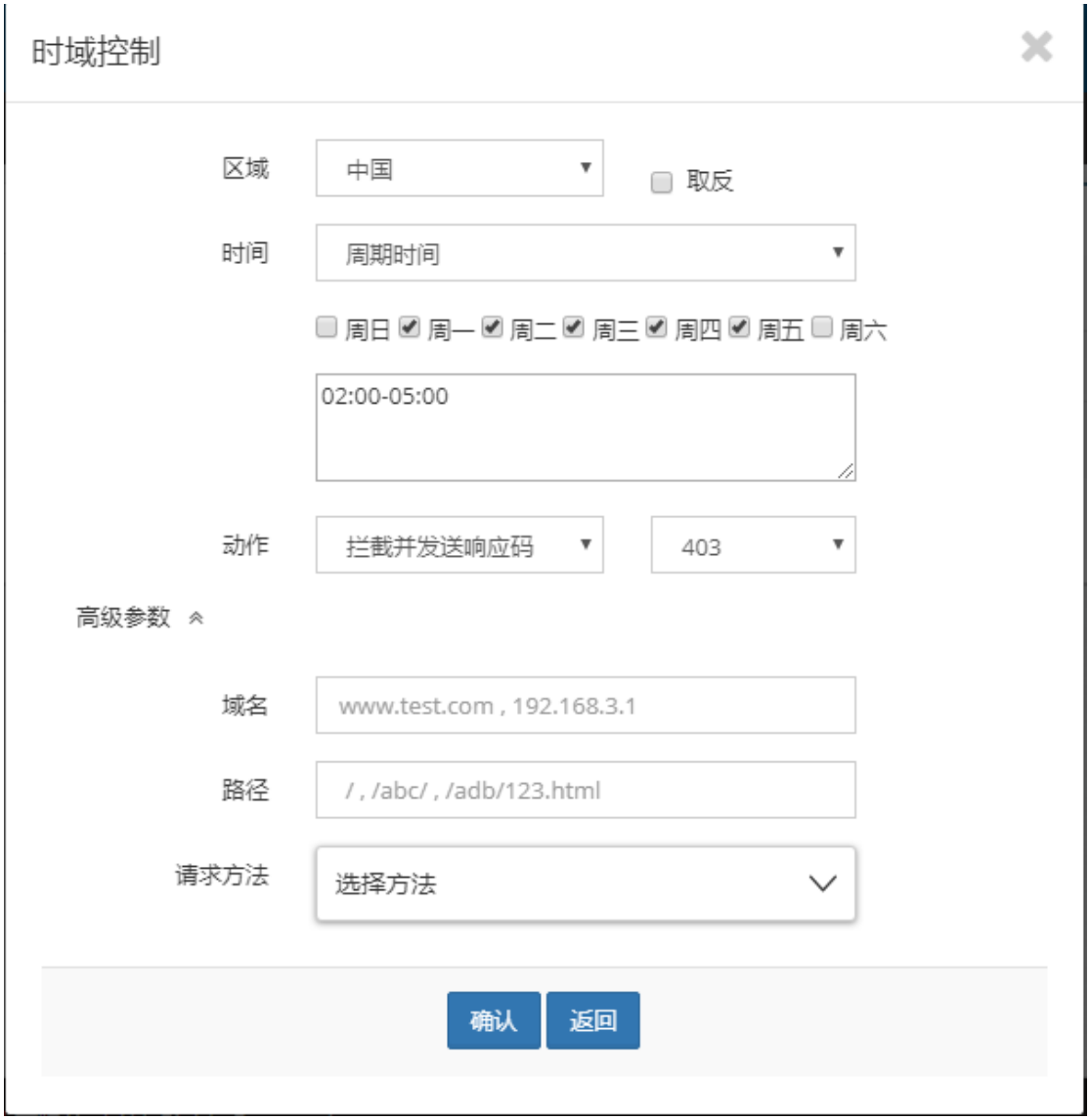


图 37：时域控制参数

4.5.11 虚拟补丁

为防止攻击防护功能所内置的防护规则针对 WEB 应用的动态页面无法覆盖到所有的攻击手段，以及防止 0 DAY 的攻击，通过配置天泰 WEB 应用防火墙的虚拟补丁功能实现更为严格和准确的防护体系。

表 19：虚拟补丁参数-1

参数	说明
排名	虚拟补丁的优先级
规则	可自定义规则，参数值类型可用正则表达式定义　如下接收字符串的规则示

	例 名称：表单提交的参数名称 特征：所提交参数值的类型特征（正则表达式定义） 选择 ：选择特征对象（选择后可编辑） 长度范围：定义参数值的长度最小、最大值 例如 receive [a-zA-Z0-9-_]* 1->5 名称：receive 特征：简单字符串 特征对象：a-zA-Z0-9 长度:在 1 到 5 之间
描述	对于规则的描述
动作	对触发规则的 HTTP 请求处理方式： **拦截并发送响应码**：阻止该次 HTTP 请求，发送错误码 **重定向**：触发操作规则以后重定向至指定页面或 URL **连接重置**：重新进行 HTTP 请求 **放行**：降低严格过滤的等级大部分请求只记录不阻止，建议与告警配合使用
域名	虚拟补丁生效的网站域名（缺省为对所有域名下该页面生效）
路径	虚拟补丁生效的网站路径
请求方法	可选择 GET、POST、PATCH、DELETE、PUT 等五种请求方法

图 38：虚拟补丁

4.5.12 内容替换

点击【添加】内容替换，通过设置替换内容可以批量替换服务器 HTTP 应答内容的内容。可替换的类型有网页中的文本、JS、CSS、XML 等内容。

例如 将/index 页面中的 welcome 替换为 欢迎 就如图所示，将替换前与替换后的内容填入即可，替换内容支持正则表达式，可做更为准确的匹配替换，参数配置见下表 30：

表 20：内容替换参数

参数	说明
替换第一次匹配的内容	只替换第一次匹配到的内容

域名	要替换的域名
路径	要替换的路径
请求方法	对所选请求方法下的页面执行内容替换，允许选择 GET、POST、PATCH、DELETE、PUT 等五种请求方法
响应码	对指定响应码的 http 请求页面进行内容替换，响应码可以是 200, 403, 404 等
数据类型	选择需要替换内容的 MIME 类型，text/html 是缺省选中的数据类型，不显示在页面上

图 39：内容替换

4.5.13 高级选项

高级包括 location 头转换、x-forwarded-for、真实 IP 来源。当需要响应头重定向时采用 location 头转换，识别通过 HTTP 代理或负载均衡方式连接到 Web 服务器的客户端最原始的 IP 地址的 HTTP 请求头字段开启 x-forwarded-for。

表 21：高级选项参数

参数	说明
LOCATION 转换	当网站 LOCATION 重定向到与其他 URL 或端口时配置进行转换的 URL 或部分 URL，每行 1 条规则，中间使用“=>”分割，例如： http://xx.com=>http://zz.com:82 example.com=>test.com.cn
x-forwarded-for	选择识别真实 IP 的模式，模式有保持、替换、附加三种
真实 IP 获取来源	选择从哪里获得真实 IP

图 40：应用交付高级设置

五. 事件告警

5.1 概述

事件告警模块是对所有的系统事件，安全事件，拦截日志，告警通知的统一管理，通过查看系统事件，了解本系统最近的操作动作，查看操作结果，并根据操作结果得到的系统配置进行防护的过程中得到安全事件、拦截日志，最后根据不同的事件条件，定制不同的响应策略，从而使系统管理人员及时有效的对系统进行管理。

5.2 安全事件

5.2.1 事件

安全事件分为查询和事件两个部分，查询功能主要在海量日志下可以准确定位需要查找的攻击日志信息，事件部分记录了所有的攻击日志

查询参数见下表 37：

表 22：安全事件参数

参数	说明
开始时间	输入需要查询的开始时间
结束时间	输入需要查询的结束时间
级别	选择需要查询的事件级别
特征名称	输入需要查找的攻击特征名称
源地址	来源 IP 地址
方法	选择需要查看的事情的请求方法
域名	输入需要查找的网站域名
路径	输入需要查找的网站路径
动作	选择事件发生后采取的动作
事件 ID	根据 ID 查找事件

图 41：安全事件查询功能

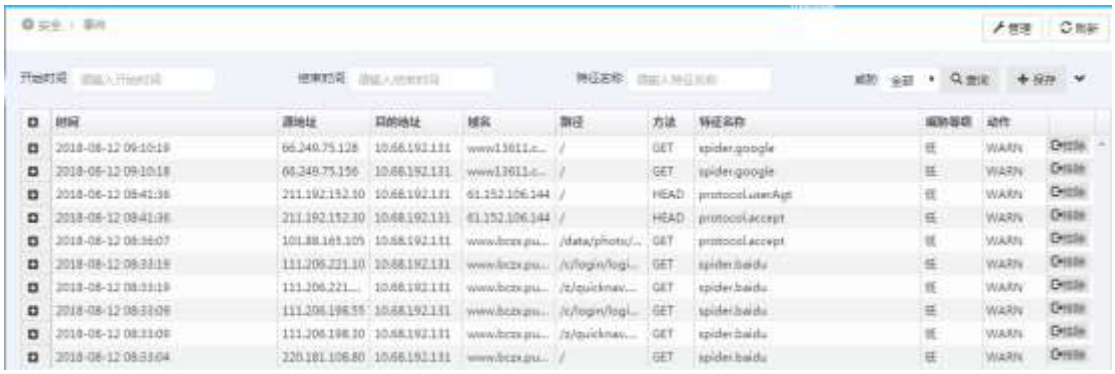


图 42：攻击日志列表

图 60 所示列表为设备所记录并拦截的所有日志内容。

点击【排除】可显示该次事件类型中访问路径所触发的特征规则如图 61，每一条路径可匹配一下所有规则。

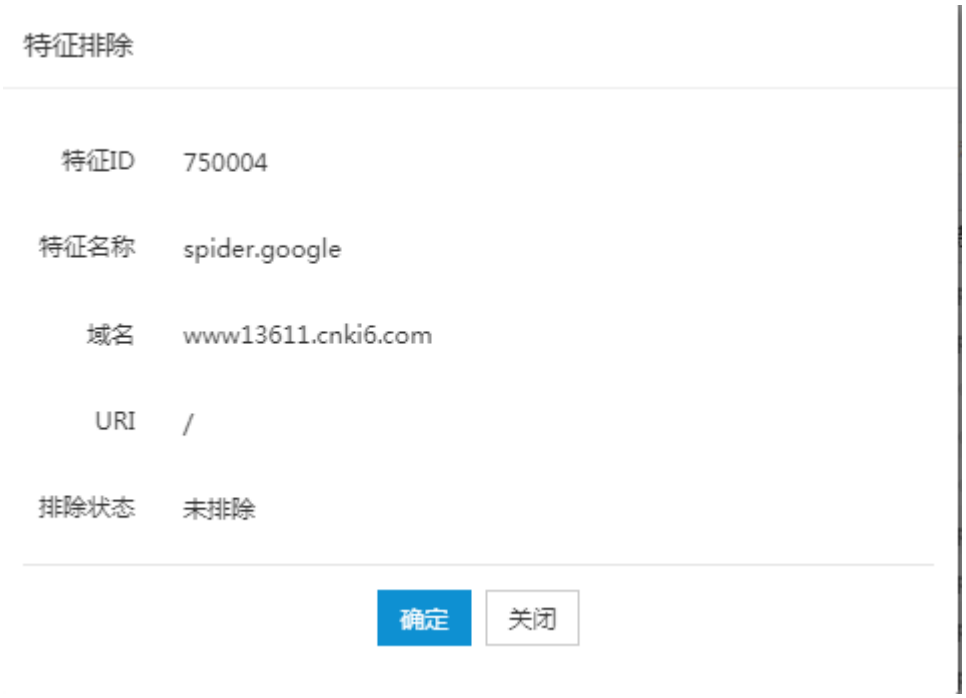


图 43：规则排除

5.2.2 告警

告警信息

针对不同的告警条件，配置不同的响应策略，触发这些规则时进行告警响应，响应包括了邮件告警和 IP 阻断。告警响应包括一些告警规则和已产生的告警响应。如图 64 所示，分别为添加告警信息内容和显示发生告警信息的内容，包括邮件通知和 IP 阻断。

1. 配置事件告警

点击【添加】按钮新增告警

图 44：告警通知配置

表 23：告警配置参数

参数	说明
告警配置名称	该条告警的名称
告警等级	该条告警所显示的危急等级
攻击类型	选择告警包含的事件类型，可以添加多个，不能重复
事件等级	选择触发告警的事件类型重要等级

安全策略	选择采取的安全策略
发生次数	事件发生次数，取值范围 1-999
时间范围	事件发生的时间范围，取值为 1-60 分
IP 阻断	选择是否启用告警 IP 阻断
阻断时间	配置 IP 阻断的时间，单位为分钟，取值范围 1-72000
邮件通知	是否用邮件通知该条告警信息
电子邮件地址	配置接收该告警的电子邮件地址。

2. 告警历史查询

可根据时间和名称条件查询

图 45 告警历史查询

3. 告警的动作策略

3.1 添加 IP 阻断

1） ip 阻断列表查询

点击【阻断 IP 列表】，下图为被阻断 IP 的列表，当有攻击发生时触发告警以后该 IP 地址将从网络层拦截，该 IP 无法访问网站，只有在该处解除阻断以后方可继续访问。

图 46：阻断 IP 列表

2） ip 白名单

可点击【白名单】，添加信任 IP 列表，信任 IP 列表里面的 IP 不会阻断，除信

任 IP 之外的全部阻断

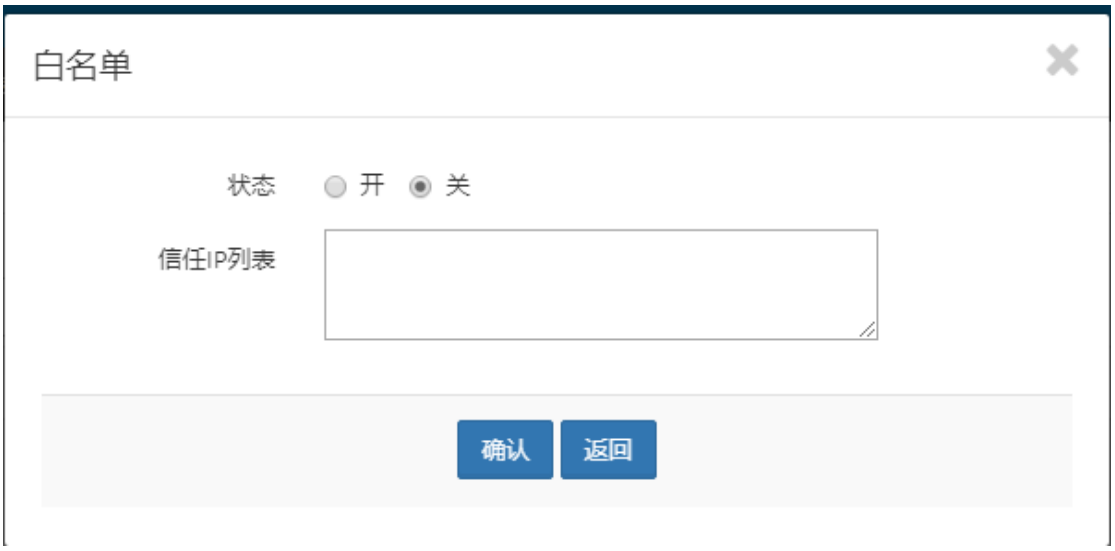


图 47 IP 白名单

3） ip 黑名单

可点击【黑名单】，添加 IP 或 IP 段，黑名单 IP 列表里面的 IP 会被阻断，可自定义阻断时长

图 48 IP 黑名单

5.2.3 特征库

特征库管理

可以先根据特征 ID 查询所有系统特征

图 49 特征查询

再点击【特征管理】对触发的误报特征进行排除

1. 已排除特征管理

点击【特征管理】可以查看已经被排除的特征，也可以根据特征 ID 进行查询

图 50 特征管理

2. 手动添加特征排除

点击【添加】添加特征管理 配置参数见下表

图 51 添加排除特征管理

表 24 排除特征管理参数

参数	说明
特征 ID	特征 ID 号，可以检测是否已经在排除列表
域名	可以是域名或 IP 地址
路径	网站的路径

六. 网络配置

6.1 概述

网络配置模块主要针对设备接入网络拓扑时对设备接口、路由等的配置。主要包含对接口配置、桥配置、VLAN 配置、BONDING 配置、路由配置、策略路由配置等。通过此模块可以顺利的将设备接入到网络拓扑中。

由于阿里云的特性限制，不建议配置网络部分的所有配置。

6.2 接口配置

WAF 采用与微软相近的方式来进行接口的配置，符合配置用户使用习惯。主要包括接口地址配置和接口属性配置。在接口配置界面中，将显示设备上所有的物理接口，当接口在网桥、VLAN 等网络中被选用在接口界面将无法配置。

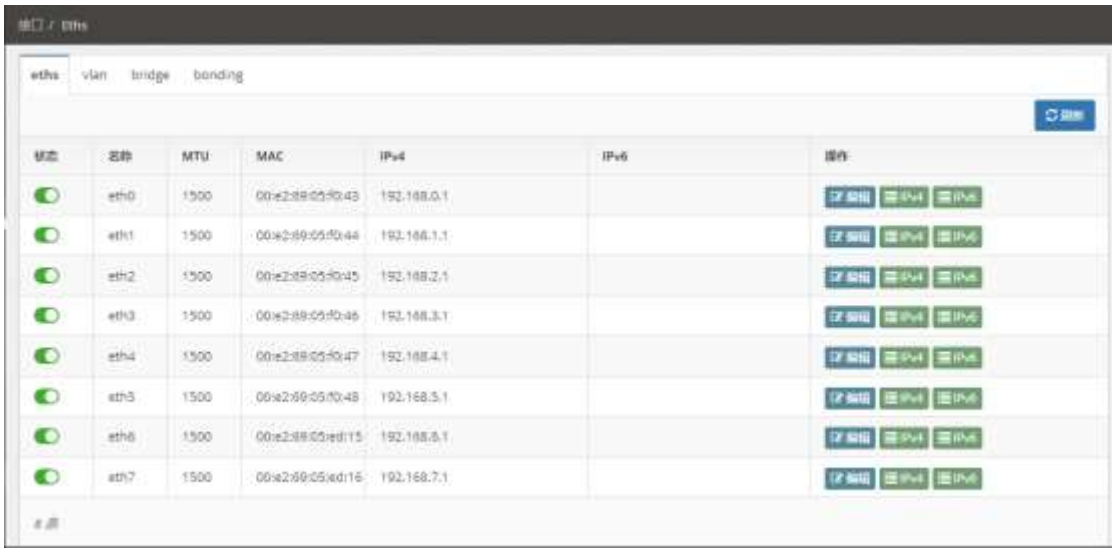


图 52：网络接口

天泰 WEB 应用防火墙支持 IPv4 和 IPv6 两种网络地址，点击 **IPv4** 和 **IPv6** 两个按钮即可对其接口进行配置，点击 **IPv4 配置**（图 52）再点图 53【编辑】添加该接口上的 IP 地址、子网掩码

图 53：IPv4 地址配置

网关地址和 DNS 点击【网关&DNS】按钮可以配置。

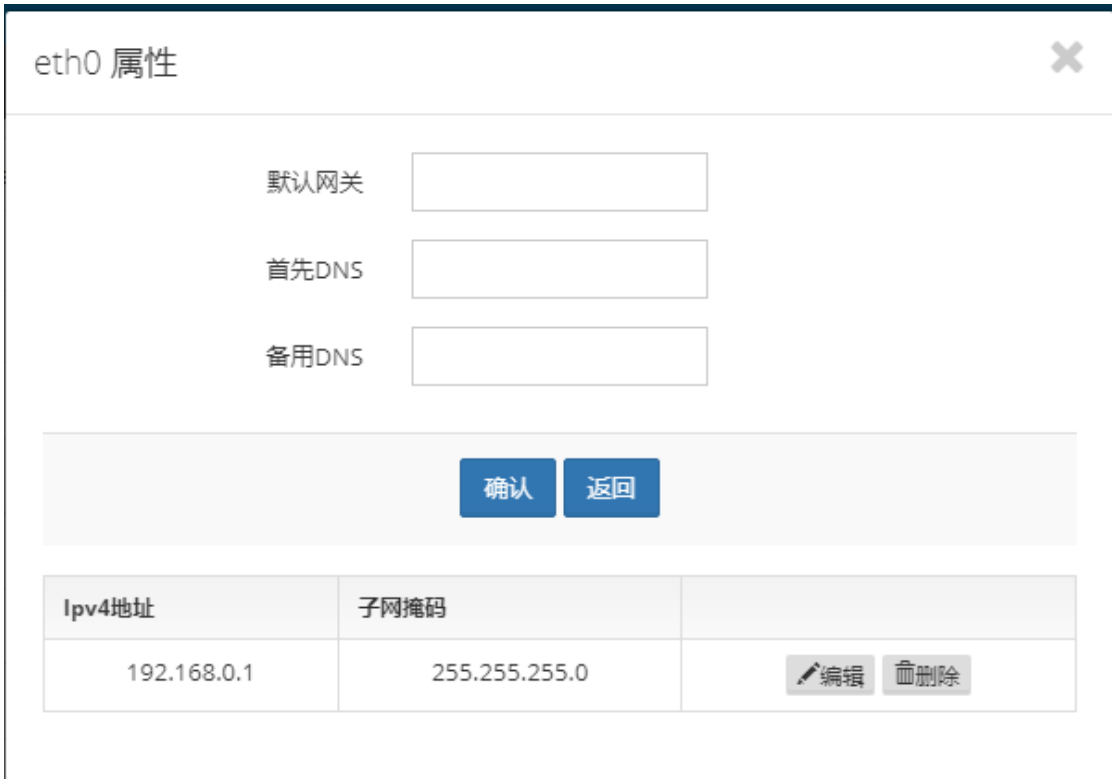


图 54 网关&DNS 配置

天泰 WEB 应用防火墙支持接口从地址，可在一个物理接口设置多个 IP 地址方便你根据实际网络情况进行设置。

配置如图 53 再次点击**添加**，即可在该接口上增加新的 IP 地址，该地址配置完成即刻生效。

图 55：IPv4 从地址

IPV6 地址采用相同的方法添加

图 56：IPv6 地址配置

图 110 所示的【编辑】为接口属性配置，可配置该物理接口上的 MAC 地址、MTU。

图 57：接口物理属性

6.3 VLAN 配置

天泰 WEB 应用防火墙可以在每个物理接口上创建 VLAN，只需填写 VLAN 号即可。进入【接口】-【VLAN】菜单后，点击【添加】创建 VLAN,VLAN 创建好之后，可对配置的 VLAN 配置 IP 地址。

图 58：VLAN 配置

VLAN 的 ID 号最大为 4094

6.4 网桥配置

当天泰 WEB 应用防火墙选择串联到网络中时需要添加网桥，使 WAF 能接入到该 LAN 中进行工作，使用网桥以后设备不会改变原有的网络结构和配置，由于 WAF 自带 bypass 功能，因此当设备发生故障时不会影响到数据的通信。

选择网络接口进行绑定，为了使 BYPASS 生效，建议使用 ETH0 和 ETH1、ETH2 和 ETH3 这中顺序组成的网桥。进入【bridge】点击【添加】如图 116，选择 eth2 和 eth3 为网桥，点击【创建】

图 59：创建网桥

创建完成以后，按照**章节 8.2** 的接口配置添加 IP 地址即可

图 60 网桥配置 IP

6.5 BONDING

Bonding 即为端口汇聚，当设备部署在两台端口汇聚的交换机中间时需要在 WAF 上创建 Bonding，参数如下表：

表 25：端口汇聚参数

参数	说明
BONDING 成员	选择 BONDING 的网络接口
工作模式	选择 bonding 的工作模式：冗余/均衡

图 61：BONDING 配置

6.6 线路

线路可以指定流量走哪条线路到 waf 并到达应用，waf 可以配置虚拟线路

【线路】-【添加】

图 62 线路添加

表 26 线路参数

参数	说明
线路名称	线路名字，可自定义
模式	Waf 在网络的部署模式，包含虚拟网线，透明代理，路由牵引，应用代理
成员	线路使用到的接口
服务器接口	服务器到 waf 之间连接的接口

6.6.1 默认线路

默认线路为应用代理，成员为所有接口都通

6.6.2 虚拟网线

应用场景：主要应用于多网桥的情况下。当需要利用多网桥来部署 WAF 设备，建议使用虚拟网线，主要是由于多网桥下容易出现 MAC 表错乱问题，虚拟网线设置后，不需要查找 MAC 表，数据从一个口进来，直接从虚拟网线设置的另外一个口转发。

图 63 虚拟网线

表 27 虚拟网线模式配置参数

参数	说明
线路名称	线路名字，可自定义
模式	虚拟网线
成员	线路使用到的接口
服务器接口	服务器到 waf 之间连接的接口

出口网关	出口网关 IP 地址

描述其配置选项、使用场景、附上拓扑图，以 WAF 与服务器同网段举例
使用场景：waf 需要在线实时监控所有流量。

图 64 透明代理

表 28 透明代理模式配置参数

参数	说明
线路名称	线路名字，可自定义
模式	透明代理
成员	线路使用到的接口
服务器接口	服务器到 waf 之间连接的接口

图 65 透明代理拓扑

6.6.3 路由牵引

路由牵引通常用在多路的网络环境中，有两种常见的网络环境：

1 TRUNK 环境，服务器存在多个不同的 VLAN 中；

2 多出口环境，服务器分在不同的区域中，每个区域都有独立的出口，相当于是两个独立的网络环境。

图 66 路由牵引配置

表 29 路由牵引模式配置参数

参数	说明
线路名称	线路名字，可自定义
模式	透明代理
成员	线路使用到的接口
服务器接口	服务器到 waf 之间连接的接口

图 67 路由牵引拓扑

6.6.4 应用代理

应用代理模式是将 WEB 应用防火墙（WAF）以代理服务器的方式运行，对网站的请求行为进行代理转发过滤。

应用代理模式通常有路由（网关）和单臂两种部署方式，路由模式是将 WAF 当做路由器或防火墙来部署在网络环境中；单臂模式是将 WAF 旁路接到服务器交换机上，通过修改地址映射（NAT）来引导数据走向，让请求先经过 WAF，再由 WAF 代理转发给服务器。

图 68 应用代理配置

表 30 应用代理模式配置参数

参数	说明
线路名称	线路名字，可自定义
模式	应用代理
成员	线路使用到的接口

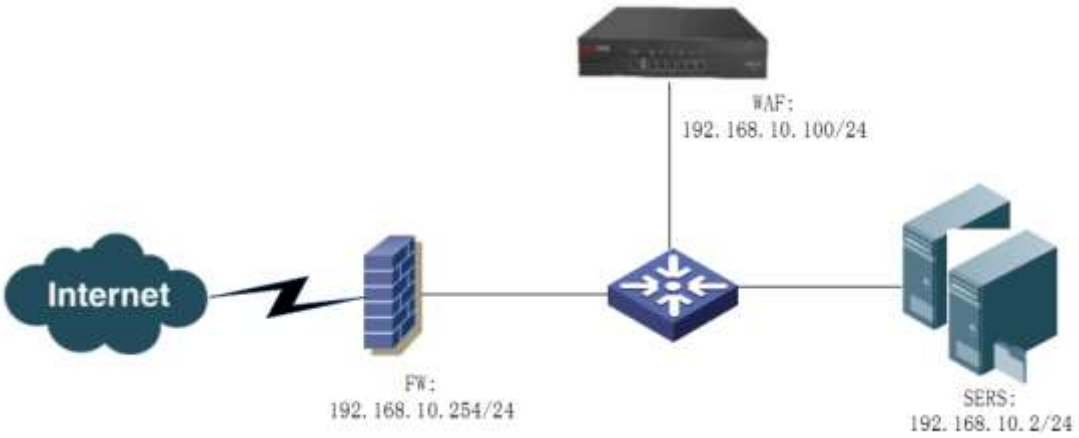


图 69 应用代理单臂拓扑

图 69 出口网关拓扑

6.7 MAC 地址

网络中如果有网络设备开启了 MAC 绑定，例如网络防火墙或者路由器开启 MAC 绑定，将服务器 IP 地址与服务器的 MAC 做了绑定，则 WAF 上开启 MAC 改写以防止防火墙或路由器丢弃 WAF 的数据包造成网络服务不可用。

图 70 mac 地址改写

表 31 mac 地址改写配置参数

参数	说明
服务器地址	后台服务器 IP 地址
MAC 改写为	配置填写选择数据包来源的 MAC 地址，如：XX:XX:XX:XX:XX:XX

6.8 静态路由

WAF 部署位置与服务器不在同一网段，其它 LAN 中的用户无法访问到 WAF 时需要配置一条或多条静态路由，配置参数如下表 50：

表 32：静态路由参数

参数	说明
目标网路	该路由的目标 IP 地址或范围
子网掩码	该 IP 范围的掩码
下一跳	WAF 发送数据包至下一个网络设备的地址
接口	转发该条路由的接口

图 71：添加静态路由

6.9 策略路由

为满足单台 WAF 防护多个链路需求，通过配置**策略路由**功能，可将 WAF 支持在多个物理或虚拟链路上，策略路由分为路由表和路由规则两个部分。

路由表指定了所配置链路的走向；

路由规则指定来源或目的地址；

图 72 策略路由 1

图 73：策略路由 2

参数配置如下表：

表 33：路由表参数

参数	说明
目标网络	路由到达的目标地址
子网掩码	目标网络掩码
类型	VIA：下一条地址，通常为该接口的网关地址 SRC：WAF 接口地址
接口	选择 WAF 接口
接口地址/下一跳	填写 VIA 或者 SRC 的地址
路由表	选择策略路由所在的路由表

表 34：路规则参数

参数	说明
IP 地址	当类型为 FROM 时，地址段为源地址，TO 类型时，为目的地址
子网掩码	目标网络子网掩码
源地址	目标的源地址
类型	路由规则类型
路由表	该条路由规则所在的路由表

七. 系统配置

7.1 概述

系统配置主要为 WAF 对设备进行全方位的接入管理，包括 WEB 管理平台配置，工作模式配置，设备信息配置等，通过此模块，可以方便的改变设备的全局运行状态。

7.2 工作模式

天泰 WEB 应用防火墙支持多种部署模式，包括透明代理、无 IP 透明、应用代理、应用 IDS 模式，用户可根据实际情况选择不同的工作模式。

具体可在【网络】-【线路】-【模式】中选择，详细功能说明参考 6.6 章节

7.3 WEB 管理

点击【系统】-【设置】-【web 管理】WEB 管理配置可以修改 WAF 访问的协议、端口等安全配置，使得对访问设备的用户进行有效的安全管理。

表 35：WEB 管理参数

参数	说明
协议	选择登录 WAF 使用的协议：HTTP/HTTPS
端口	访问设备的端口号，不能使用 80、60000
Token 有效时长	登录 WAF 以后超时重新登录的时间，取值范围：5-60 分钟
锁定前失败次数	锁定账号前允许尝试的次数
锁定时间	锁定帐号时间

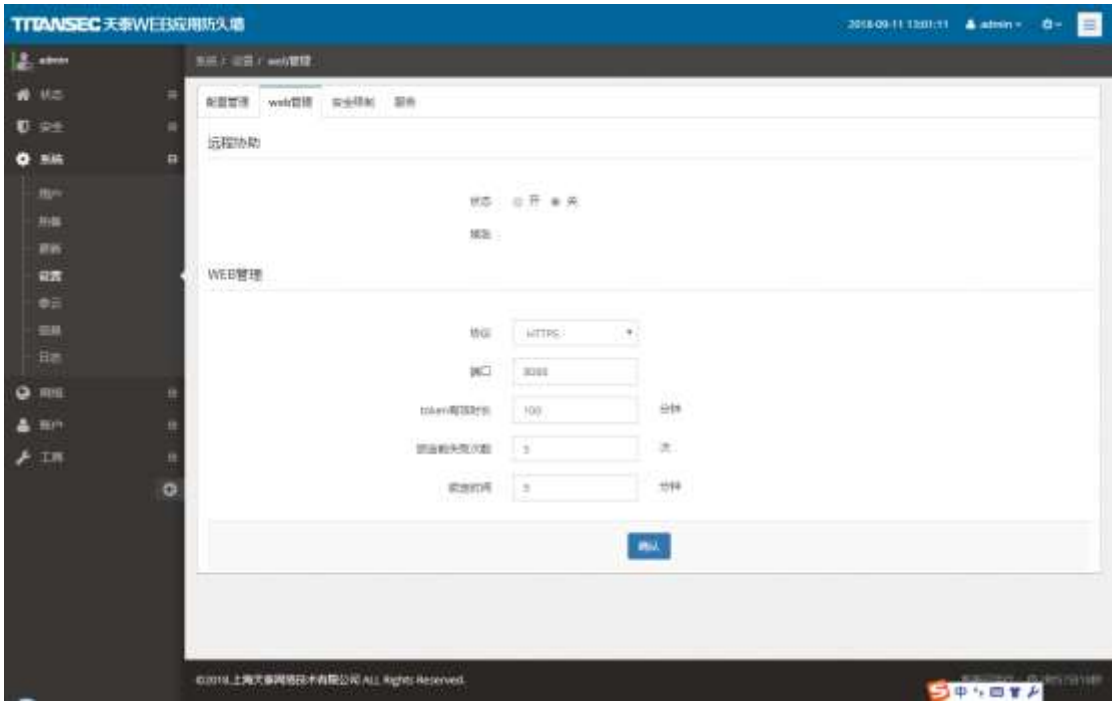


图 74 web 管理

HTTPS 默认端口 443，当 WEB 应用占用 443 端口时，管理平台将无法使用 443 端口。

7.4 远程协助

WAF 支持远程协助功能，当用户无法进行高级配置的时候，远程协助允许技术人员协助用户进行配置，问题诊断。

表 36：远程协助

参数	说明
域名	填写任意数字、字母，将该字段发送给售后技术支持。

注：相关信息即为应用中必须配置有至少一个应用。

图 75 远程协助

7.5 账户配置

WAF 支持三种管理角色，分别是管理员、操作员、审计员，不同的角色拥有不同的管理权限，管理员权限最高，可以进行任何配置，操作员可以对设备进行操作，但是没有创建其他角色的权限，审计员只能对设备进行信息查看，不能修改任何配置。

图 76：创建账户

详细的账户配置信息说明见下图

表 37：账户创建

参数	说明
账户名	支持英文和数字
密码	最少 5 位字符
手机号码	手机号码
角色	选择账户的角色包含 admin 和网站管理员
可信 IP 列表	填写可信的 IP 地址，以换行分割

7.6 配置管理

WAF 支持配置导入及导出，当进行设备硬件升级，环境调试等情况时，只需要导入先前配置，立刻恢复到指定配置。

配置导出可以导出网络、服务、系统特征、系统设置、用户信息的配置

配置导入可以导入已备份的配置，文件格式为.upk

恢复出厂设置可以将设备恢复到出厂默认设置

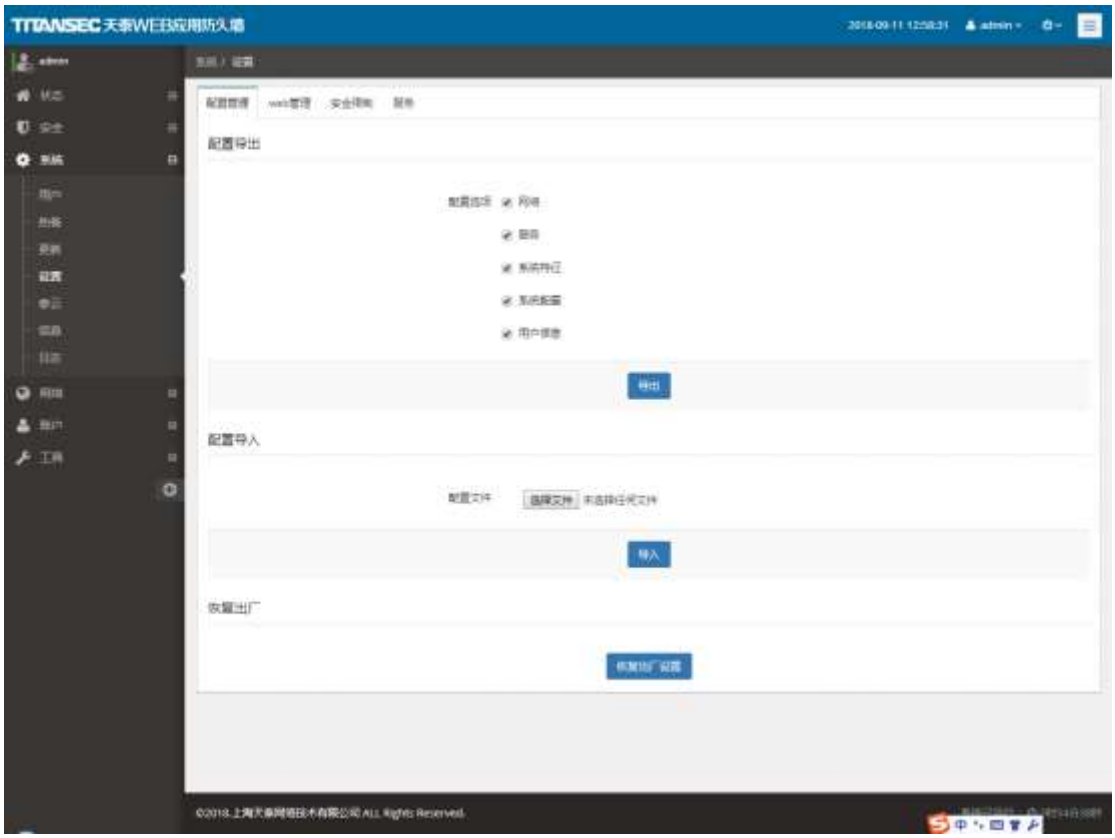


图 77：配置管理

7.7 设备注册

点击【系统】-【信息】可以查看机器的型号序列号和注册信息等

图 78 设备注册

7.8 邮件服务管理

WAF 所提供的各类邮件外发功能均需要配置邮件服务器，为邮件告警提供服务。

表 38：邮件服务参数

参数	说明
状态	日志外发功能开启或关闭
地址	外发的服务器地址
端口	外发的服务端口
日志类型	外发的日志类型可选安全日志、访问日志、操作日志
服务器信息	邮件服务器 SMTP 地址，可以是 IP 地址或域名
端口	邮件服务器服务端口
发送人邮件地址	配置发件人邮件地址（显示在邮件发件人的位置）
用户名	登录邮件服务器地址
密码	登录邮件服务器密码
登录认证	登录该邮件服务器是否需要认证

使用安全连接	配置服务器安全通道，具体请联系邮件提供商。
接收人邮件地址	配置接收人邮件地址（显示在邮件收件人的位置）

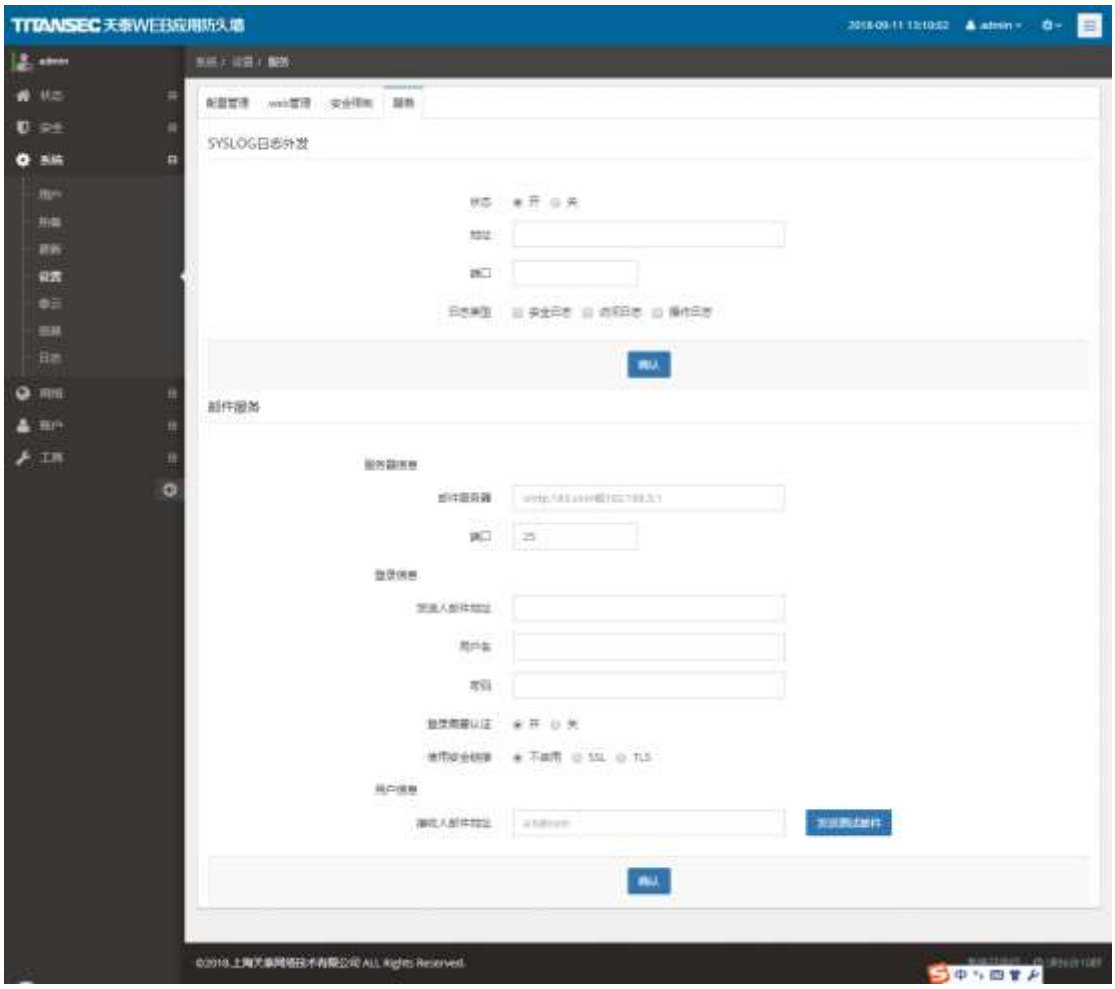


图 79：邮件服务器配置

7.9 系统更新

WAF 支持在线、离线更新两种方式。请及时关注天泰网络网站，获取最新的更新信息，或联系当地技术支持。

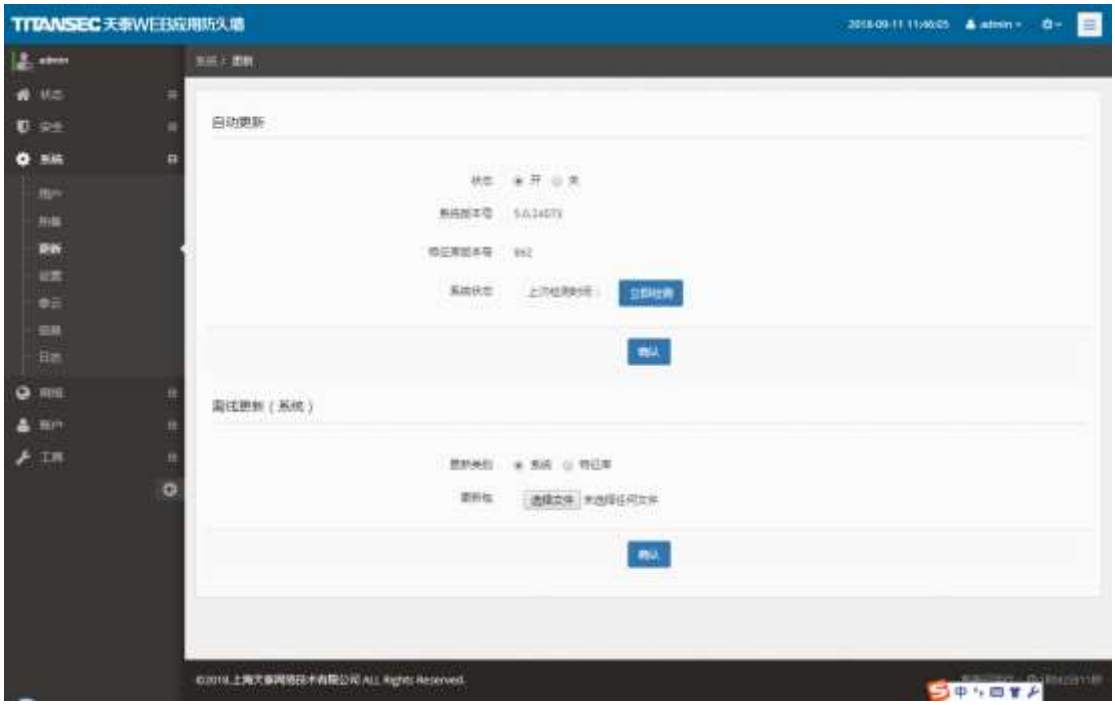


图 80：设备升级

TITAN WAF 更新包格式为 UPK，更新过程中 WEB 管理无法提供服务。

更新时，请先阅读更新说明，并严格按照说明的步骤操作，如有疑问，请联系技术支持。

7.10 系统日志

系统运行日志显示日志的记录时间、用户、登录 IP、操作、状态，也可根据开始时间、结束时间、登录用户和登录 IP 来查询

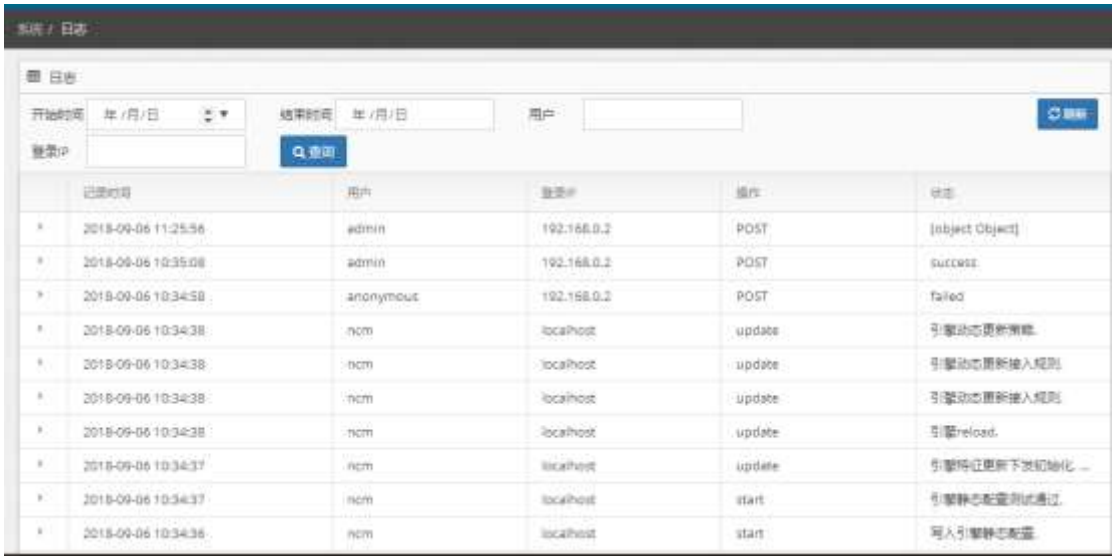


图 81：系统日志

WAF 也提供日志外发功能，需要配置邮件服务器

表 39：邮件服务参数

参数	说明
状态	日志外发功能开启或关闭
地址	外发的服务器地址
端口	外发的服务端口
日志类型	外发的日志类型可选安全日志、访问日志、操作日志

7.11 安全限制

点击【系统】-【设置】-【安全限制】

设置登录 waf 的用户的安全限制密码强度，匹配规则，密码有效期，允许登录该账户的 IP，和能否同用户重复登录

图 82 安全限制

表 40 安全限制配置参数

参数	说明
密码复杂度	可选择不同强度的密码设置规则
正则	匹配正则表达式
描述	对安全信息的描述
密码有效期	有效期内需更换密码
可信任 IP 列表	账号只允许在信任 IP 地址登录

允许同一账号重复登录	账号重复登录开启或关闭

7.12 泰 云

点击【系统】-【泰云】进入泰云管理平台配置，输入 IP 和用户名密码点击连接即能连接泰云管理平台。

图 83 泰云连接

八. 工具

8.1 Ping

Ping 工具用来检测天泰 WEB 应用防火墙与后台服务器，网络网关的连通性

图 84 ping

8.2 Httping

用来监测天泰 WEB 应用防火墙与后台服务器之间应用联通情况

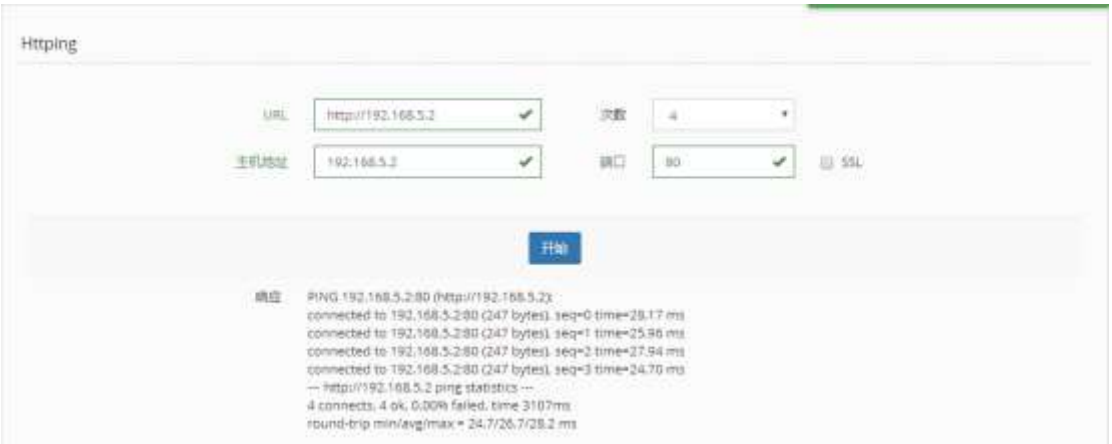


图 85 Httping

8.3 Arping

工具将记录显示设备获取到网络中所有设备的 MAC 地址和 IP 地址以及其所在的网络接口。

图 86 Arping

8.4 NsLookup

用来监测 天泰 WEB 应用防火墙域名解析的情况

图 88 NsLookup

8.5 HttpRequest

用来发起完整 HTTP 请求的工具，一般用来监测后台服务器对特性请求的应情况。 包括服务器的 IP 地址，网站的端口、域名、请求的 HTTP 方法。

图 89 HttpRequest

8.6 TcpDump

TcpDump 可以帮助你将经过 WAF 的数据包的“头”完整截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤，格式支持 Wire shark 软件打开查看。Tcpdump 可以存储最新的 5 条下载记录

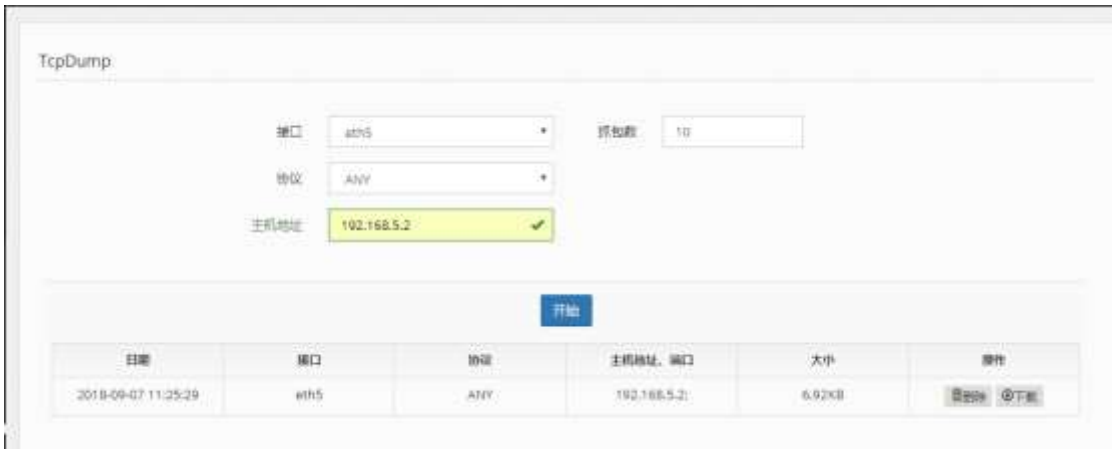


图 87 TcpDump

8.7 TracertRoute

TraceRoute 用来监测天泰 WEB 应用防火墙到目的网络之间路由系统的情况

图 88 TracerRoute

附录A 出厂参数

A 1 WEB 管理员初始账号

用户名	manager operator auditor
密 码	titan2wsx

附录B 漏洞攻击防护内容

配置 WEB 安全防护策略时，可配置的漏洞攻击防护主要如下针对 web 服务器、网站的漏洞进行的非法攻击：

访问 Allaire ColdFusion startstop.html 页面操作

Microsoft FrontPage shtml.exe 恶意访问攻击

Microsoft FrontPage shtml.dll 恶意访问攻击

Real Networks RealServer 远程拒绝服务攻击

Microsoft IIS WebDAV 超长请求远程拒绝服务攻击

利用 NCSA nph-test-cgi 脚本漏洞远程浏览目录

利用 Hylafax faxsurvey 脚本漏洞远程执行命令

Microsoft IIS 4.0 .htr ISAPI 扩展远程缓冲区溢出攻击

Microsoft IIS .ida/.idq ISAPI 扩展远程缓冲区溢出攻击

Windows 系统下 Code Red 网络蠕虫攻击

Windows 系统下 Code Red II 网络蠕虫攻击

Microsoft FrontPage 2000 fp30reg.dll 缓冲区溢出攻击

利用 NCSA test-cgi 脚本获得目录内容列表

Microsoft IIS 4.0/5.0 Unicode 解码漏洞攻击

利用 IRIX pfdispaly.cgi 脚本漏洞远程执行命令或读取文件

Microsoft IIS 4.0/5.0 CGI 文件名错误解码攻击

利用 IRIX webdist.cgi 脚本漏洞远程执行命令

利用 PHP-Nuke index.php 脚本漏洞远程执行命令

Microsoft IIS 5.0 WebDAV 远程缓冲区溢出攻击

Cisco ACS 管理 CGI 程序远程缓冲区溢出攻击

Windows Media 服务 nsiislog.dll 远程缓冲区溢出攻击

Microsoft FrontPage POST 请求远程缓冲区溢出攻击

Windows Media 服务 NSIISlog.DLL 超长 MX_STATS_LogLine 参数远程缓冲区溢出攻击

利用 Web 服务器处理请求文件名漏洞执行命令攻击

Apache Web Server 分块编码传输方式远程溢出攻击

Windows 95/98 UNC 远程溢出攻击

Apache Web Server 分块畸形编码传输

PHP Post 文件上传缓冲区溢出攻击

PHP-Nuke Search 功能 SQL 注入攻击

Apache_W32 Web Server 分块编码传输方式远程溢出攻击

PHPNews sendtofriend.php 远程 SQL 注入攻击

Microsoft Windows GDI+ JPG 解析组件缓冲区溢出攻击

Windows NT IIS MSDAC RDS 远程执行命令攻击

HP OpenView 网络节点管理器远程命令执行攻击

Microsoft IIS w3who ISAPI DLL 远程缓冲区溢出攻击

Netscape Enterprise HTTP 协议 Accept 字段远程缓冲区溢出漏洞

Apache Tomcat JK Web Server Connector 超长 URL 栈溢出攻击

Alt-N WebAdmin USER 参数远程溢出攻击

利用 Microsoft IIS .ida ISAPI 扩展获取绝对路径攻击

Microsoft FrontPage fp30reg.dll 漏洞扫描探测

Microsoft IIS 5.0 .printer ISAPI 扩展映射存在性扫描探测

Index Server .htw 读取文件漏洞扫描探测

利用 Index Server .htw 漏洞远程读取文件

NCSA test-cgi 脚本漏洞扫描探测

Microsoft IIS 4.0 FrontPage 98 扩展察看 CGI 脚本源代码攻击

Microsoft IIS 4.0 showcode.asp 脚本漏洞扫描探测

利用 Microsoft IIS 4.0 showcode.asp 脚本漏洞遍历目录读取文件

Microsoft IIS 5.0 codebrws.asp 脚本漏洞扫描探测

利用 Microsoft IIS 5.0 codebrws.asp 脚本漏洞遍历目录读取文件

通过 Web 服务访问 Windows 2000 的 SAM 文件

利用 Microsoft IIS .idq ISAPI 扩展获取绝对路径攻击

Microsoft IIS 5.0 +.htr 文件泄漏漏洞获取源代码攻击

IRIX webdist.cgi 脚本漏洞扫描探测

Windows NT IIS MSDAC RDS 远程命令执行漏洞扫描探测

Allaire ColdFusion 4.0x cfcache.map 脚本漏洞扫描探测

通过 Web 服务访问.htaccess 文件

通过 Web 服务访问 password.txt 文件获取数据信息

Microsoft IIS 5.0 .printer ISAPI 扩展映射远程缓冲区溢出攻击

利用 Microsoft IIS bdir.htr 脚本漏洞浏览目录

Windows Apache 服务器请求路径处理遍历目录攻击

利用 ht://dig htsearch 脚本漏洞读取系统文件

漏洞扫描器 Nessus 扫描探测 CGI 漏洞

Microsoft IIS 5.0 'Translate: f'头标记获取源码攻击

通过 Web 服务执行 tftp.exe 程序

通过 Web 服务执行 cmd.exe 程序

利用 Microsoft NTFS ::$DATA 漏洞获取 ASP 源码攻击

利用 Microsoft IIS .htr 文件名截断漏洞获取脚本源码攻击

利用../字串突破 CGI 脚本过滤访问上级目录

通过 Web 服务利用'../'串遍历目录攻击

Microsoft IIS 4.0/5.0 .asp ISAPI 扩展远程缓冲区溢出攻击

Frontpage fpremadm.exe 文件扫描探测

Frontpage fpadmin.htm 文件扫描探测

HTTP 服务基本登录认证

通过 Web 服务执行 root.exe 程序

ComVironment grab_globals.lib.php 脚本远程文件包含攻击

Windows 系统下熊猫烧香蠕虫病毒刷计数器操作

Windows 系统下熊猫烧香蠕虫病毒下载恶意代码

协议命令参数超长

Hidden Page Response

Null Host Request

Test page Request

附录C 缩略语

ARP	Address Resolution Protocol	地址解析协议
ACL	Access Control List	访问控制列表
ACK	Acknowledgement	确认字符
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
DOS	Denial of Service	拒绝服务攻击
IDC	Internet Data Center	国际互联网数据中心
CSRF	Cross-site request forgery	跨站请求伪造
CGI	Common Gateway Interface	公共网关接口
CSS/XSS	Cross Site Scripting	跨站脚本攻击
HA	High Availability	高可用性
HTTP	Hypertext Transfer Protocol	超文本传输协议
LAN	Local Area Network	局域网
IP	Internet Protocol	网络之间互连的协议
ICMP	Internet Control Message Protocol	Internet 控制报文协议
IGMP	Internet Group Management Protocol	Internet 组管理协议
MAC	Media Access Control	介质访问控制
MIME	Multipurpose Internet Mail Extensions	功能网络邮件扩充服务
NSLOOKUP	Name Server LookUp	域名查询
SQL	Structured Query Language	结构化查询语言
SYN	Synchronize	同步字符
TCP	Transmission Control Protocol	传输控制协议
TITAN WAF	TITAN Web Application Firewall	天泰 WEB 应用防护系统
WAN	Wide Area Network	广域网
URL	Uniform Resource Locator	统一资源定位符
UDP	User Datagram Protocol	用户数据包协议

附录D 常见 HTTP 响应码

HTTP 2xx	请求成功
HTTP 200	正常；请求已完成。
HTTP 201	正常；紧接 POST 命令。
HTTP 202	正常；已接受用于处理，但处理尚未完成。
HTTP 203	正常；部分信息 — 返回的信息只是一部分。
HTTP 204	正常；无响应 — 已接收请求，但不存在要回送的信息。
HTTP 3xx	重定向
HTTP 301	已移动 — 请求的数据具有新的位置且更改是永久的。
HTTP 302	已找到 — 请求的数据临时具有不同 URI。
HTTP 303	请参阅其它 — 可在另一 URI 下找到对请求的响应，且应使用 GET 方法检索此响应。
HTTP 304	未修改 — 未按预期修改文档。
HTTP 305	使用代理 — 必须通过位置字段中提供的代理来访问请求的资源。
HTTP 306	未使用 — 不再使用；保留此代码以便将来使用。
HTTP 4xx	客户机中出现的错误
HTTP 400	错误请求 — 请求中有语法问题，或不能满足请求。
HTTP 401	未授权 — 未授权客户机访问数据。
HTTP 401.1	未授权：登录失败
HTTP 401.2	未授权：服务器配置问题导致登录失败
HTTP 401.3	ACL 禁止访问资源
HTTP 401.4	未授权：授权被筛选器拒绝
HTTP 401.5	未授权：ISAPI 或 CGI 授权失败
HTTP 402	需要付款 — 表示计费系统已有效。
HTTP 403	禁止访问
HTTP 403.1	禁止访问：禁止可执行访问
HTTP 403.2	禁止访问：禁止读访问
HTTP 403.3	禁止访问：禁止写访问

HTTP 403.4	禁止访问：要求 SSL
HTTP 403.5	禁止访问：要求 SSL 128
HTTP 403.6	禁止访问：IP 地址被拒绝
HTTP 403.7	禁止访问：要求客户证书
HTTP 403.8	禁止访问：禁止站点访问
HTTP 403.9	禁止访问：连接的用户过多
HTTP 403.10	禁止访问：配置无效
HTTP 403.11	禁止访问：密码更改
HTTP 403.12	禁止访问：映射器拒绝访问
HTTP 403.13	禁止访问：客户证书已被吊销
HTTP 403.15	禁止访问：客户访问许可过多
HTTP 403.16	禁止访问：客户证书不可信或者无效
HTTP 403.17	禁止访问：客户证书已经到期或者尚未生效
HTTP 404	无法找到文件
HTTP 404.1	无法找到 Web 站点
HTTP 405	资源被禁止
HTTP 406	无法接受
HTTP 407	要求代理身份验证
HTTP 410	永远不可用
HTTP 412	先决条件失败
HTTP 414	请求 - URI 太长
HTTP 415	介质类型不受支持 — 服务器拒绝服务请求，因为不支持请求实体的格式。
HTTP 5xx	**服务器中出现的错误**
HTTP 500	内部错误 — 因为意外情况，服务器不能完成请求。
HTTP 500.100	内部服务器错误 - ASP 错误
HTTP 500-11	服务器关闭
HTTP 500-12	应用程序重新启动
HTTP 500-13	服务器太忙
HTTP 500-14	应用程序无效

HTTP 500-15	不允许请求 global.asa
HTTP 501	未执行 — 服务器不支持请求的工具。
HTTP 502	错误网关 — 服务器接收到来自上游服务器的无效响应。
HTTP 503	无法获得服务 — 由于临时过载或维护，服务器无法处理请求。

附录E 常见 MIME 值参照表

类型/子类型	扩展名
application/envoy	evy
application/fractals	fif
application/futuresplash	spl
application/hta	hta
application/internet-property-stream	acx
application/mac-binhex40	hqx
application/msword	doc
application/msword	dot
application/octet-stream	*
application/octet-stream	bin
application/octet-stream	class
application/octet-stream	dms
application/octet-stream	exe
application/octet-stream	lha
application/octet-stream	lzh
application/oda	oda
application/olescript	axs
application/pdf	pdf
application/pics-rules	prf
application/pkcs10	p10
application/pkix-crl	crl
application/postscript	ai

application/postscript	eps
application/postscript	ps
application/rtf	rtf
application/set-payment-initiation	setpay
application/set-registration-initiation	setreg
application/vnd.ms-excel	xla
application/vnd.ms-excel	xlc
application/vnd.ms-excel	xlm
application/vnd.ms-excel	xls
application/vnd.ms-excel	xlt
application/vnd.ms-excel	xlw
application/vnd.ms-outlook	msg
application/vnd.ms-pkicertstore	sst
application/vnd.ms-pkiseccat	cat
application/vnd.ms-pkistl	stl
application/vnd.ms-powerpoint	pot
application/vnd.ms-powerpoint	pps
application/vnd.ms-powerpoint	ppt
application/vnd.ms-project	mpp
application/vnd.ms-works	wcm
application/vnd.ms-works	wdb
application/vnd.ms-works	wks
application/vnd.ms-works	wps
application/winhlp	hlp
application/x-bcpio	bcpio
application/x-cdf	cdf

application/x-compress	z
application/x-compressed	tgz
application/x-cpio	cpio
application/x-csh	csh
application/x-director	dcr
application/x-director	dir
application/x-director	dxr
application/x-dvi	dvi
application/x-gtar	gtar
application/x-gzip	gz
application/x-hdf	hdf
application/x-internet-signup	ins
application/x-internet-signup	isp
application/x-iphone	iii
application/x-javascript	js
application/x-latex	latex
application/x-msaccess	mdb
application/x-mscardfile	crd
application/x-msclip	clp
application/x-msdownload	dll
application/x-msmediaview	m13
application/x-msmediaview	m14
application/x-msmediaview	mvb
application/x-msmetafile	wmf
application/x-msmoney	mny
application/x-mspublisher	pub

application/x-msschedule	scd
application/x-msterminal	trm
application/x-mswrite	wri
application/x-netcdf	cdf
application/x-netcdf	nc
application/x-perfmon	pma
application/x-perfmon	pmc
application/x-perfmon	pml
application/x-perfmon	pmr
application/x-perfmon	pmw
application/x-pkcs12	p12
application/x-pkcs12	pfx
application/x-pkcs7-certificates	p7b
application/x-pkcs7-certificates	spc
application/x-pkcs7-certreqresp	p7r
application/x-pkcs7-mime	p7c
application/x-pkcs7-mime	p7m
application/x-pkcs7-signature	p7s
application/x-sh	sh
application/x-shar	shar
application/x-shockwave-flash	swf
application/x-stuffit	sit
application/x-sv4cpio	sv4cpio
application/x-sv4crc	sv4crc
application/x-tar	tar
application/x-tcl	tcl

application/x-tex	tex
application/x-texinfo	texi
application/x-texinfo	texinfo
application/x-troff	roff
application/x-troff	t
application/x-troff	tr
application/x-troff-man	man
application/x-troff-me	me
application/x-troff-ms	ms
application/x-ustar	ustar
application/x-wais-source	src
application/x-x509-ca-cert	cer
application/x-x509-ca-cert	crt
application/x-x509-ca-cert	der
application/ynd.ms-pkipko	pko
application/zip	zip
audio/basic	au
audio/basic	snd
audio/mid	mid
audio/mid	rmi
audio/mpeg	mp3
audio/x-aiff	aif
audio/x-aiff	aifc
audio/x-aiff	aiff
audio/x-mpegurl	m3u
audio/x-pn-realaudio	ra

audio/x-pn-realaudio	ram
audio/x-wav	wav
image/bmp	bmp
image/cis-cod	cod
image/gif	gif
image/ief	ief
image/jpeg	jpe
image/jpeg	jpeg
image/jpeg	jpg
image/pipeg	jfif
image/svg+xml	svg
image/tiff	tif
image/tiff	tiff
image/x-cmu-raster	ras
image/x-cmx	cmx
image/x-icon	ico
image/x-portable-anymap	pnm
image/x-portable-bitmap	pbm
image/x-portable-graymap	pgm
image/x-portable-pixmap	ppm
image/x-rgb	rgb
image/x-xbitmap	xbm
image/x-xpixmap	xpm
image/x-xwindowdump	xwd
message/rfc822	mht
message/rfc822	mhtml

message/rfc822	nws
text/css	css
text/h323	323
text/html	htm
text/html	html
text/html	stm
text/iuls	uls
text/plain	bas
text/plain	c
text/plain	h
text/plain	txt
text/richtext	rtx
text/scriptlet	sct
text/tab-separated-values	tsv
text/webviewhtml	htt
text/x-component	htc
text/x-setext	etx
text/x-vcard	vcf
video/mpeg	mp2
video/mpeg	mpa
video/mpeg	mpe
video/mpeg	mpeg
video/mpeg	mpg
video/mpeg	mpv2
video/quicktime	mov
video/quicktime	qt

video/x-la-asf	lsf
video/x-la-asf	lsx
video/x-ms-asf	asf
video/x-ms-asf	asr
video/x-ms-asf	asx
video/x-msvideo	avi
video/x-sgi-movie	movie
x-world/x-vrml	flr
x-world/x-vrml	vrml
x-world/x-vrml	wrl
x-world/x-vrml	wrz
x-world/x-vrml	xaf
x-world/x-vrml	xof

附录F 自定义规则参数

参数	说明
Args	HttpRequest 中的请求字段(name=valus)
ArgsNames	HttpRequest 中的请求字段名称(name)
RequestHeaders	请求头字段(name=valus)
RequestHeadersName	请求头字段名称(name)
RequestCookies	HttpRequest 中的 Cookie 字段(name=value)
RequestCookiesNames	HttpRequest 中的 cookies 字段名称(name)
QueryString	查询字符串
RemoteAddr	请求地址
RequestBaseName	请求页面名称 eg:index.html
RequestBody	请求体
RequestFilename	请求文件名称
RequestLine	请求行
RequestMethod	请求方法
RequestProtocol	请求协议
RequestUri	请求 URI
RequestUriRaw	请求的原始 URI
FilesNames	上传文件时,文件名称
Files	上传文件时,文件属性
ResponseBody	响应体
ResponseStatus	响应码
XML	针对 webservice,请求文件为 XML 文件
TX	内部存储变量.eg:正则中的捕获