Web 应用防火墙

用户使用指南

天翼云科技有限公司

前言

概述

本文详细介绍了 Web 应用防护系统 V6.0（以下简称 WAF）的 Web 管理界面和串口管理界面的所有功能特点及使用方法。

本手册仅作为使用指导，实际产品可能会由于版本升级或其他原因，与手册描述有略微差异。

读者对象

本文档主要适用于以下读者：

- 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

本文假设读者对下面的知识有一定的了解：

- 网络安全相关知识
- Linux 和 Windows 操作系统
- TCP/IP 协议

内容简介

章节	概述
1 产品概述	介绍 WAF 的产品特点。
2 Web 管理系统概述	介绍 WEB 管理系统的基本信息。
3 系统监控	介绍 WEB 管理系统监控的详细信息。
4 安全管理	介绍 WAF 的站点和策略的详细配置方法。
5 统计报表	介绍系统各类报表的查看方法和查看内容。
6 日志分析	介绍系统各类日志的查看方法和查看内容。
7 系统管理	介绍系统管理和维护的常用操作内容和方法。
A 正则表达式语法	介绍配置策略时使用的正则表达式的语法。

格式约定

符号	说明
粗体字	命令和关键字
斜体字	文档名、变量

符号	说明
	对描述内容的补充和引用信息
	使用设备时的技巧和建议
	需要特别注意的事项和重要信息
	有可能造成人身伤害的警告信息。
【XXX】	菜单名称和按钮名称的表示方式
A > B	菜单项选择的表示方式

修订记录

日期	修订版本	修改记录
2025-01-23	02	1、产品概述取消典型应用说明 2、Web 管理系统概述取消概述说明 3、系统管理-网络配置-工作组管理取消串联部署和旁路部署模式的工作管理说明 4、取消安全交付相关功能 5、取消慢速攻击相关功能
2024-05-10	01	初次发布.

目录

1 产品概述 1

1.1 概述 1

2 Web 管理系统概述 2

2.1 Web 页面布局 2

2.2 系统常用操作 3

3 系统监控 5

3.1 概览 5

3.2 查看安全事件 8

3.2.1 查看实时数据 8

3.2.2 查看历史数据 9

3.3 查看业务负载 10

3.3.1 查看实时数据 10

3.3.2 查看历史数据 10

3.4 查看接口流量 11

3.4.1 查看实时数据 11

3.4.2 查看历史数据 12

3.5 查看系统负载 13

3.5.1 查看实时数据 14

3.5.2 查看历史数据 14

3.6 封禁管理 16

3.6.1 封禁 IP 管理 16

3.6.2 封禁 Session 管理 16

3.6.3 封禁 UA 管理 17

3.7 查看站点访问量统计 18

3.7.1 查看实时数据 18

3.7.2 查看历史数据 18

3.8 查看流量控制 20

3.8.1 查看实时数据 20

3.8.2 查看历史数据 20

3.9 服务器存活状态检测 21

3.9.1 查看实时状态 21

3.9.2 检测配置 23

3.10 设备监控 24

3.11 查看系统信息 25

4 安全管理 27

4.1 安全管理概述 27

4.1.1 防护思路 27

4.1.2 防护体系 27

4.1.3 站点防护流程 28
4.2 网络层防护 28
4.2.1 配置策略启停 29
4.2.2 配置网络层访问控制 29
4.2.3 配置 TCP Flood 防护 32
4.2.4 配置 ARP 欺骗防护 33
4.3 站点防护 35
4.3.1 管理站点组 35
4.3.2 管理站点 42
4.3.3 管理虚拟站点 70
4.4 自学习策略 76
4.4.1 新建自学习策略 77
4.4.2 编辑自学习策略 78
4.4.3 删除自学习策略 79
4.4.4 启用自学习策略 80
4.4.5 停用自学习策略 80
4.4.6 其他操作 80
4.5 自学习结果 81
4.6 规则库管理 81
4.6.1 查询通用防护规则 81
4.6.2 配置自定义特征库 83
4.7 策略管理 85
4.7.1 协议校验 85
4.7.2 基础防护 88
4.7.3 高级防护 105
4.7.4 精准防护 125
4.7.5 其他防护 127
4.8 模板管理 133
4.8.1 站点模板 133
4.8.2 虚拟站点模板 135
4.9 代理信息配置 137
4.10 上传文件管理 139
4.10.1 SSL 证书管理 139
4.10.2 XSD/WSDL 文件管理 141
4.10.3 伪装响应文件管理 144
5 统计报表 145
5.1 安全报表 145
5.1.1 查看告警分类统计报表 145
5.1.2 查看告警时段统计报表 148
5.2 流量报表 150
5.3 区域访问量统计报表 153
5.4 PCI-DSS 合规报表 154

6 日志分析 157
6.1 查看安全防护日志 157
6.1.1 查看 Web 安全日志 157
6.1.2 查看网络层访问控制日志 159
6.1.3 查看 DDoS 防护日志 160
6.1.4 查看 Web 防篡改日志 160
6.1.5 查看 ARP 防护日志 161
6.1.6 查看 Web 访问日志 162
6.1.7 查看会话追踪日志 164
6.2 查看流量控制日志 165
6.3 查看系统运行日志 166
6.4 查看登录日志 167
6.5 查看操作日志 167
6.6 导出日志 168
6.7 日志管理配置 169
6.7.1 日志导出备份 169
6.7.2 Syslog 配置 171
6.7.3 SNMP 配置 172
6.7.4 日志发送参数配置 177
6.7.5 A 接口配置 178
6.7.6 Kafka 配置 178
6.7.7 敏感参数配置 179
7 系统管理 181
7.1 网络配置 181
7.1.1 工作组管理 181
7.1.2 路由配置 182
7.1.3 DNS 配置 184
7.2 系统部署 186
7.2.1 配置运行模式 186
7.2.2 HA 配置 188
7.2.3 VRRP 配置 190
7.2.4 VRRP 配置信息管理 194
7.3 系统工具 196
7.3.1 系统信息 196
7.3.2 规则升级 197
7.3.3 配置同步 202
7.3.4 许可证 204
7.3.5 时间语言 205
7.3.6 系统控制 206
7.3.7 端口设置 206
7.4 测试工具 207
7.4.1 Ping 工具 207
7.4.2 邻居表 208

7.4.3 Traceroute 工具 208
7.4.4 抓包工具 209
7.4.5 系统支持工具 211
7.4.6 扫描工具 212
7.4.7 调试日志追踪 213
7.5 流量控制管理 216
7.6 系统参数配置 218
7.6.1 系统参数 218
7.6.2 内核参数 219
7.6.3 Apache 参数 220
7.6.4 其他参数 220
7.7 SSL 硬件加速 221
7.8 系统运维 221
7.9 REST API 222
A 正则表达式语法 223
A.1 单个字符 223
A.2 转义字符 223
A.3 量词 224
A.4 分组 224
A.5 样例 225

1 产品概述

1.1 概述

无论是个人还是企业，对互联网的依赖在不断增强。在企业应用中，Web 技术正在承载着越来越多的核心业务。但不幸的是，绝大部分安全专家都认为：目前 Web 应用存在极大的安全漏洞，安全措施远远落后于攻击方法。

Web 应用防火墙（简称 WAF）能够保护 Web 应用免遭在线攻击。凭借持续更新的威胁知识库，WAF 系统使安全专业人员、网络管理者和应用开发者有能力降低 Web 应用安全风险，更好地保障 Web 应用稳定运行。

客户价值

- **降低数据泄漏风险**

  Web 承载的交互式应用是数据库的门户，攻击者经常通过 SQL 注入等方法入侵数据库，造成数据泄露。WAF 系统能检查 HTTP 请求的各个字段，用精炼的规则对攻击实施过滤，加上 HTTP 协议合规检查、状态码过滤等机制，降低数据泄露风险。

- **支撑 Web 服务可用性**

  DDoS 攻击对 Web 服务可用性的威胁最大，WAF 系统集成专业 DDoS 防护功能，包括多种动态防护算法，可以在线过滤 DDoS 攻击，与 SQL 注入防护等功能一起使用，提供从网络层到应用层的攻击过滤，支撑 Web 服务可用性。

- **控制恶意访问**

  自动化攻击工具能构造大规模的恶意访问，给 Web 应用稳定性造成很大危害。WAF 系统支持多种 Web 访问控制，可以满足不同用户的需求，包括 HTTP 访问控制、自动化攻击工具识别、控制非法文件上传和下载、阻止盗链和爬虫等。

- **保护 Web 客户端**

  用户访问站点时，如果遭受 CSRF 攻击，用户就会对该站点失去信任。因此，保护 Web 客户端也是 Web 服务提供者的责任和关切。WAF 系统可以提供 CSRF 防护、XSS 防护、Cookie 签名和加密等安全策略，保护 Web 客户端。

产品优势

- **集成专业 DDoS 防护功能**
- **支持多种易于使用的 Web 访问控制策略**
- **支持灵活的自定义规则**
- **支持路由旁路部署方式**
- **支持特定域名的流量控制**

关键功能

- **降低数据泄露风险**
  - SQL 注入防护
  - HTTP 协议防护

- Web 漏洞攻击防护
- 信息泄露（状态码过滤/伪装）
- Web 内容安全防护
- 暴力破解防护
- XML 攻击防护

- **支撑 Web 服务可用性**
  - HTTP Flood 防护
  - TCP Flood 防护
- **控制恶意访问**
  - URL 访问控制
  - 文件非法下载/上传防护
  - 盗链防护
  - 爬虫防护
- **保护 Web 客户端**
  - CSRF 防护
  - XSS 防护
  - Cookie 安全（加密/签名）

2 Web 管理系统概述

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WAF的管理和配置。

本章介绍了 Web 管理系统的基本信息，具体包括以下内容：

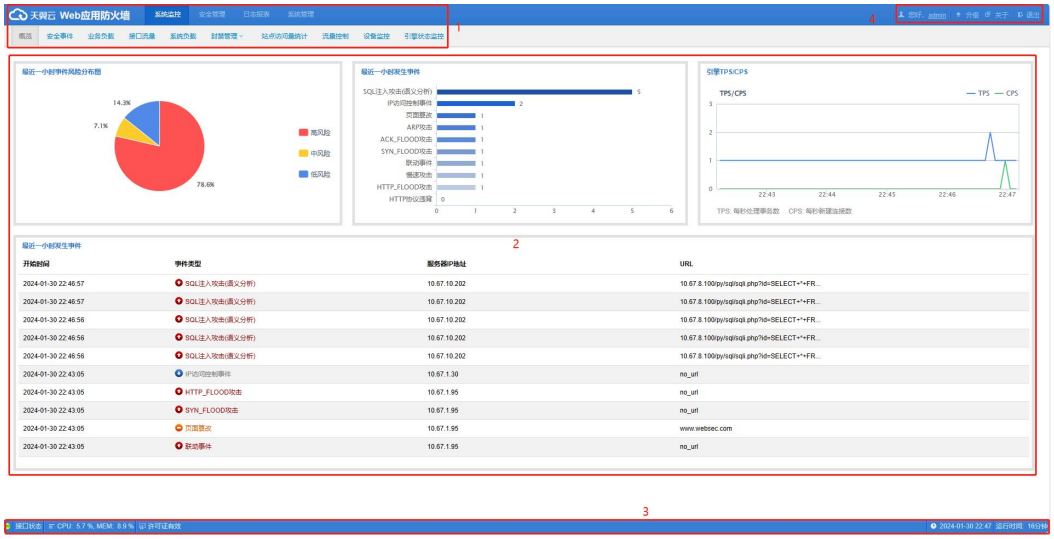
功能	描述
Web 页面布局	介绍 Web 页面布局的情况。
系统常用操作	介绍常用的图标含义。

2.1 Web 页面布局

admin 用户成功登录后，进入系统当前运行的页面，布局如图 2-1 所示。

说明	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，显示的内容有所不同。

图 2-1 Web 管理页面布局



Web 页面布局说明如表 2-1 所示。

表 2-1 页面布局

编号	区域	描述
1	菜单栏	系统的功能主菜单。
2	工作区	系统各类功能的配置、操作、浏览都在这里进行。
3	状态栏	显示系统运行的基本信息，详细信息请参见 3.11 查看系统信息。
4	快捷键区	系统设定的几个快捷按键： • 您好，admin：修改当前用户信息。 • 简体中文：修改 Web 页面语言。 • 升级：升级 WAF 系统。 • 关于：WAF 的产品信息。 • 退出：退出 Web 管理系统。 说明 为确保用户帐号的安全，建议用户单击 退出 退出系统。

2.2 系统常用操作

Web 管理系统常用操作按键的功能，如表 2-2 所示。

表 2-2 常用按键功能

按键	功能
	编辑当前配置项。
	删除当前配置项。
	复制当前配置项。
	启动某个操作
	停止正在运行的操作。
	在列表中上移某个项。
	在列表中下移某个项
保存	保存配置信息。
重置	将页面恢复为修改前的配置参数。

3 系统监控

系统监控模块为用户提供当前系统监控的安全事件、业务负载、通过 WAF 的接口流量、系统负载、封禁 IP 管理、站点访问量统计、流量控制以及系统状态等信息，为用户了解当前网络的安全状况提供有效帮助。

主要包括以下内容：

功能	描述
概览	查看最近一小时内的事件风险分布图、安全事件统计信息及引擎 TPS/CPS 数据。
查看安全事件	查看安全事件的实时数据和历史数据，及事件类型分布图。
查看业务负载	查看业务负载（TPS/CPS、并发连接数、引擎流量）的实时数据和历史数据。
查看接口流量	查看接口流量的实时数据和历史数据。
查看系统负载	查看系统负载（CPU 监控、内存监控、磁盘使用率）的实时数据和历史数据。
封禁 IP 管理	管理被封禁的源 IP 封禁状态。
查看站点访问量统计	查看访问指定站点的流量统计信息。
查看流量控制	查看指定对象的实时和历史流量控制情况。
服务器存活状态检测	查看被检测服务器的存活状态。
设备监控	配置设备 CPU 内存、分区以及进程的监控信息。
查看系统信息	查看系统状态栏的详细信息。

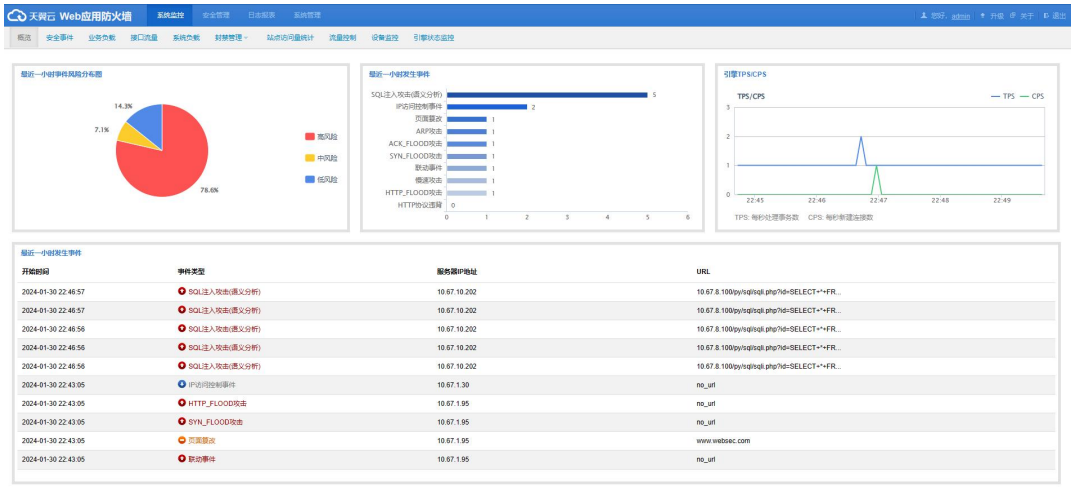
3.1 概览

首次成功登录 WAF 后，默认进入系统监控下的概览页面，或者选择菜单 **系统监控 > 概览**，进入概览页面，如图 3-1 所示。

系统概览页面展示了 WAF 防护的服务器上最近一小时内的攻击事件总数列表、同时会实时更新并展示最近 10 条攻击事件及事件风险分布等详细信息，具体包括：

- 最近一小时事件风险分布图
- 最近一小时发生事件统计图
- 最近五分钟内引擎的 TPS/CPS 流量图
- 最近 10 条实时事件告警列表

图 3-1 概览信息



下面详细介绍查看实时告警事件详情的方法。

实时告警事件的风险级别分为如下几类：

- ：中等风险的事件。
- ：高风险事件。
- ：低风险事件。

告警事件类型及相应风险级别的定义，如表 3-1 所示。

表 3-1 告警类型及风险级别

告警类型	风险等级
HTTP 协议违背	中
Web 服务器漏洞攻击	风险等级取决于触发的规则
Web 插件漏洞攻击	风险等级取决于触发的规则
数据安全传输	低
HTTP 访问控制事件	低
爬虫事件	低
跨站攻击	风险等级取决于触发的规则
SQL 注入攻击	风险等级取决于触发的规则
LDAP 注入攻击	风险等级取决于触发的规则
SSI 指令攻击	风险等级取决于触发的规则
XPATH 注入攻击	风险等级取决于触发的规则
命令注入攻击	风险等级取决于触发的规则
路径穿越攻击	风险等级取决于触发的规则
远程文件包含	风险等级取决于触发的规则
目录索引信息泄露	风险等级取决于触发的规则
WebShell 页面访问	高

告警类型	风险等级
文件非法上传	高
非法下载	中
服务器信息泄露	高
资源盗链	中
跨站请求伪造	高
恶意扫描	高
Cookie 篡改	中
页面内容非法	中
敏感信息过滤	高
暴力破解攻击	高
XML 攻击	高
违背白名单	中
SYN Flood 攻击	高
ACK Flood 攻击	高
HTTP Flood 攻击	高
页面篡改	高
自定义攻击	中
ARP 攻击	高
IP 访问控制事件	低

单击图 3-1 中最近一小时发生事件列表“事件类型”一栏中的实时事件，可查看该事件告警的详细信息，如图 3-2 所示。在实时告警事件中查看的日志详情和通过安全防护日志看到的日志详情一致，有关安全防护日志的介绍情参见 6.1 查看安全防护日志。

图 3-2 告警事件详情

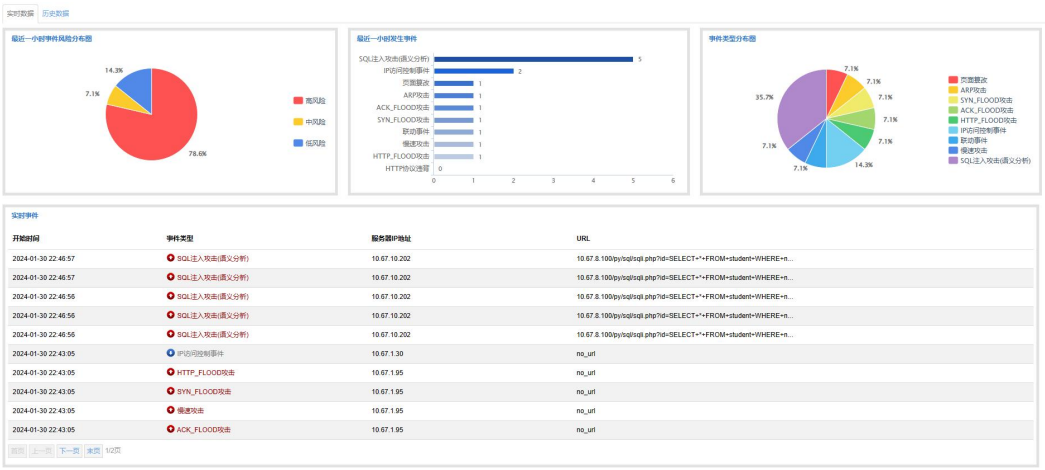
3.2 查看安全事件

用户可以在安全事件页面查看最近一小时内发生的实时安全事件概览，也可在历史数据中查询指定条件下发生的安全事件，安全事件的历史数据的内容滞后于实时数据约 1～2 分钟。

3.2.1 查看实时数据

选择菜单 **系统监控 > 安全事件 > 实时数据**，进入安全事件实时数据展示页面，如图 3-3 所示。安全事件的实时数据与概览信息相似，包括最近一小时事件风险分布图、最近一小时发生事件统计图、事件类型分布图和最近一小时内所有实时事件告警列表。

图 3-3 实时安全事件

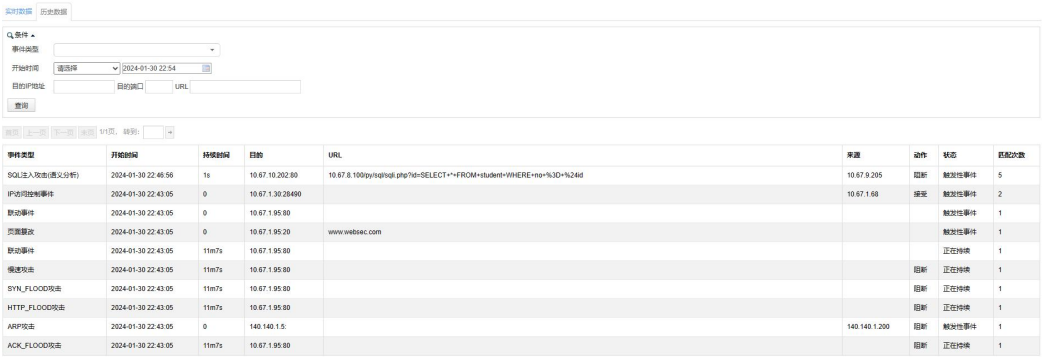


在安全事件中查看实时事件详情的方法与概览页面相同，请参见相应介绍，此处不再赘述。

3.2.2 查看历史数据

选择菜单 **系统监控 > 安全事件 > 历史数据**，进入安全事件历史数据展示页面，如图 3-4 所示。用户可设置多个条件查询系统记录的安全事件，方便快速掌握相关范围内的安全事件情况。

图 3-4 历史安全事件



历史数据安全事件查询条件的详细说明如表 3-2 所示。

表 3-2 安全事件历史数据查询参数说明

配置项	描述
事件类型	查询的安全事件类型，由系统内置。
开始时间	指定安全事件发生的开始时间。
目的 IP 地址	发生安全事件的目的 IP 地址，IP 地址支持 IPv4 和 IPv6。
目的端口	发生安全事件的目的端口号。

配置项	描述
URL	发生安全事件的目的 URL。

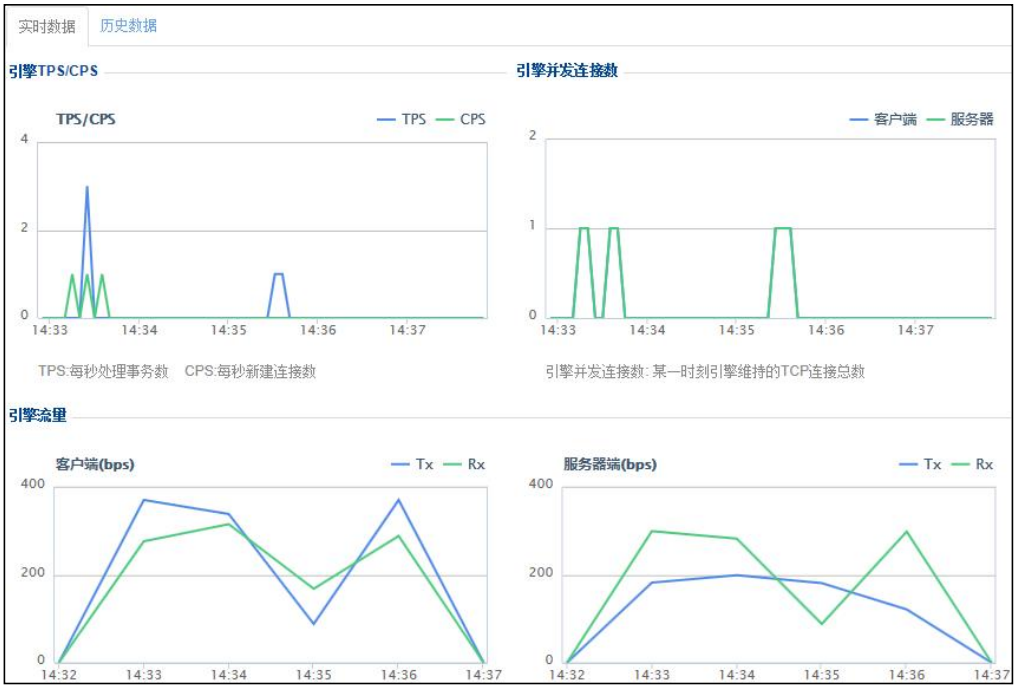
3.3 查看业务负载

业务负载记录了通过引擎代理的端口流量，分为实时数据和历史数据，历史数据的内容滞后于实时数据约 1～2 分钟。

3.3.1 查看实时数据

选择菜单 **系统监控** > **业务负载** > **实时数据**，进入系统业务负载监控页面，如图 3-5 所示。

图 3-5 实时业务负载



实时业务负载展示了五分钟内引擎 TPS/CPS 数据图、引擎并发连接数图和引擎客户端/服务器端的 bps 流量趋势图。其中引擎流量趋势图，展示客户端和服务器端在最近五分钟内的流量信息，包括 Rx（接收）流量信息 Tx（发送）流量信息。

3.3.2 查看历史数据

选择菜单 **系统监控** > **业务负载** > **历史数据**，进入业务负载历史数据展示页面，如图 3-6 所示。

图 3-6 历史业务负载

业务负载历史数据记录过去某段时间 TPS/CPS、引擎并发连接数、客户端和服务器端引擎流量变化趋势，并以趋势图和列表的方式展示。

用户可以通过设定查询类型和时间段来查看引擎历史流量，并以以趋势图和列表的方式展示。历史数据业务负载查询条件的详细说明如表 3-3 所示。

表 3-3 业务负载历史数据查询参数说明

配置项	描述
查询类型	查询的数据流量类型，分为 **TPS/CPS**、**引擎并发连接数**、**引擎流量**三类。
选择时间	单击图示的黄色时间段，可以分别查看最近 **1 小时**、**6 小时**、**12 小时**、**1 天**、**2 天**、**3 天**、**4 天**、**5 天**、**6 天**、**7 天**的访问量情况。
自定义时间	在时间文本框内单击鼠标左键，在进入的日历表中选择日期和时间（起始时间和结束时间必须设置），自定义时间范围查看历史流量。

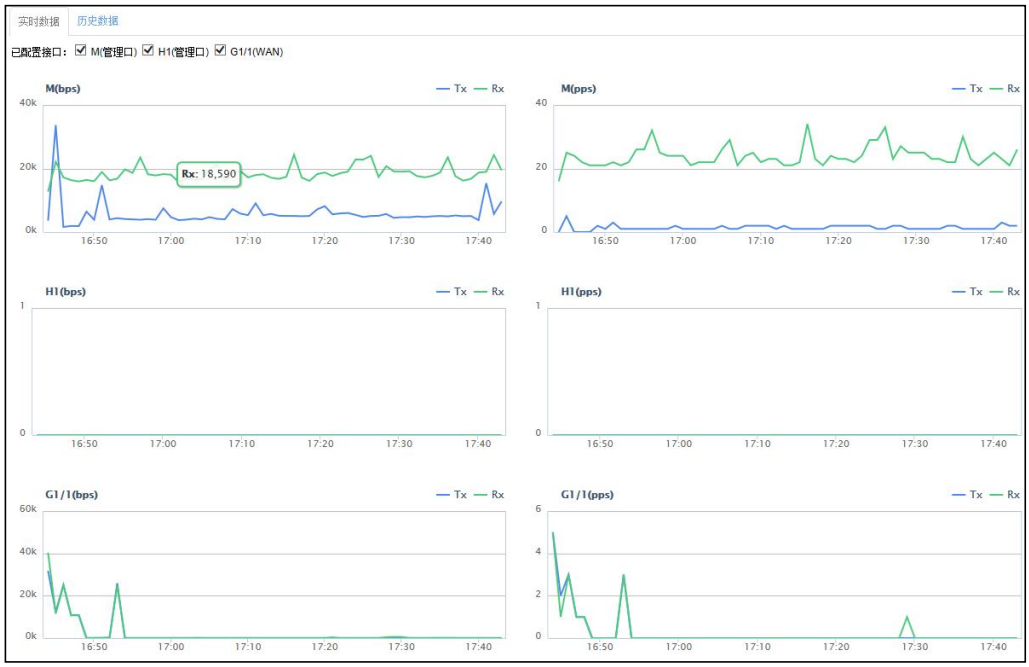
3.4 查看接口流量

接口流量记录了 WAF 所有接口接收和发送的流量信息，分为实时数据和历史数据，历史数据的内容滞后于实时数据约 1～2 分钟。

3.4.1 查看实时数据

选择菜单 **系统监控** > **接口流量** > **实时数据**，进入接口流量实时监控页面，如图 3-7 所示。

图 3-7 实时接口流量



接口实时数据分别按照 bps 和 pps 展示最近一小时内指定接口的 Rx（接收）和 Tx（发送）数据流量趋势图。用户可以勾选实时数据页面左上角的接口，查看不同的接口流量，用户勾选接口后，系统会记录下该接口，再次登录时系统会按照上一次的选择来显示接口流量趋势图。

3.4.2 查看历史数据

选择菜单 **系统监控** > **接口流量** > **历史数据**，进入接口流量历史数据展示页面，如图 3-8 所示。

图 3-8 历史接口流量

网口	Rx(bps/pps)		Tx(bps/pps)	
	平均值	最大值	平均值	最大值
M(管理口)	18K/25	20.3K/28	5.5K/2	8.9K/3
H1(管理口)	0/0	0/0	0/0	0/0
G1/1(WAN)	1.6K/0	11.3K/2	1.6K/0	11.6K/2
G1/2(未分配接口)	0/0	0/0	0/0	0/0
G1/3(未分配接口)	0/0	0/0	0/0	0/0
G1/4(未分配接口)	0/0	0/0	0/0	0/0
G2/1(未分配接口)	0/0	0/0	0/0	0/0
G2/2(未分配接口)	0/0	0/0	0/0	0/0
G2/3(未分配接口)	0/0	0/0	0/0	0/0
G2/4(未分配接口)	0/0	0/0	0/0	0/0

接口流量历史数据记录过去某段时间接口流量的变化趋势，并以趋势图和列表的方式展示。

- 接口流量趋势图

  展示指定接口在指定时间内的 bps 和 pps 流量趋势图。
- 接口流量列表

  展示所有接口在指定时间内的 bps 和 pps 的流量平均值和最大值。

接口流量历史数据查询条件的详细说明如表 3-4 所示。

表 3-4 **接口流量历史数据查询参数说明**

配置项	描述
选择时间	单击图示的黄色时间段，可以分别查看最近 **1 小时**、**6 小时**、**12 小时**、**1 天**、**2 天**、**3 天**、**4 天**、**5 天**、**6 天**、**7 天**的访问量情况。
自定义时间	在时间文本框内单击鼠标左键，在进入的日历表中选择日期和时间（起始时间和结束时间必须设置），自定义时间范围查看历史流量。

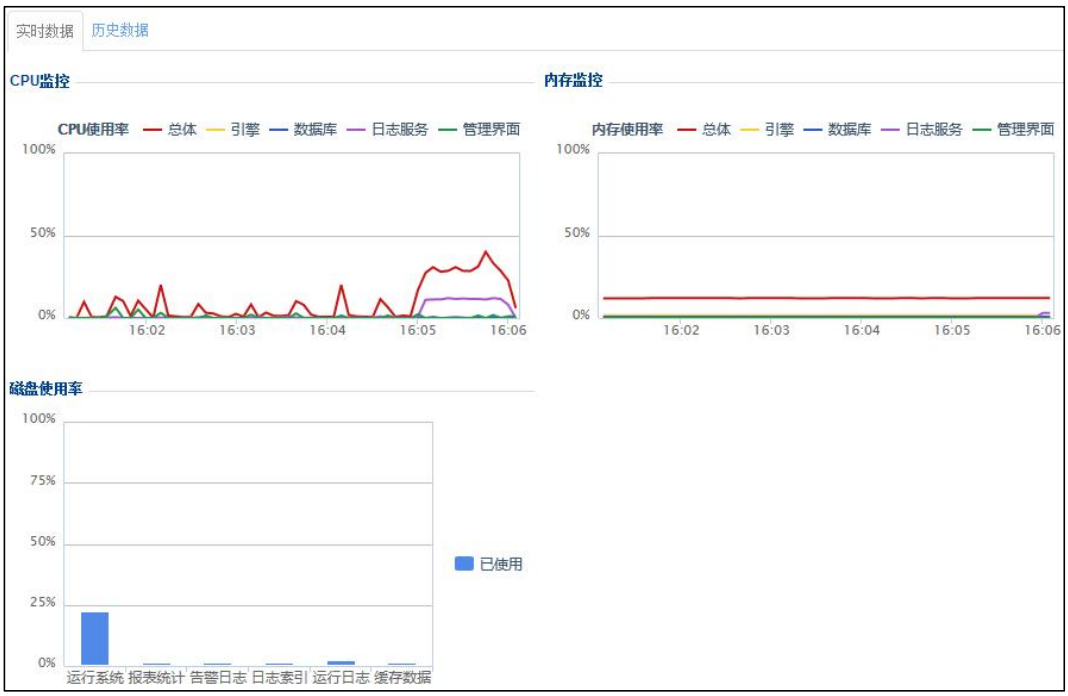
3.5 查看系统负载

系统负载页面展示 WAF 设备的 CPU/内存/磁盘使用率信息，分为实时数据和历史数据，历史数据的内容滞后于实时数据约 1 分钟。

3.5.1 查看实时数据

选择菜单 **系统监控** > **系统负载** > **实时数据**，进入系统负载实时监控页面，如图 3-9 所示。

图 3-9 实时系统负载



系统负载实时数据展示 WAF 设备的磁盘使用率柱状图、最近 5 分钟内 CPU 使用率趋势图、内存使用率趋势图。

3.5.2 查看历史数据

选择菜单 **系统监控** > **系统负载** > **历史数据**，进入系统负载历史数据展示页面，如图 3-10 所示。系统负载历史数据记录过去某段时间设备 CPU 和内存使用情况。

图 3-10 历史系统负载

时间	总体	数据库	管理界面	引擎	日志服务	User	Sys	Hi	Si	Ni	Wa	St
2017-05-19 15:06:04	5	0	0	0	0.8	1	3.7	0	0.2	0	0.2	0
2017-05-19 15:06:09	3.5	0	0	0	0.5	1.2	2.2	0	0	0	0.5	0
2017-05-19 15:06:14	2.8	0	0	0	0	1	1.5	0	0.2	0	0.2	0
2017-05-19 15:06:19	3	0	0	0	0	1	2	0	0	0	0	0
2017-05-19 15:06:24	12.2	0	0	0.2	0	4.5	7.7	0	0	0	0	0
2017-05-19 15:06:29	5.7	0	0	0	0.8	1.2	4.2	0	0.2	0	0	0
2017-05-19 15:06:34	2.8	0	0	0.2	0.2	1	1.8	0	0	0	0	0
2017-05-19 15:06:39	2.7	0	0	0.2	0.2	0.7	2	0	0	0	0	0
2017-05-19 15:06:44	2.7	0	0	0.2	0	1	1.5	0	0.2	0	0	0
2017-05-19 15:06:49	12.2	0	0	0	0	4	8.2	0	0	0	0	0
2017-05-19 15:06:54	3.7	0	0	0.2	0	1.2	2.2	0	0.2	0	0	0
2017-05-19 15:06:59	3.3	0	0	0.2	0	1.2	1.7	0	0.2	0	0.2	0
2017-05-19 15:07:04	2.5	0	0	0	0	1	1.5	0	0	0	0.2	0
2017-05-19 15:07:09	2.8	0	0	0	0	0.7	1.7	0	0.2	0	0.2	0
2017-05-19 15:07:14	12.7	0	0	0	0.2	4.5	8.2	0	0	0	0.2	0

首页 上一页 下一页 末页 1/48页，转到:

系统负载查询条件的详细说明如表 3-5 所示。

表 3-5 系统负载历史数据查询参数说明

配置项	描述
查询类型	查询的系统负载类型，分为 **CPU**、**内存**。
选择时间	单击图示的黄色时间段，可以分别查看最近 **1 小时**、**6 小时**、**12 小时**、**1 天**、**2 天**、**3 天**、**4 天**、**5 天**、**6 天**、**7 天**的访问量情况。
自定义时间	在时间文本框内单击鼠标左键，在进入的日历表中选择日期和时间（起始时间和结束时间必须设置），自定义时间范围查看历史数据。

3.6 封禁管理

封禁管理包括封禁 IP 管理、封禁 Session 管理和封禁 UA 管理。

3.6.1 封禁 IP 管理

封禁 IP 管理页面展示了所有触发策略后被封禁的源 IP 的事件信息，被封禁的源 IP 在封禁时间内的所有 HTTP 请求数据都会被 WAF 阻断。封禁 IP 以站点组为单位进行管理，管理员可以手动取消对源 IP 的封禁。

 说明	只有策略中配置动作参数为阻断且同时配置了封禁源 IP，当该策略被某个站点组引用后被触发时，才能对站点组进行封禁 IP 管理。

进入 **系统监控** > **封禁管理** > **IP 管理** 页面，选择站点组，封禁 IP 管理列表显示该站点组下所有站点被触发的封禁 IP 事件。

- 启用 IP 封禁管理

  单击“是否启用 IP 封禁管理”的是或否按钮，启用或禁用 IP 封禁功能。

 说明	如果未启用 IP 封禁管理，配置策略中的 IP 封禁功能不生效。

- 取消封禁

  在封禁 IP 列表中，选择一个或多个 IP，单击【取消 IP 封禁】按钮，取消相应 IP 的封禁。

- 查询 IP 封禁

  在“源 IP 地址”参数的输入框中输入 IP 地址，单击【查询】按钮，即可快速查询该 IP 对应的封禁信息。

3.6.2 封禁 Session 管理

封禁 Session 管理页面展示了所有触发相关策略后被封禁的 HTTP 会话信息。封禁 Session 以站点组为单位进行管理，管理员可以手动取消对 Session 的封禁。

 说明	只有策略中配置动作参数为阻断且同时配置了封禁 Session，当该策略被某个站点组引用后被触发时，才能对站点组进行封禁 Session 管理。

进入 **系统监控** > **封禁管理** > **Session 管理** 页面。单击页面左侧的站点组名称，右侧的封禁 Session 管理列表中显示该站点组下所有站点被触发的封禁 Session 事件。

- 启用/禁用封禁 Session 管理

  单击“是否启用封禁 Session 管理”字段后的单选按钮，启用或禁用封禁 Session 功能。

说明	如果未启用封禁 Session 管理，配置策略中的 Session 封禁功能不生效。

- 取消封禁

  在封禁 Session 列表中，选择一个或多个 Session，单击【取消 Session 封禁】按钮，取消相应 Session 的封禁。

- 查询封禁的 Session

  在“封禁 Session”参数的输入框中输入 Session 信息，单击【查询】按钮，即可快速查询该 Session 对应的封禁信息。

3.6.3 封禁 UA 管理

封禁 UA 管理页面展示了所有触发策略后被封禁的 UA（user-agent）信息。封禁 UA 以站点组为单位进行管理，管理员可以手动取消对 UA 的封禁。

说明	只有策略中配置动作参数为阻断且同时配置了封禁 UA，当该策略被某个站点组引用后被触发时，才能对站点组进行封禁 UA 管理。

进入 **系统监控** > **封禁管理** > **UA 管理** 页面。单击页面左侧的站点组名称，右侧的封禁 UA 管理列表中显示该站点组下所有站点被触发的封禁 UA 事件。

- 启用/禁用封禁 UA 管理

  单击“是否启用封禁 UA 管理”字段后的单选按钮，启用或禁用封禁 UA 功能。

说明	如果未启用封禁 UA 管理，配置策略中的 UA 封禁功能不生效。

- 取消封禁

  在封禁 UA 列表中，选择一个或多个 UA，单击【取消 UA 封禁】按钮，取消相应 UA 的封禁。

- 查询封禁的 UA

在“封禁 UA”参数的输入框中输入 UA 信息，单击【查询】按钮，即可快速查询该 UA 对应的封禁信息。

3.7 查看站点访问量统计

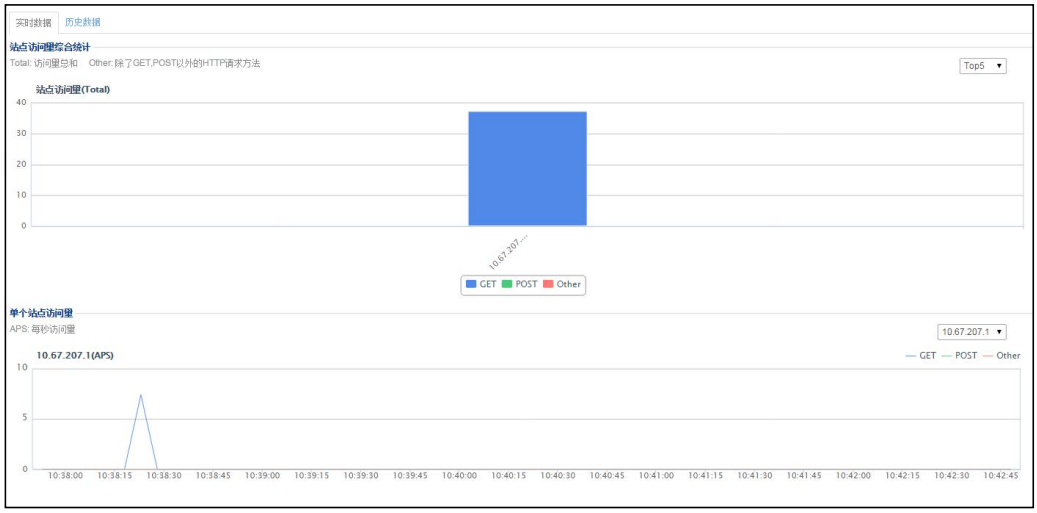
站点访问量统计页面展示指定站点的流量统计信息，分为实时数据和历史数据，历史数据的内容滞后于实时数据约 1 分钟。

WAF 只对开启了站点访问量统计功能的站点进行访问量信息统计，开启站点访问量统计的介绍请参见 4.3.2.1 新建站点。

3.7.1 查看实时数据

选择菜单 **系统监控** > **站点访问量统计** > **实时数据**，进入站点访问量统计实时监控页面，如图 3-11 所示。

图 3-11 实时站点访问量统计



站点访问量统计实时数据默认展示最近 5 分钟内 Top5 的站点总访问量柱状图和最近 5 分钟内单个站点的访问量趋势图。

3.7.2 查看历史数据

选择菜单 **系统监控** > **站点访问量统计** > **历史数据**，进入站点访问量统计历史数据展示页面，如图 3-12 所示。站点访问量统计历史数据记录过去某段时间的总站点访问量柱状图和单个站点的访问量趋势图。

图 3-12 历史站点访问量统计

站点访问量统计业务负载查询条件的详细说明如表 3-6 所示。

表 3-6 站点访问量统计历史数据查询参数说明

配置项	描述
排名类型	查询的站点访问量排名顺序，分为 **Top5**、**Top10**、**Top15**、**Top20**。
查询类型	查询的站点访问量统计类型，分为**详细数据**、**报表**。
选择时间	单击图示的黄色时间段，可以分别查看最近 **1 小时**、**6 小时**、**12 小时**、**1 天**、**2 天**、**3 天**、**4 天**、**5 天**、**6 天**、**7 天**的访问量情况。
自定义时间	在时间文本框内单击鼠标左键，在进入的日历表中选择日期和时间（起始时

配置项	描述
	间和结束时间必须设置），自定义时间范围查看历史数据。

3.8 查看流量控制

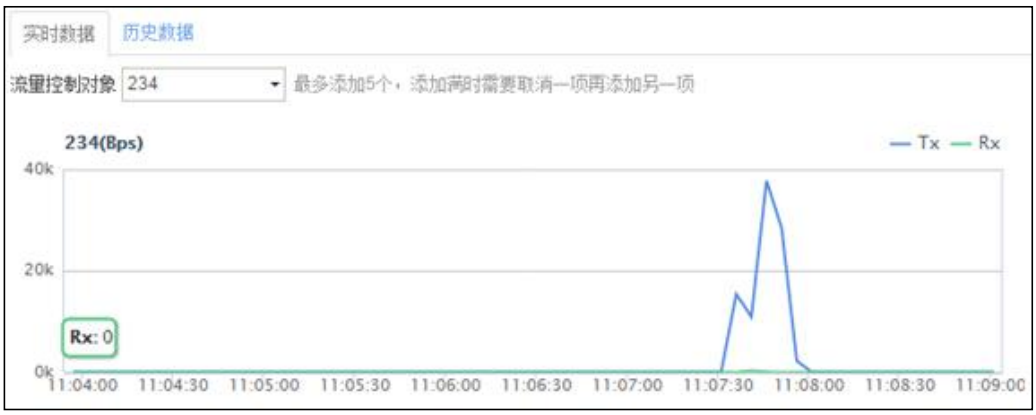
只有反向代理模式下才能使用流量控制功能，流量控制的详细配置请参见 7.5 流量控制。

流量控制页面展示了 WAF 对指定对象进行流量限速后的实时数据和历史数据，历史数据的内容滞后于实时数据约 1～2 分钟。

3.8.1 查看实时数据

选择菜单 **系统监控** > **流量控制** > **实时数据**，进入流量控制实时监控页面，如图 3-13 所示。

图 3-13 实时流量控制



流量监控实时数据展示了最近 5 分钟内 WAF 对一个或多个指定对象的流量进行限速的情况。

最多只能同时查看五个流量控制对象的限速情况，如需查看其他流量控制对象，必须重新选择相应的流量控制对象。

3.8.2 查看历史数据

选择菜单 **系统监控** > **流量控制** > **历史数据**，进入流量控制历史数据展示页面，如图 3-14 所示。

图 3-14 历史流量控制

流量控制历史数据记录过去某段时间内 WAF 对指定对象的流量进行限速的情况。

3.9 服务器存活状态检测

WAF 在串联部署以及旁路部署模式时，可以根据配置对服务器进行存活状态检测。

3.9.1 查看实时状态

需要确认服务器存活状态检测功能已经开启，并对服务器信息进行管理后，才能查看实时服务器存活状态。

选择菜单 **系统监控** > **服务器存活状态检测** > **实时检测**，进入服务器存活状态实时检测页面，如图 3-15 所示。

图 3-15 实时服务器存活状态

服务器列表中显示已经添加的目标服务器的 IP 地址、服务器端口、URL 以及服务器存活状态等信息。其中，服务器存活状态栏中显示图标表示服务器存活；显示图标表示服务器失活；显示图标表示停用探测功能。

服务器存活状态检测启停控制

如图 3-15 所示，当前页面显示服务器存活状态检测已开启。

单击【关闭】按钮，可以关闭服务器存活状态检测功能。

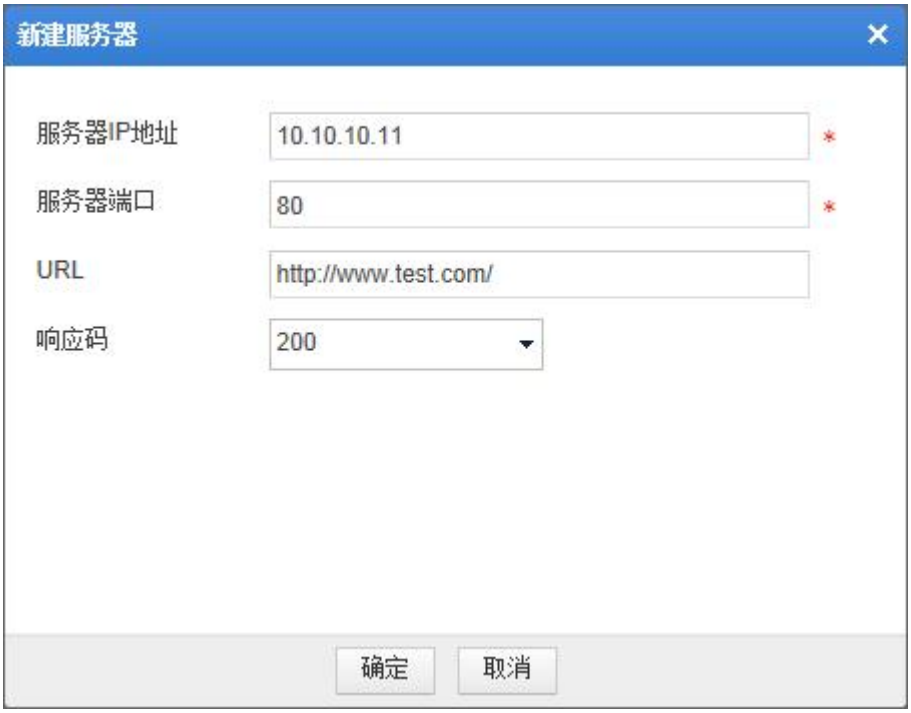
管理服务器

管理员可以对服务器进行新建、编辑、启/停用、重置以及删除的操作。

新建服务器

步骤 1 单击图 3-15 中的【新建】按钮，弹出新建服务器对话框，如图 3-16 所示。

图 3-16 新建服务器



步骤 2 配置服务器参数信息，服务器参数说明如表 3-7 所示。

表 3-7 服务器参数说明

配置项	描述
服务器 IP 地址	目标服务器的 IP 地址。
服务器端口	目标服务器端口。
URL	需要进行服务器存活状态检测的 URL 路径。
响应码	目标服务器返回给 WAF 的响应码。可选项有：**200**、**301**、**302**、**401**。

步骤 3 单击【确定】按钮，保存配置。

----结束

编辑服务器

在服务器列表中，单击服务器对应操作栏中的图标，弹出编辑服务器对话框，用户可以修改服务器的 IP 地址、端口、URL 以及响应码。

启/停用服务器

启/停用服务器有两种方法：

- 单个启/停用

  在服务器列表中，单击服务器对应操作栏中的图标/，启用/停用对该服务器的存活状态检测。

- 批量启/停用

  在服务器列表中，勾选多个服务器，单击【批量操作】按钮，在下拉菜单中选择启用/停用，启用/停用对多个服务器的存活状态检测。

重置服务器

对于已经启用服务器存活状态检测功能，并且处于失活状态的服务器，单击对应操作栏中的图标，可将该服务器的状态重新置为存活状态，此后该服务器的实际工作状态遵从服务器存活状态探测功能的工作流程。

删除服务器

删除服务器有两种方法：

- 单个删除

  在服务器列表中，单击服务器对应操作栏中的图标，删除该条服务器信息。

- 批量删除

  在服务器列表中，勾选多个服务器，单击【批量操作】按钮，在下拉菜单中选择删除，删除多条服务器信息。

3.9.2 检测配置

选择菜单 **系统监控** > **服务器存活状态检测** > **检测配置**，进入服务器存活状态检测参数配置页面，在该页面可以配置服务器存活状态检测参数，如图 3-17 所示。

图 3-17 服务器存活状态检测参数

服务器存活状态检测参数的说明如表 3-8 所示。

表 3-8 **服务器存活状态检测参数**

配置项	描述
轮询探测周期（秒）	对服务器的存活状态进行轮询探测的周期。周期范围：5~62400，单位：秒。
单个周期内失败重连次数	在一个轮询探测周期内，若第一次进行服务器存活状态检测失败时，WAF 重新向服务器发起连接的次数。 重连次数的范围随轮询探测周期变化。
失活检测周期个数	服务器退出失活状态需要经历的检测周期个数。即，N 个周期内 WAF 向服务器发起的所有探测都成功，则服务器退出失活状态。

3.10 设备监控

在设备监控页面，用户可以对 CPU 内存、磁盘分区以及进程的监控进行设置。

选择菜单 **系统监控** > **设备监控**，进入设备监控页面，在该页面可以配置 CPU 内存监控、分区监控以及进程监控，如图 3-18 所示。

图 3-18 **设备监控**

- CPU 内存监控

  首先配置是否启用 CPU 内存监控，开启监控后设定 CPU 和 MEM 内存的阈值。超过阈值时发生告警，告警信息同时记录在系统运行日志中。

- 分区监控

  首先配置是否启用分区监控，分区监控的主要对象是设备运行过程中关键分区（如告警日志分区）在磁盘空间中的占用率。WAF 通过两级告警阈值对关键分区进行监控。

  - 普通阈值

    当关键分区的磁盘占用率首次超过普通阈值时，WAF 记录一条运行日志，日志内容包括关键分区的实际使用率和普通阈值；若持续超过普通阈值会重复记录日志；如果是告警日志分区，WAF 记录运行日志的同时进行日志清空操作，用户可选择是否备份告警日志后清空。

  - 警戒阈值

当关键分区的磁盘占用率首次超过警戒阈值时，WAF 记录一条运行日志，日志内容包括关键分区的实际使用率和警戒阈值；若持续超过警戒阈值会重复记录日志；如果是告警日志分区，WAF 记录运行日志的同时，不备份告警日志直接进行日志清空操作。

分区监控的参数说明如表 3-9 所示。

表 3-9 分区监控参数说明

配置项	描述
普通阈值	当关键分区所占磁盘空间超过该阈值时，WAF 会记录运行日志；如果是告警日志分区，WAF 还会清空告警日志。
是否备份	当告警日志分区所占磁盘空间超过普通阈值进行告警日志清空操作时，是否先备份告警日志再清空。
警戒阈值	当关键分区所占磁盘空间超过该阈值时，WAF 会记录运行日志；如果是告警日志分区，WAF 不提供提前备份告警日志功能，直接清空。

- 进程监控

  进程监控开启后，可实时监测进程的有效性。

3.11 查看系统信息

系统状态栏中展示 WAF 系统运行的详细信息，包括：引擎状态、接口状态信息、设备 CPU 和 MEM 的使用率信息、许可证状态、系统时间和系统运行时间，如图 3-19 所示。

图 3-19 系统状态栏

系统状态栏的详细信息如表 3-10 所示。

表 3-10 系统状态栏信息

显示信息	描述
引擎状态指示图标	显示引擎的状态信息： •  ：引擎处于调试状态； •  ：引擎处于工作异常状态； •  ：引擎处于工作正常状态。
接口状态	将鼠标移到接口状态区域，显示当前设备的接口信息，包括接口属性、工作状态、速率和双工配置等信息；也是查看接口状态信息的快捷键，单击进入工作组管理页面。
CPU:9.5%, MEM:23.8%	显示设备的 CPU、内存使用率；也是查看系统负载的快捷键，单击自动跳转到系统负载实时数据页面。
许可证有效	查看许可证状态的快捷键，单击自动跳转到许可证管理页面。
2017-05-19 16:11	显示系统的当前时间；也是系统时间管理快捷键，单击自动跳转到时间语言管理页面。
运行时间: 2天 20小时 26分钟	显示系统开启后的运行时间。

4 安全管理

本章包括以下内容：

功能	描述
网络层防护	介绍网络层防护的配置方法。
站点防护	介绍站点的详细配置方法。
自学习策略	介绍自学习策略的详细配置方法。
自学习结果	介绍自学习结果的查看和配置方法。
规则库管理	介绍规则库的查看和自定义规则库的配置方法。
策略管理	介绍 WAF 所有类型的策略的详细配置方法。
模板管理	介绍 WAF 策略模板的配置方法。
代理信息配置	介绍代理信息的配置方法。
上传文件管理	介绍 SSL 证书以及 XSD/WSDL 文件的管理方法。

4.1 安全管理概述

本节介绍 WAF 产品的防护思路、防护体系和防护流程三部分内容。

4.1.1 防护思路

WAF 就像网站服务器的防护卫士，对网站的防护分为如下三个阶段：

1. **事前：Web 漏洞扫描**
   - Web 漏洞扫描

     通过 WAF 内置的扫描工具，可以发现网站的漏洞，在网站没有遭受攻击之前将漏洞修补。
2. **事中：策略配置、自学习策略**
   - 策略配置

     通过配置各类策略，WAF 可以对遭受攻击的网站服务器进行实时防护。
   - 自学习策略

     通过对站点配置自学习策略对站点数据和流量特征进行学习，从而配置精准的白名单策略，实现对服务器更精准的防护。

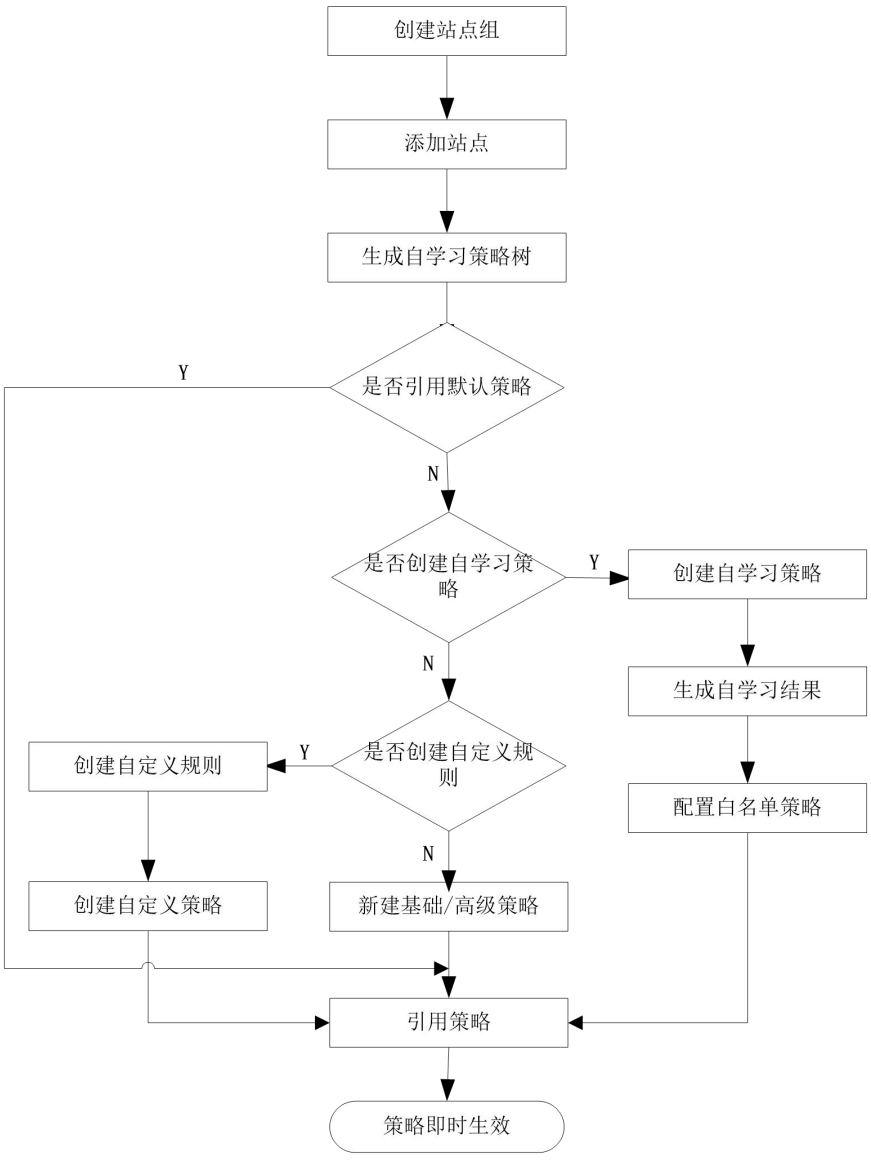
4.1.2 防护体系

一旦网页的内容被攻击者恶意攻击甚至篡改，就有可能造成恶劣的社会影响，给网站的拥有者造成不可计数的损失。WAF 部署在网络的客户端和服务器之间，通过多层级的防护有效阻断或降低服务器遭受的攻击。

4.1.3 站点防护流程

通常情况下，被防护的服务器在 WAF 界面以站点的形式进行管理，配置站点及防护策略的过程如图 4-1 所示。

图 4-1 站点防护配置过程



4.2 网络层防护

网络层的防护是 WAF 的第一道防护线，是基于网络层的全局防护，包括如下几类防护：

- 网络层访问控制（反向代理模式不支持）
- TCP Flood 防护（当前场景不支持）
- ARP 欺骗防护（当前场景不支持）

4.2.1 配置策略启停

策略启停主要控制网络层访问控制、TCP Flood 防护、ARP 欺骗防护以及防透传的启用和停用，要使配置的策略生效，必须在策略启停中开启对应的功能。

选择菜单 **安全管理 > 网络层防护 > 策略启停**，进入策略启停状态配置页面，用户可通过策略列表查看并设置策略的启用状态，如图 4-2 所示。

图 4-2 策略启停

其中网络层访问控制策略和 TCP Flood 策略默认开启（状态为图标），ARP 欺骗策略、防透传以及重用客户端 tcp 序列号配置默认关闭（状态为 图标）。

- 启用策略

  在图 4-2 所示策略列表中，单击某条策略相应“操作”栏中的图标，策略状态显示为，表示该策略功能启用。

- 停止策略

  在图 4-2 所示策略列表中，单击某条策略相应“操作”栏中的图标，策略状态显示为 ，表示该策略功能停止。

4.2.2 配置网络层访问控制

网络层访问控制主要是对网络层和传输层的控制，是防火墙具有的功能，而 WAF 将此功能集成，方便用户直接使用 WAF 配置网络层的访问控制。

网络层访问控制策略仅当 WAF 设备处于串联部署模式和旁路部署模式时适用，不适用于反向代理模式。

注意	**网络层访问控制策略是 WAF 的第一防护门槛，数据包首先进行该策略的匹配，然后才去匹配其他策略。**

新建网络层访问控制策略

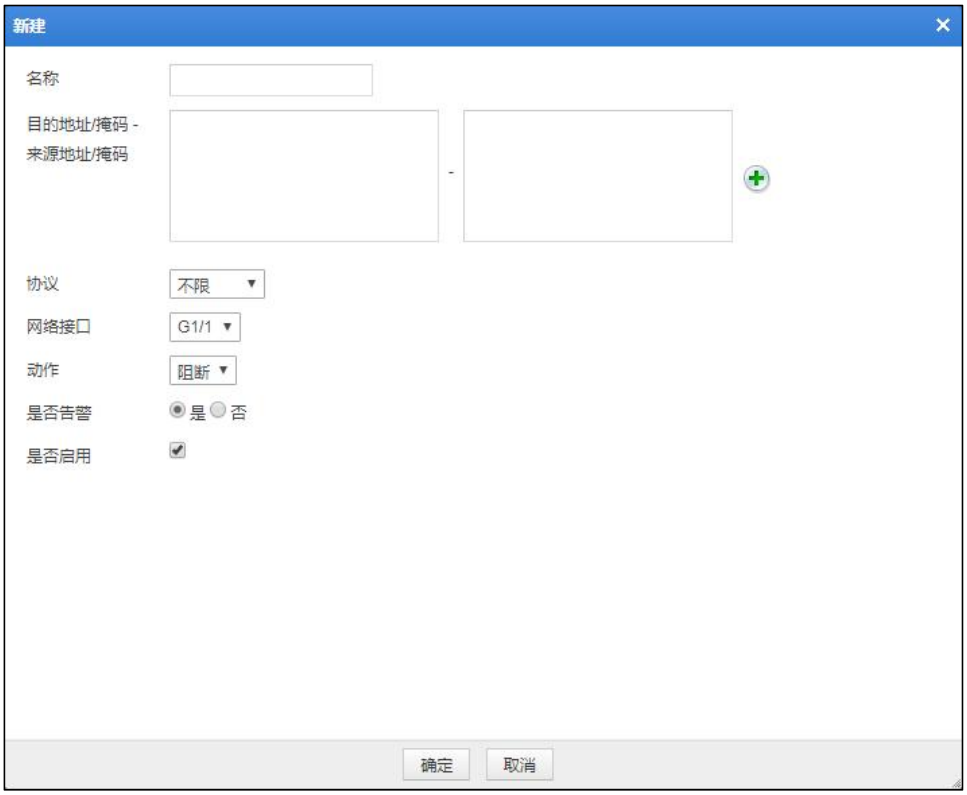
新建网络层访问控制策略的具体操作如下：

步骤 1 选择菜单 **安全管理 > 网络层防护 > 网络层访问控制**，进入网络层访问控制策略列表，如图 4-3 所示。

图 4-3 网络层访问控制

步骤 2 单击【新建】按钮，弹出新建网络层访问控制策略对话框，如图 4-4 所示。

图 4-4 新建网络层访问控制策略



步骤 3 配置网络层访问控制策略参数，参数的详细信息如表 4-1 所示。

表 4-1 网络层访问控制策略参数信息

配置项	描述
名称	网络层访问控制策略的名称。
目的地址/掩码-来源地址/掩码	通过 WAF 数据包的“目标 IP 地址和掩码-源 IP 地址和掩码”对，支持 IPv4 和 IPv6。 支持多个“目标 IP 地址和掩码-源 IP 地址和掩码”对，单击图标，增加“目标 IP 地址和掩码-源 IP 地址和掩码”对，最多可增加到 50 对。

配置项	描述
	说明 • 每个目的地址/掩码-来源地址/掩码框中最多只能配置 10 条，多条地址/掩码之间用回车换行进行分隔。 • 支持“来源地址/掩码-目的地址/掩码”一对多，即：目的地址/掩码框中配置一条，则来源地址/掩码中框中可配置多条；反之，来源地址/掩码框中配置一条，则目的地址/掩码中框中可配置多条。 • 若一条策略中配置的“目的地址/掩码-来源地址/掩码”对有重复按照策略顺序进行匹配。
协议	支持四种类型的协议防护：ICMP、ICMPV6、TCP、UDP，选择不限，表示不对协议进行限制。 若协议选择 TCP 或 UDP，还需配置目标流量的来源端口和目的端口范围。
网络接口	WAF 的工作口，控制的数据包是从 WAF 的哪个接口接收到的。
动作	有三种类型的动作： • 阻断：将数据丢弃,同时断开 TCP 连接； • 接受：数据匹配策略后，继续匹配其他的策略； • 转发：数据匹配策略后，不进行其他策略的匹配，直接将数据包转发出去。
是否告警	是否产生告警日志。
是否启用	是否启用该条策略。

注意	因为配置网络层的访问控制策略是针对全局的，所以配置时需注意： • 如果要配置网络层的阻断策略，必须配置一条动作为阻断且网络接口为 WAN 口的网络层访问控制策略。 • 如果要配置网络层的转发策略，必须配置一条动作为转发且网络接口为 WAN 口的网络层访问控制策略。 • 如果要配置网络层的接受策略，必须分别配置两条网络层访问控制策略。其中一条动作为接受且网络接口为 WAN 口，另一条动作为接受且网络接口为 LAN 口。

步骤 4 单击【确定】按钮，保存配置。

----结束

编辑网络层访问控制策略

网络层访问控制策略配置完成后，管理员可以重新编辑其参数，具体操作如下所示：

步骤 1 在图 4-3 所示网络层访问控制策略列表中，单击某个网络层访问控制策略“操作”栏中的图标，可以重新编辑该网络层访问控制策略的参数。

步骤 2 编辑完成后，单击【确定】按钮，保存配置并返回到网络层访问控制策略列表界面。

----结束

删除网络层访问控制策略

WAF 支持删除单条网络层访问控制策略。

在图 4-3 所示网络层访问控制策略列表中，单击某条网络层访问控制策略“操作”栏中的图标，进入删除确认窗口，然后单击该窗口中的【确定】按钮，即可删除该网络层访问控制策略。

启动/停止网络层访问控制策略

- 在图 4-3 所示网络层访问控制策略列表中，单击某条网络层访问控制策略相应“操作”栏中的图标，策略状态显示为，表示该策略开启。
- 在图 4-3 所示网络层访问控制策略列表中，单击某条网络层访问控制策略相应“操作”栏中的图标，策略状态显示为，表示该策略停止。

4.2.3 配置 TCP Flood 防护

TCP/IP 的实现只能允许一定数量的 TCP 连接，TCP Flood 正是利用这一点进行攻击，主要有如下两类：

- SYN Flood 攻击

  攻击机发送大量的 syn 包给服务器，导致服务器忙于应付，影响正常的访问。
- ACK Flood 攻击

  攻击机发送大量的 ack 包给服务器，影响服务器对正常请求的响应。

TCP Flood防护策略通过配置防护阈值实现对SYN Flood攻击和ACK Flood攻击的防护。WAF 对每秒客户端给服务器发送的数据包进行统计，如果发包数目超过阈值则认为是攻击，WAF 随即进入防护状态，根据内置的防护算法对该攻击进行防护。

配置 TCP Flood 防护策略的具体操作如下：

步骤 1 选择菜单 **安全管理** > **网络层防护** > **TCP Flood 防护**，进入 TCP Flood 防护编辑页面，如图 4-5 所示。

图 4-5 TCP Flood 防护策略

步骤 2 编辑 TCP Flood 防护策略参数，参数详细信息如表 4-2 所示。

表 4-2 **编辑 TCP Flood 防护策略参数信息**

配置项	描述
SYN Flood 防护阈值	每秒接收到的 syn 包超过该值，则认为是攻击，默认值为 6000。
ACK Flood 防护阈值	每秒接收到的 ack 包超过该值，则认为是攻击，默认值为 20000。
是否丢弃 syn64	如果选择“是”，当检测到 options 字段为空的数据包时，WAF 就直接丢弃。

步骤 3 单击【确定】按钮，保存配置。

步骤 4 在策略启停页签中启用 TCP Flood 防护策略。

----结束

4.2.4 配置 ARP 欺骗防护

常见的 ARP(Address Resolution Protocol)攻击有如下两种：

- 仿冒网关：ARP 病毒通过发送错误的网关 MAC 对应关系给受害者，这可能导致以下问题：
  - 从拒绝服务攻击层面看，可能导致受害者与真实网关的通讯受到破坏，受害者响应的数据无法投递到真实网关，造成事实上的拒绝服务。
  - 从数据安全层面看，可能导致受害者响应的数据被投递到攻击者指定的 MAC 上。一旦攻击者获取这些数据，甚至篡改数据后再转发给真实网关，就会造成数据窃取、篡改的安全事件。
- 仿冒终端用户/服务器
  - 欺骗网关：发送错误的终端用户的 IP-MAC 对应关系给网关，导致网关无法和真实终端用户正常通信，并可能造成因投递错误而带来的数据窃取、篡改等安全事件。
  - 欺骗终端用户：发送错误的终端用户/服务器的 IP-MAC 对应关系给其他终端用户，导致两个终端用户之间无法正常通信。

开启 ARP 防护功能后，WAF 会首先学习 IP-MAC 对应关系。在 LAN 口，首次收到来源 IP 是“代理服务”中指定服务器 IP 的 ARP 报文（ARP 查询或 ARP 响应包）时，WAF 会记录此 IP-MAC 对应关系，作为被保护服务器的 IP-MAC 对应关系的基准。

自学习 MAC 表建立后，WAF 将以表中的 IP-MAC 对应关系为基准进行 ARP 防护。LAN 口收到的数据报文，若源 IP 和端口是“代理服务”中指定的服务器 IP 和端口，则要求其源 MAC 必须与自学习 MAC 表中记录的 MAC 一致；

在 ARP 欺骗防护页面，可以进行查看自学习 MAC 表和对 MAC 绑定配置列表的内容进行新建、编辑、删除、启动和停止的操作。下面介绍如何查看自学习 MAC 表和新建 MAC 绑定。有关如何编辑、删除、启动和停止 MAC 绑定的方法与对网络层访问控制策略的操作相同，详情请参考网络层访问控制策略的相关介绍，此处不再赘述。

4.2.4.1 查看自学习 MAC 表

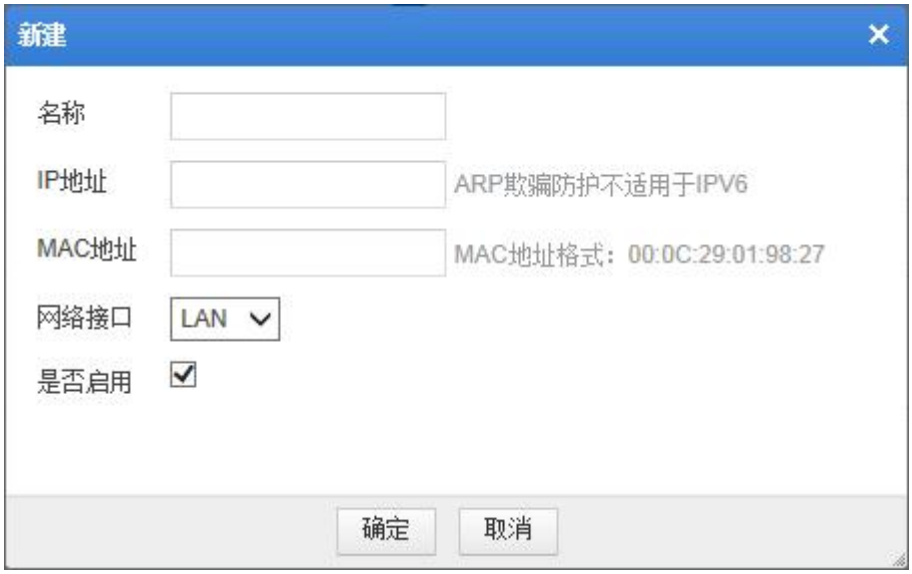
选择菜单 **安全管理 > 网络层防护 > ARP 欺骗防护**，进入 ARP 欺骗防护配置页面，如图 4-6 所示。“自学习 MAC 表”位于页面下方，显示系统自动学习到的当前 IP 和 MAC 绑定情况。

图 4-6 ARP 欺骗防护

4.2.4.2 新建 MAC 绑定

在图 4-6 所示的 MAC 绑定配置列表中，单击【新建】按钮，弹出新建 MAC 绑定对话框，如图 4-7 所示。

图 4-7 新建 MAC 绑定



配置 MAC 绑定的详细信息如表 4-3 所示。

表 4-3 添加 MAC 绑定参数信息

配置项	描述
名称	MAC 绑定策略的名称。
IP 地址	需要绑定 MAC 的对应 IP，只能绑定被代理服务器和网关的 IP，IP 地址仅支持 IPv4。
MAC 地址	需要绑定的 MAC 地址，只能绑定被代理服务和网关的 MAC。

配置项	描述
网络接口	有两种：WAN 口和 LAN 口 • 选择 WAN 口表示在 WAN 口检测数据包中 MAC 和 IP 的对应； • 选择 LAN 口表示在 LAN 检测数据包中 MAC 和 IP 的对应。 绑定网关的 MAC 一般选择 WAN 口，绑定代理服务的 MAC 一般选择 LAN 口。
是否启用	是否启用该条策略。

说明	• MAC 表建立后不能自动更新，只能通过手动绑定 IP 和 MAC 地址来更新 MAC 表项。 • 系统重启后，会自动重新自学习 MAC 表。 • WAF 只会对代理服务配置时指定的 IP 地址(即被保护服务器的 IP)进行 ARP 防护。

4.3 站点防护

站点是 WAF 进行防护的对象，是由单个或多个 IP 地址组成的集合。通常，多个同类型的站点、虚拟站点一起组合成为一个站点组。WAF 针对站点组配置各种策略进行防护。

选择菜单 **安全管理** > **站点防护**，进入站点防护管理页面，如图 4-8 所示。

图 4-8 **站点防护**

在左侧的站点组树图中：

- “root”为默认的站点组根目录；
- “test”为管理员新建的站点组；
- “vmsite”为站点组“test”中的虚拟站点。

下面将详细介绍如何对站点组、站点以及虚拟站点进行管理。

4.3.1 管理站点组

管理员可以对站点组进行如下操作：

- 新建站点组
- 编辑站点组
- 管理区域访问量全局统计
- 调整站点组优先级
- 策略一键控制

- 删除站点组

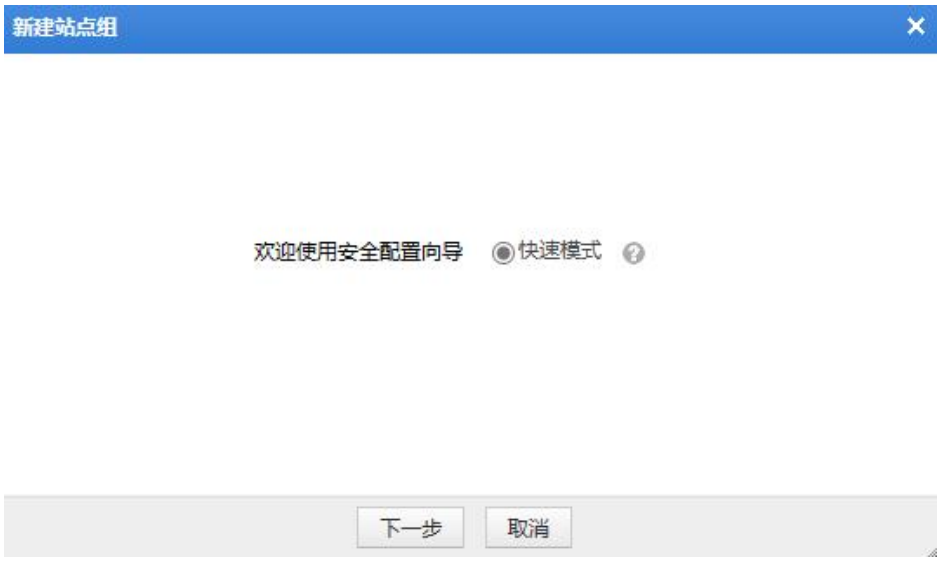
4.3.1.1 新建站点组

系统支持使用快速模式新建站点组。使用该模式进行站点安全配置时，会自动生成一套安全解决方案。该安全方案中会加载系统的默认配置策略，但不对任何服务器生效。只有在站点组管理中，添加对应的服务器信息后，才能对指定的服务器进行安全防护。

步骤 1 单击站点组树图右上角的图标，或者“root”根目录右侧的图标，弹出新建站点组对话框。

如图 4-9 所示

图 4-9 新建站点组



步骤 2 单击【下一步】按钮，进入站点组命名界面，如图 4-10 所示。

图 4-10 快速模式站点组命名

步骤 3 输入站点组名称，单击【完成】按钮，完成新建站点组并返回站点防护页面。

此时，新建的站点组内没有任何站点，需要后续添加站点和策略，才能对站点组内站点进行防护。添加站点的详细操作请参见新建站点（反向代理模式）。

----结束

步骤 4 单击【新建】按钮，进入新建站点界面，如图 4-11 所示。

图 4-11 新建站点

步骤 5 配置站点参数，参数说明如表 4-4 所示。

表 4-4 站点参数

配置项	描述
服务器名称	站点的名称，不能包含<>"字符，最长不能超过 25 个字符。
服务器类型	访问站点使用的协议，有 HTTP 和 HTTPS 两类。 如果选择 https 协议，还需配置证书文件。
服务器 IP 地址	防护服务器的 IP 地址，支持多个 IP 地址，单击图标，增加 IP 地址，最多可增加到 25 个。 说明 • 仅在串联模式、旁路模式下支持多服务器 IP 地址。 • IP 地址可以是单个 IP 地址和 IP 地址段,IP 地址支持 IPv4 和 IPv6。 • 若一个站点中配置的 IP 段有重复，匹配时，命中其中 1 个 IP 段即停止匹配。
服务器端口	访问防护服务器的端口。 • 服务器类型为 HTTP 时，最多可输入 128 个端口，多个端口以逗号分隔。 • 服务器类型为 HTTPS 时，只能输入一个端口。
开启 Web 访问日志	选择是否开启 web 访问日志。开启后，该站点所有经过 WAF 的访问请求都会记录访问日志；如果不开启，则不进行记录。
开启访问量统计	选择是否开启访问量统计。开启后，该站点所有经过 WAF 的访问流量都会进行流量统计；如果不开启，则不进行统计。
HTTP 解码失败告警	选择是否开启 HTTP 解码失败告警。开启后，WAF 对来自该站点的请求进行解码，当解码失败后，WAF 将进行告警；如果不开启，则解码失败后不会进行告警。

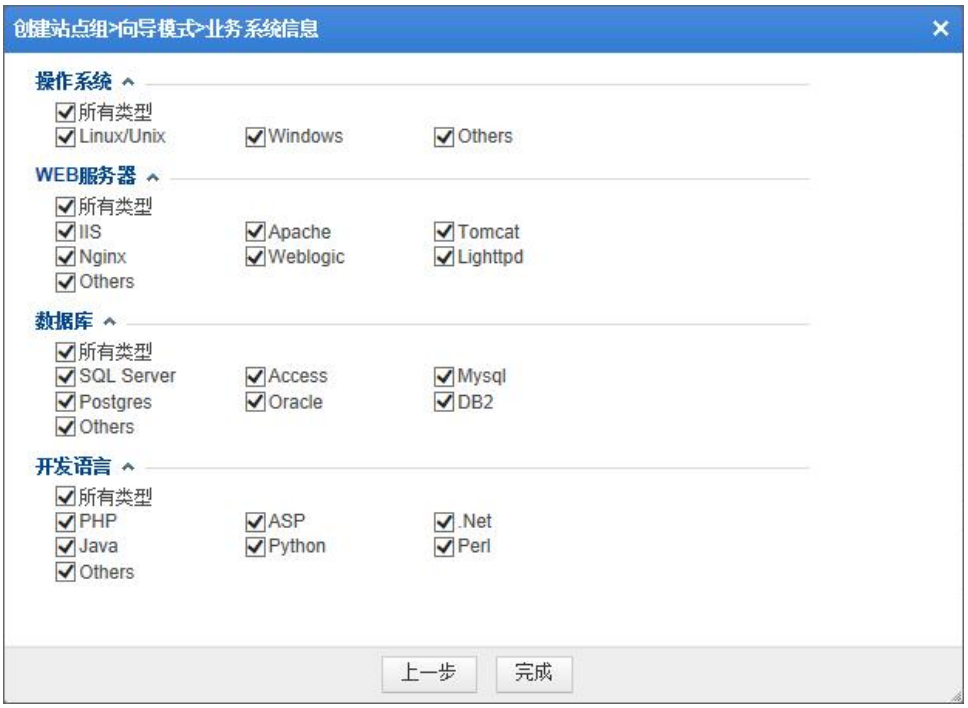
配置项	描述
HTTP 解码失败动作	WAF 会对客户端请求数据先做解码，解码失败后会根据选择的动作进行处理。 • **全部阻断**：所有检测项动作均为阻断，其中一个检测项解码失败后，WAF 会直接关闭当前连接。 • **全部放过**：所有检测项动作均为放过，其中一个检测项解码失败后，WAF 会将该连接所有请求数据直接转发，不过任何安全防护策略。 • **自定义**：自定义某一检测项的动作为阻断或放过，在触发此检测项时，根据选择的动作，WAF 进行阻断和放过操作。
开启 gzip	选择是否开启 gzip。 如果 WAF 配置了跨站请求伪造防护、敏感信息过滤、内容过滤、webshell 防护 4 个响应方向策略中的一个或多个，那么： • 开启 gzip，WAF 支持检测并向客户端返回 gzip 压缩的响应报文； • 不开启 gzip，WAF 支持检测，但客户端收到的响应报文未进行压缩传输。
gzip 压缩等级	开启 gzip 后选择 gzip 压缩等级。 压缩等级取值范围：1~9，值越高，压缩率越高，压缩速度越慢（1 最高压缩速度，9 最高压缩率）。
Content-type	WAF 进行 gzip 压缩的文件类型。 WAF 默认支持压缩的常见文件类型包括：text、application/x-javascript、application/json、application/javascript。 用户可根据需要自行输入文件类型。
SSL 协议选择	选择 SSL 协议类型，可选项包括： • 通用协议：选择通用协议新建普通站点。 • 国密协议：选择国密协议则新建的是国密站点。 说明 此配置项仅当以下条件均满足时才需配置： 服务器类型选择“HTTPS”。 系统维护员（maintainer）在 系统管理 > 系统参数配置 > 其他参数 中开启了国密模式。 • 反向代理部署模式不支持 SSL 协议选择字段
证书文件	如果服务器类型选择 HTTPS 协议，还需配置协议使用的证书。可以选择已有证书或上传新的证书。 • **选择已有证书**：选择系统内置或用户已上传的证书，管理员可以管理已有的证书文件，详情请参见 4.11 上传文件管理。 • **上传证书**：上传新的证书到 WAF。
SSL 卸载	是否启用 SSL 卸载功能。 说明 仅当服务器类型为 HTTPS 时可配置的高级选项。
客户端	• SSL 版本：WAF 支持的 SSL 版本，可以选择多个 SSL 版本。 • 加密算法：选择 WAF 与客户端通信使用的 SSL 加密算法，可以选择单个或多个，算法由系统内置。

配置项	描述
	说明 仅当服务器类型为 HTTPS 时可配置的高级选项。
服务器	• SSL 版本：WAF 支持的 SSL 版本，可以选择多个 SSL 版本。 • 加密算法：选择 WAF 与服务器通信使用的 SSL 加密算法，可以选择单个或多个，算法由系统内置。 说明 仅当服务器类型为 HTTPS 时可配置的高级选项。

步骤 6 单击【确定】按钮，新建站点完成，界面自动返回站点列表界面。

步骤 7 单击【下一步】按钮，进入配置站点组业务系统信息界面，如图 4-12 所示。

图 4-12 选择站点组业务系统信息



步骤 8 配置业务系统信息。

管理员可以选择站点防护服务器的操作系统、WEB 服务器、数据库服务器以及开发语言的类型。

默认情况下，业务系统信息为全部选择状态；管理员可以根据业务系统的实际情况进行相应的选择。

步骤 9 单击【完成】按钮，保存配置，完成向导模式站点组新建操作。界面自动返回到站点防护页面。

----结束

4.3.1.2 编辑站点组

编辑站点组包括修改站点组基本信息、站点组内站点信息、站点组内虚拟站点信息。

在站点组树图中单击某一站点组，打开该站点的管理配置页面，如图 4-13 所示。

图 4-13 站点组管理配置

编辑站点组基本信息

- 单击站点组基本信息列表“操作”栏中的图标，编辑该站点组的名称及业务系统信息。
- 单击站点组基本信息列表“操作”栏中的图标，跳转到该站点组的自学习策略配置页面。自学习策略配置的详细操作请参见 4.4 自学习策略。

编辑站点组中的站点信息

- 单击【新建站点】按钮，为站点组添加新站点。
- 单击站点列表操作栏中的图标，编辑站点信息。

编辑站点组中的虚拟站点信息

- 单击【新建虚拟站点】按钮，为站点组添加新虚拟站点。
- 单击虚拟站点列表操作栏中的图标，编辑虚拟站点信息。

4.3.1.3 管理区域访问量全局统计

区域访问量全局统计是指，对站点资源中所有配置了防护策略被 WAF 防护的站点 IP 进行访问量统计，区域访问量统计的站点包含虚拟站点。

- 单击站点组树图右上角的图标，启用区域访问量全局统计功能，功能启用后图标变为。
- 单击站点组树图右上角的图标，停用区域访问量全局统计功能，功能停用后图标变为。

4.3.1.4 调整站点组优先级

选择菜单 **安全管理** > **站点防护**，进入站点防护管理页面，如图 4-8 所示。

单击站点组列表中各个站点组相应的图标或，向上或向下调整站点组的优先级，排在上面的站点组优先级高于排在下面的站点组。

4.3.1.5 策略一键接受

一键接受同时作用于站点组及虚拟站点，范围包括 Web 安全防护（内置 HTTP 协议校验除外）和数据安全传输。

开启后，不论站点组及虚拟站点应用的策略动作为何，其防护检测状态都置为接受。

开启/关闭策略一键接受有两种方法：

- 在站点组树图中，单击站点组根目录 root，进入站点组列表管理页面，勾选一个或多个站点组，单击【批量操作】按钮，在批量操作下拉菜单中选择“开启/关闭一键接受”，为多个站点组开启/关闭一键接受功能。
- 在站点组树图中，单击某个站点组，在右侧该站点组管理页面中单击【开启】/【关闭】按钮，开启/关闭该站点组一键接受功能。

4.3.1.6 删除站点组

删除站点组有两种方法：

- 在站点组树图中，鼠标移动到某个站点组时，显示删除图标，如图 4-14 所示，单击该图标，单击确认删除对话框中的【确定】按钮，删除对应的站点组。

图 4-14 删除站点树中的站点组

- 单击站点组树图中根目录“root”，进入站点组列表页面，单击站点组列表中站点名称后的图标，单击确认删除对话框中的【确定】按钮，删除对应站点组。

----结束

4.3.2 管理站点

管理员可以对站点进行如下操作：

- 新建站点
- 启用/停用站点
- 批量操作
- 配置站点安全策略
- 删除站点

4.3.2.1 新建站点

在串联模式/旁路模式下新建站点和在反向代理模式下有所区别，下面分别介绍 3 种情况下新建站点的具体步骤。

新建站点（串联/旁路）

步骤 1 单击站点组树图中的某一站点组，进入该站点组管理页面。

步骤 2 单击站点列表右下方的【新建站点】按钮，弹出新建站点对话框，如图 4-15 所示。

图 4-15 新建站点 – 串联/旁路

步骤 3 配置站点参数，参数说明如表 4-4 所示。

步骤 4 单击【完成】按钮，保存配置，并返回站点组管理页面。

如还需增加站点，单击【继续新建】按钮，继续新建站点。

----结束

步骤 5 配置站点参数，参数说明如表 4-5 所示。

表 4-5 站点参数说明

配置项	描述
服务器名称	站点的名称，不能包含<>"字符，最长不能超过 25 个字符。
服务器类型	访问站点使用的协议，有 HTTP 和 HTTPS 两类。。 说明

配置项	描述
	仅当系统维护员在 **系统管理** > **站点控制** 中开启了 HTTPS 站点开关后，才有 HTTPS 选项。
服务器 IP 地址	防护服务器的 IP 地址，支持输入 IP 段，IP 地址支持 IPv4 和 IPv6。如果定义单个 IP 地址，只输入开始 IP 地址即可。
服务器端口	访问防护服务器的端口。 最多可输入 128 个端口，多个端口以逗号分隔。
开启 Web 访问日志	选择是否开启 web 访问日志。开启后，该站点所有经过 WAF 的访问请求都会记录访问日志；如果不开启，则不进行记录。
开启访问量统计	选择是否开启访问量统计。开启后，该站点所有经过 WAF 的访问流量都会进行流量统计；如果不开启，则不进行统计。
HTTP 解码失败告警	选择是否开启 HTTP 解码失败告警。开启后，WAF 对来自该站点的请求进行解码，当解码失败后，WAF 将进行告警；如果不开启，则解码失败后不会进行告警。
证书文件	如果服务器类型选择 HTTPS 协议，还需配置协议使用的证书。可以选择已有证书或上传新的证书。 • **选择已有证书**：选择用户上传服务器的 SSL 证书，管理员可以管理已有的证书文件，详情请参见 4.11 上传文件管理。 • **上传证书**：上传新的证书到 WAF。

步骤 6 单击【完成】按钮，保存配置，并返回站点组管理页面。

如还需增加站点，单击【继续新建】按钮，继续新建站点。

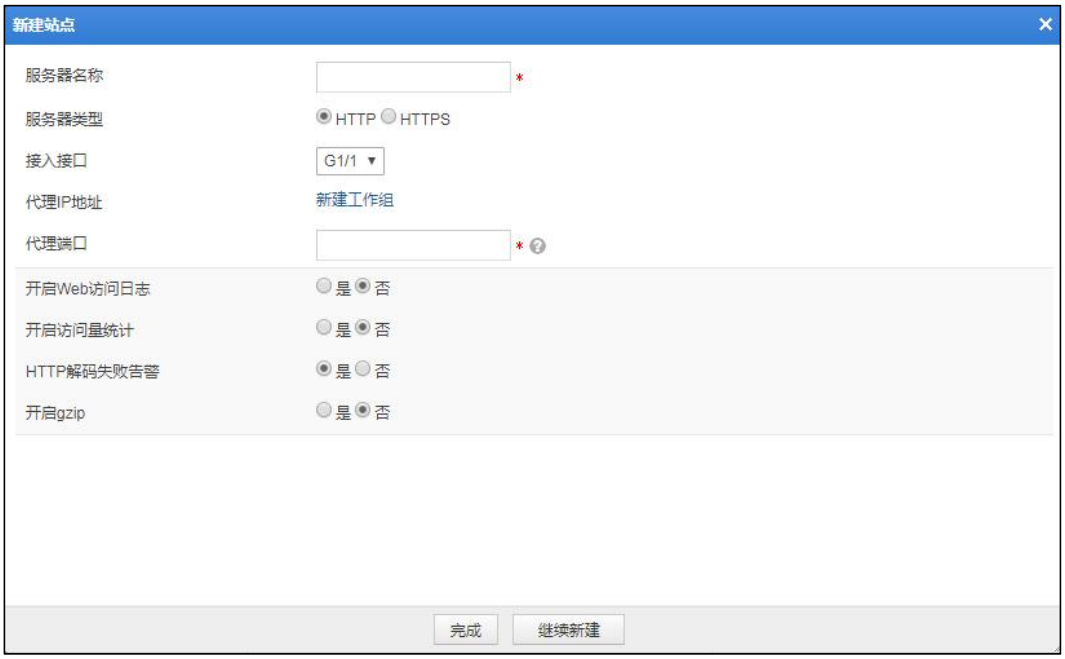
----结束

新建站点（反向代理模式）

步骤 1 单击站点组树图中的某一站点组，进入该站点组管理页面。

步骤 2 单击站点列表右下方的【新建站点】按钮，弹出新建站点对话框，如图 4-16 所示。

图 4-16 新建站点 – 反向代理模式



步骤 3 配置站点参数，参数说明如表 4-6 所示。

表 4-6 站点参数说明 – 反向代理模式

配置项	描述
服务器名称	站点的名称，不能包含<>"字符，最长不能超过 25 个字符。
服务器类型	访问站点使用的协议，有 http 和 https 两类。 如果选择 https 协议，还需配置证书文件。
接入接口	代理接入的接口，只能选择 WAN 工作口，有关工作口的配置请参见 7.1.1 工作组管理。
代理 IP 地址	代理接口的 IP 地址，选择接入接口后，会自动展示出该接口上已有的 IP 地址，若该接口上未配置地址，可直接编辑接口，详情请参见 7.1.1 工作组管理的相关介绍。在接口配置中，IP 地址支持 IPv4 和 IPv6。一个接口上可配置 253 个 IP 地址。
代理端口	WAF 代理的通信端口。 服务器类型为 HTTP 或 HTTPS 时，都只能输入一个端口。
开启 Web 访问日志	是否开启 web 访问日志。开启后，所有经过 WAF 的访问请求都会记录访问日志；如果不开启，则不进行记录。
开启访问量统计	是否开启访问量统计。开启后，该站点所有经过 WAF 的访问流量都会进行流量统计；如果不开启，则不进行统计。
HTTP 解码失败告警	选择是否开启 HTTP 解码失败告警。开启后，WAF 对来自该站点的请求进行解码，当解码失败后，WAF 将进行告警；如果不开启，则解码失败后不会进行告警。
开启 gzip	选择是否开启 gzip。 如果 WAF 配置了跨站请求伪造防护、敏感信息过滤、内容过滤、webshell 防护 4 个响应方向策略中的一个或多个，那么： • 开启 gzip，WAF 支持检测并向客户端返回 gzip 压缩的响应报文；

配置项	描述
	• 不开启 gzip，WAF 支持检测，但客户端收到的响应报文未进行压缩传输。
gzip 压缩等级	开启 gzip 后选择 gzip 压缩等级。 压缩等级取值范围：1~9，值越高，压缩率越高，压缩速度越慢（1 最高压缩速度，9 最高压缩率）。
Content-type	WAF 进行 gzip 压缩的文件类型。 WAF 默认支持压缩的常见文件类型包括：text、application/x-javascript、application/json、application/javascript。 用户可根据需要自行输入文件类型。
SSL 协议选择	选择 SSL 协议类型，可选项包括： • 通用协议：选择通用协议新建普通站点。 • 国密协议：选择国密协议则新建的是国密站点。 说明 此配置项仅当以下条件均满足时才需配置： • 服务器类型选择 HTTPS 协议； • 系统维护员在 **系统管理** > **系统参数配置** > **其他参数** 中开启了国密模式。
证书文件	如果服务器类型选择 https 协议，还需配置协议使用的证书。可以选择已有证书或上传新的证书。 • **选择已有证书**：选择系统内置或用户已上传的证书，管理员可以管理已有的证书文件，详情请参见 4.11 上传文件管理。 • **上传证书**：上传新的证书到 WAF。
SSL 卸载	是否启用 SSL 卸载功能。 说明 仅当服务器类型为 HTTPS 时可配置的高级选项。
客户端	• SSL 版本：WAF 支持的 SSL 版本，可以选择多个 SSL 版本。 • 加密算法：选择 WAF 与客户端通信使用的 SSL 加密算法，可以选择单个或多个，算法由系统内置。 说明 仅当服务器类型为 HTTPS 时可配置的高级选项。
服务器	• SSL 版本：WAF 支持的 SSL 版本，可以选择多个 SSL 版本。 • 加密算法：选择 WAF 与服务器通信使用的 SSL 加密算法，可以选择单个或多个，算法由系统内置。 说明 仅当服务器类型为 HTTPS 时可配置的高级选项。

步骤 4 单击【完成】按钮，保存配置，并返回站点组管理页面。

如还需增加站点，单击【继续新建】按钮，继续新建站点。

----结束

4.3.2.2 启用/停用站点

新建的站点默认为启用状态。

单击站点组树图中的根目录“root”，进入站点组列表页面，或者单击站点组树图中的某一站点组，进入该站点组管理页面，均可对站点进行启用/停用操作。

- 单击某个未启用站点“操作”栏中的图标，对应站点状态变为，表示该站点已启用。
- 单击某个已启用站点“操作”栏中的图标，对应站点状态变为，表示该站点已停用。

4.3.2.3 批量操作

管理员可以批量对多个站点组及站点组下的站点进行开启/关闭站点访问量、删除、启用、停用操作。

站点访问量是指，站点资源中所有站点的访问量统计数据，这里的站点不包括虚拟站点。

步骤 1 在站点组树图中单击根目录“root”，进入站点组列表管理页面。

步骤 2 选择多个需要操作的站点或站点组。

步骤 3 单击【批量操作】按钮，显示批量操作下拉菜单。

步骤 4 单击需要进行的操作。

----结束

4.3.2.4 配置站点安全策略

站点安全策略包括：

- HTTP Flood 防护策略
- 数据安全传输策略
- Web 安全防护策略
- 例外控制策略
- 会话追踪策略
- 风险级别控制策略
- Web 解码
- 误报分析
- 误报分析结果

配置 HTTP Flood 防护策略

当 WAF 判断出客户端攻击服务器后，会在服务器发给客户端的数据包中，添加一些验证信息，如果客户端返回给服务器的数据包中存在同样的验证信息，则客户端通过验证。

在站点组树图中单击某一站点组，在右侧该站点组管理页面中选择“HTTP Flood 防护”页签，进入 HTTP Flood 防护策略配置界面，如图 4-18 所示。

图 4-17 HTTP Flood 防护策略

HTTP Flood 防护策略配置包括全局参数配置、HTTP Flood 防护策略和定制防护策略三个配置。

开启/关闭 HTTP Flood 防护策略。

HTTP Flood 防护策略默认开启，单击图 4-18 中**防护控制**区域的【关闭】按钮或【开启】按钮，关闭或开启 HTTP Flood 防护策略。

配置全局参数

步骤 1 在图 4-18 中**全局设置**区域中设置 HTTP Flood 全局参数，全局参数说明如表 4-8 所示。

表 4-7 HTTP Flood 防护全局参数

配置项	描述
攻击保持时间	启动防护的时间范围，默认值为 300。
信任时间	客户端验证通过后，WAF 将客户端 IP 放到信任列表中的时间长度，默认值为 1800 秒。
验证码自动更新周期	WAF 向客户端发送的验证码是随时间变化的，更新周期就是更换验证码的时间间隔，默认值为 5 分钟。
最大信任次数	客户端被 WAF 放入信任列表后，在信任时间段内允许客户端请求超过阈值的最大次数，默认值为 7200 次。

步骤 2 单击【确定】按钮，保存配置。

----结束

新建 HTTP Flood 防护策略

步骤 1 单击图 4-18 中 **HTTP Flood 防护策略**区域的【新建】按钮，弹出新建 HTTP Flood 防护策略对话框，如图 4-19 所示。

图 4-18 新建 HTTP Flood 防护策略

步骤 2 配置 HTTP Flood 防护策略参数，参数详细信息如表 4-9 所示。

表 4-8 HTTP Flood 防护策略参数说明

配置项	描述
名称	HTTP Flood 防护策略的名称。
站点选择	HTTP Flood 防护策略适用的站点。
目标 IP&端口	代理服务的 IP 地址和端口号，IP 地址支持 IPv4 和 IPv6。
算法	算法有四种： • **HTTP Cookie**：WAF 添加的验证数据是 http 协议的 Cookie 值，如果 WAF 接收到的数据包包含 Cookie 值，则客户端通过验证。 • **URL Cookie**：该算法是 WAF 给客户端的回应数据中添加一个附带 Cookie 值的重定向 URL。如果客户端将该 Cookie 值返回给 WAF，则客户端通过验证。 • **ascii-image**：该算法是图片验证算法，将验证信息放到一定数量的字符组成的图片中发送给客户端，需要客户端给出应答验证信息，才能通过验证。 • **bmp-image**：该算法是图片验证算法，将验证信息以 bmp 格式的图片形式发送给客户端，需要客户端给出应答验证信息，才能通过验证。

配置项	描述
阈值 Get	WAF 每秒接收到 GET 请求的最大数值，超过该值认为是 flood 攻击。
阈值 Post	WAF 每秒接收到 POST 请求的最大数值，超过该值认为是 flood 攻击。

步骤 3 单击【确定】按钮，保存配置。

----结束

新建定制防护策略

步骤 1 单击图 4-18 中**定制防护策略**区域的【新建】按钮，弹出新建定制防护策略对话框，如图 4-20 所示。

图 4-19 新建定制防护策略

步骤 2 配置定制防护策略参数，参数详细说明如表 4-10 所示。

表 4-9 定制防护策略参数说明

配置项	描述
名称	定制防护策略的名称。
站点选择	定制防护策略适用的站点。
目标 IP&端口	代理服务的 IP 地址和端口号，IP 地址支持 IPv4 和 IPv6。
域名	被保护网站的域名。
路径	被防护策略保护的 URL 路径。

配置项	描述
算法	算法有四种： • **HTTP Cookie**：WAF 添加的验证数据是 http 协议的 Cookie 值，如果 WAF 接收到的数据包包含 Cookie 值，则客户端通过验证。 • **URL Cookie**：该算法是 WAF 给客户端的回应数据中添加一个附带 Cookie 值的重定向 URL。如果客户端将该 Cookie 值返回给 WAF，则客户端通过验证。 • **ascii-image**：该算法是图片验证算法，将验证信息放到一定数量的字符组成的图片中发送给客户端，需要客户端给出应答验证信息，才能通过验证。 • **bmp-image**：该算法是图片验证算法，将验证信息以 bmp 格式的图片形式发送给客户端，需要客户端给出应答验证信息，才能通过验证。

步骤 3 单击【确定】按钮，保存配置。

----结束

配置数据安全传输策略

通过配置数据安全传输，WAF 可以将普通的 HTTP 请求，强制转换成 HTTPS 请求，从而提高传输的安全性。

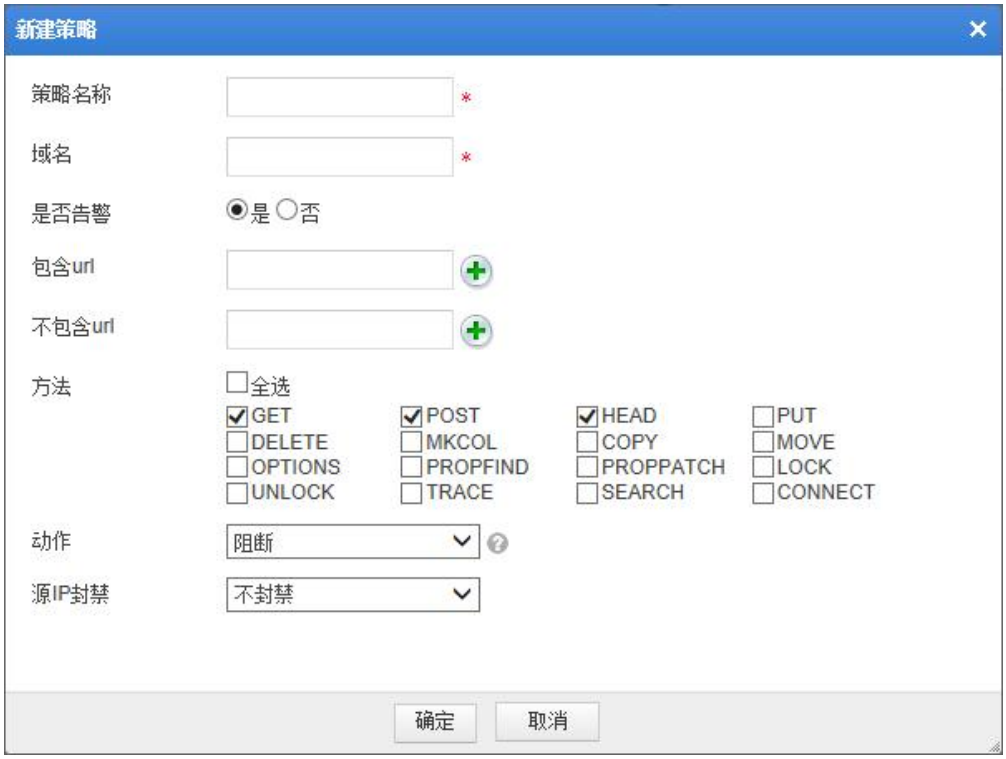
在站点组树图中单击某一站点组，在右侧该站点组管理页面中选择“数据安全传输”页签，进入数据安全传输策略管理界面，如图 4-21 所示。

图 4-20 数据安全传输策略

新建数据安全传输策略

步骤 1 单击图 4-21 中的【新建策略】按钮，弹出新建数据安全传输策略对话框，如图 4-22 所示。

图 4-21 新建数据安全传输策略



步骤 2 配置数据安全传输策略参数，参数详细说明如表 4-11 所示。

表 4-10 数据安全传输策略参数说明

配置项	描述
策略名称	数据安全传输策略的名称。
域名	被保护的域名。
是否告警	是否产生告警日志。
包含 url	需要进行数据安全传输管理的 url 路径，可输入多个。
不包含 url	不需要进行数据安全传输管理的 url 路径，可输入多个。
方法	客户端访问服务器端时可使用的进行数据安全传输管理的方法，可多选。
动作	WAF 对符合条件的请求可执行三种类型的动作： • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**，表示不对源 IP 进行封禁； • **永久封禁**，表示永久阻断该源 IP 的访问； • **自定义封禁**，表示在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。

配置项	描述
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。 • **自定义**：需在“重定向路径”中输入重新定向的 URL 地址。重定向路径应为完整的 URL，最大长度为 2048 个字符，如：http://www.example.com。 • **当前 url https**：需在“https 端口”中输入当前 https 的访问端口，默认为 443。 • **上一级页面**：表示重定向到客户端访问页面的上一级页面 HTTPS 版本。 说明 • 请确保重定向后 URL 存在，并已经在 WAF 上配置对应站点，否则该 URL 会出现无法访问，或者无防护效果。 • 根据 RFC 协议规范，除 GET，HEAD 方法外，不建议配置为重定向动作。

步骤 3 单击【确定】按钮，保存配置。

----结束

数据安全传输策略其他操作

管理员可以在图 4-21 所示数据安全传输配置列表中，对数据安全传输策略列表中的策略进行以下操作：

- 编辑策略

  单击某数据安全传输策略相应“操作”栏中的图标，可以重新编辑该数据安全传输配置的参数。

- 启用/停用策略

  新建的数据安全策略默认为启用状态。

  单击某数据安全传输策略相应“操作”栏中的图标或，启用/停用该策略。

- 删除策略

  单击某数据安全传输策略相应“操作”栏中的图标，在弹出的确认删除窗口中单击【确定】按钮，删除该策略。

- 转到站点组管理页面

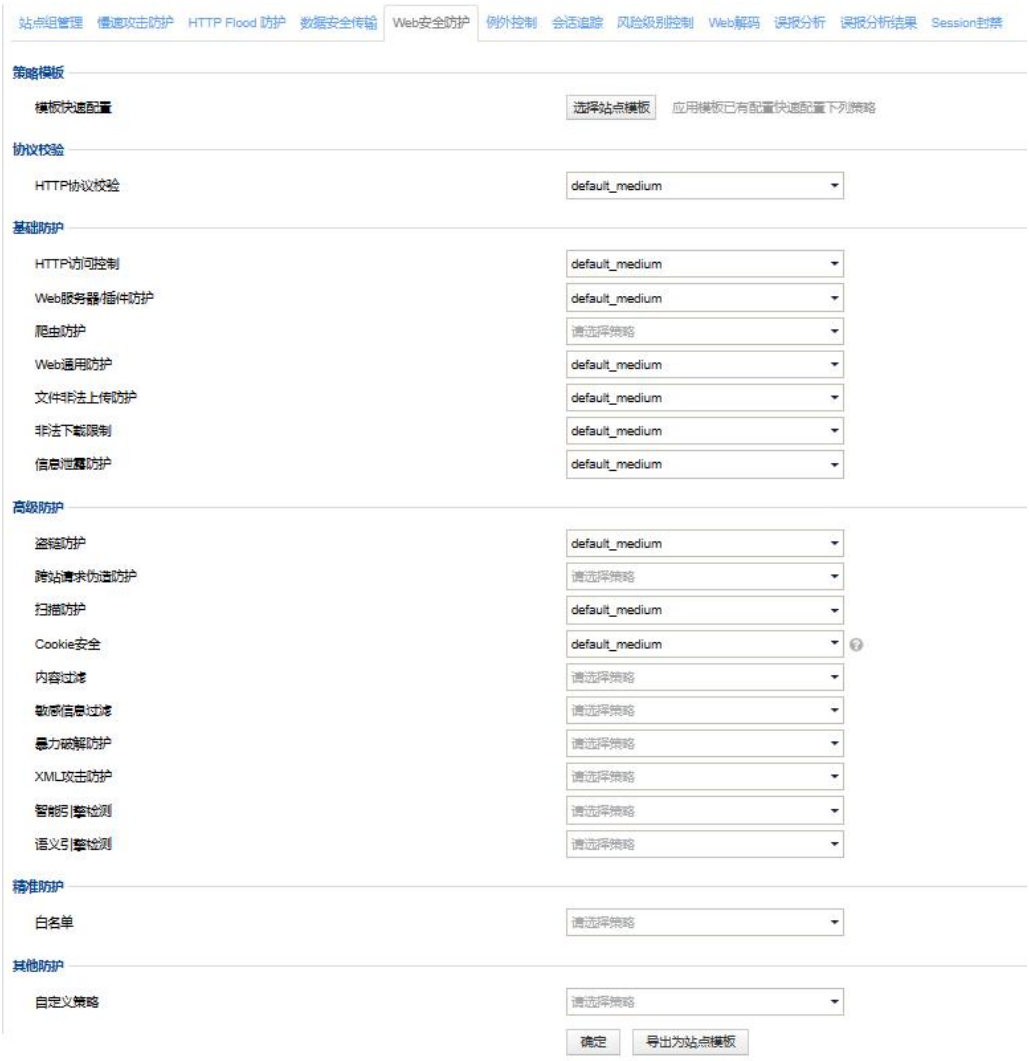
  单击某数据安全传输策略相应“操作”栏中的图标，跳转到站点所属站点组管理页面。

配置 Web 安全防护策略

Web 安全防护，可以为站点组加载已有通用配置的策略或新建策略，一个策略能被多个站点组加载。有关通用策略的配置，请参见 4.7 策略管理的相应介绍。

在站点组树图中单击某一站点组，在右侧该站点组管理页面中选择“Web 安全防护”页签，进入 Web 安全防护策略管理界面，如图 4-23 所示。

图 4-22 Web 安全防护策略



说明	• 只要 HTTP 请求中的主机名（含端口号）匹配了策略中所定义的 Host，即为命中策略。 • 以上策略匹配原则决定了，针对一个主机名只可能有一条 Cookie 安全策略被命中。WAF 对该主机名下所有命中策略的 Cookie 执行统一的加密或签名操作。 • 如果配置了多条 Cookie 安全策略，WAF 以界面呈现的顺序，从上至下进行策略匹配。用户可以在界面上调整策略的顺序，以实现特定的需求。

快速配置 Web 安全防护策略

如果配置了策略模板，即可在为站点配置 Web 安全防护时，直接选择相应的站点模板，进行策略的快速配置，无须逐一选择不同策略下不同类型的策略，有关站点模板的介绍，请参见 4.8.1 站点模板。

快速配置 Web 安全防护策略步骤如下：

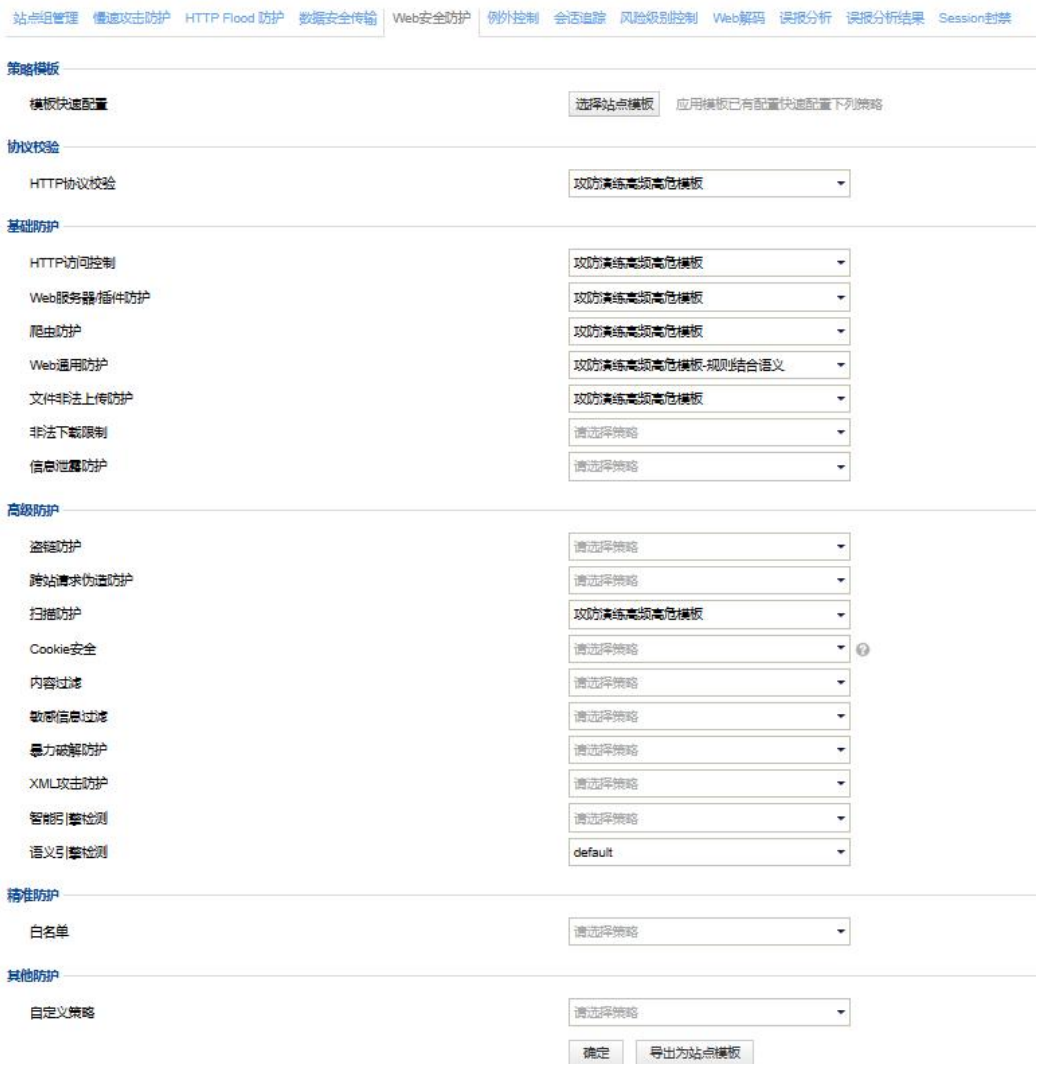
步骤 1 单击图 4-23 中**策略模板**区域中的【选择站点模板】按钮，弹出选择站点模板对话框，如图 4-24 所示。

图 4-23 选择站点模板

步骤 2 选择站点模板（以选择“default_medium”为例）。

步骤 3 单击【确定】按钮，返回 Web 安全防护策略管理页面，可见此时所有策略都已默认选择了**攻防演练高频高危模板-规则结合语义**类型的策略，如图 4-25 所示。

图 4-24 快速配置 Web 安全模板



步骤 4 单击【确定】按钮，保存配置。

如果保存失败，系统弹出“Web 安全防护策略配置失败，请稍后重试”的提示信息，此时建议用户稍等片刻，重新进行站点策略的引用操作。

----结束

引用策略

步骤 1 单击图 4-23 中**协议校验**区域中 HTTP 协议校验右侧的下拉框显示按钮，显示当前所有类型的策略，如图 4-26 所示。

图 4-25 HTTP 协议校验类型

步骤 2 选择指定协议校验策略。

步骤 3 单击图 4-23 中页面下方的【确定】按钮，保存配置。

如果保存失败，系统弹出“Web 安全防护策略配置失败，请稍后重试”的提示信息，建议用户稍等片刻，重新进行站点策略的引用操作。

----结束

取消已选策略

取消策略的具体操作如下：

步骤 1 在如图 4-23 所示的 Web 安全防护配置页面，单击某个策略右侧的下拉框显示按钮，显示当前所有类型的策略。

步骤 2 单击【取消已选策略】按钮，取消已选择的策略。

步骤 3 单击【保存】按钮，完成配置。

----结束

新建策略

步骤 1 在如图 4-23 所示的 Web 安全防护配置页面，单击某个策略右侧的下拉框显示按钮，显示当前所有类型的策略。

步骤 2 单击“新建策略”链接，进入新建当前策略页面。

新建策略的详细操作请参见 4.7 策略管理。

----结束

导出为站点模板

步骤 1 单击图 4-23 所示页面下方的【导出为站点模板】按钮，弹出确认导出为站点模板对话框。

步骤 2 单击【确定】按钮确认导出，在弹出的站点名称设置对话框中输入站点模板名称，如图 4-27 所示。

图 4-26 设置模板名称

步骤 3 单击【确定】按钮，系统提示“导出成功”，表示成功导出当前策略选择的配置为站点模板。

导出后的模板可以在站点模板中查看和管理。有关站点模板的介绍，请参见 4.8.1 站点模板。

----结束

配置例外策略

在站点组树图中单击某一站点，在右侧该站点管理页面中选择“例外控制”页签，进入例外控制策略配置界面，如图 4-28 所示。

图 4-27 例外控制策略

加载例外策略

加载例外策略的具体操作如下：

步骤 1 在如图 4-28 所示的例外控制配置页面，单击例外策略右侧的下拉框显示图标，在显示的所有当前类型的例外策略中选择策略，如图 4-29 所示。

图 4-28 选择例外策略

步骤 2 选择指定例外策略后，单击【确定】按钮，完成配置。

----结束

取消已选例外策略

取消例外策略的具体操作如下：

步骤 1 在如图 4-28 所示的例外控制配置页面，单击例外策略右侧的下拉框显示图标，在显示的所有当前类型的例外策略中单击【取消已选策略】按钮，取消已选择的例外策略，如图 4-29 所示。

步骤 2 单击【确定】按钮，完成配置。

----结束

新建例外策略

单击图 4-29 中的“新建策略”链接，进入新建当前例外策略的配置页面，新建例外策略。有关新建例外策略的详细介绍请参见 4.7.5.1 配置例外策略。

配置会话追踪策略

会话追踪（Session Tracking）通过追踪用户向 Web 应用服务器发起的访问请求以及用户所有的 Web 操作，并记录详细的访问日志，为攻击事件事后分析、攻击场景还原、以及关联用户所有的 Web 操作提供关联分析数据基础，同时还能进行用户行为研究，了解用户操作背后是否隐藏了潜在的攻击动机。

WAF 的会话追踪策略能够基于站点组对以下两种会话进行追踪。

- 用户通过客户端浏览器访问被 WAF 保护的 Web 服务器，当 WAF 与客户端浏览器成功建立连接后，WAF 向浏览器下发一个包含

  WAF_Client_Id（简称 WCI）的 cookie，此后，在 WCI 的超时时间范围内（WCI 默认超时时间为 1 天，该值可通过后台配置），该用户所有请求中都包含该信息，用于 WAF 追踪该用户的所有操作；WAF 将为从同一客户端的不同浏览器发起的请求分配不同的 WCI，从而追踪来自同一客户端所有浏览器的服务器访问操作。
- 用户通过客户端浏览器访问被 WAF 保护的 Web 服务器，如果 Web 服务器为用户返回了包含服务器 session id 的 cookie，那么 WAF 也会为该用户下发一个包含 WAF_Session_Id（简称 WSI）的一次性 cookie，此后，该用户所有请求中均包含这两个 cookie，用于 WAF 追踪该登录用户的所有操作过程。

会话追踪策略的配置步骤如下：

步骤 1 在站点组树图中单击某一站点组，在右侧该站点组管理页面中选择“会话追踪”页签，进入会话追踪策略配置页面，如图 4-30 所示。

图 4-29 会话追踪策略

步骤 2 开启/关闭会话追踪功能。

会话追踪策略默认关闭，选择“会话追踪启用”后的单选按钮，开启或关闭会话追踪功能。

步骤 3 配置会话追踪策略参数。

会话追踪策略参数说明如表 4-12 所示。

表 4-11 会话追踪策略参数

配置项	描述
会话追踪启用	是否启用会话追踪功能。
会话标示符	被追踪源 IP 的后续会话标示符。只有当源 IP 后续访问的页面类型在选择的会话标示符范围内时，会话才会被追踪。 WAF 共支持如下 11 种会话标示符，用户可根据情况在下拉列表中进行单选或多选。 （1）ASP-DOT-NET-session （2）ASPSESSIONID-session （3）ColdFusion-session （4）J2EE-JSESSIONID-Cookie-session （5）J2EE-JSESSIONID-URL-session （6）J2EE-session （7）JWS-ID-session （8）PHP-BB-MYSQL-session （9）PHPSESSID-session （10）PHPSESSIONID-session （11）SAP-session 说明 可通过后台修改配置文件的方式进行自定义会话标识符。
资源追踪模式	会话追踪时的资源追踪模式。可选项有：

配置项	描述
	• **全部**：WAF 对所有类型资源的访问行为进行追踪。 • **仅追踪指定资源**：WAF 仅对指定类型资源的访问行为进行追踪。 • **不追踪指定资源**：WAF 不对指定类型资源的访问行为进行追踪。
文件扩展名	被追踪资源的文件类型。WAF 支持输入多个扩展名，多个扩展名之间使用分号分隔。 当参数“资源追踪模式”选择**仅追踪指定资源**和**不追踪指定资源**时，必须配置。
追踪用户名	是否追踪用户名。 选择**是**，则在用户在成功登录后、注销前这一段时间内，在 WAF 上触发的所有基于单个会话触发的日志可关联到用户名。
登录参数	追踪用户名的登录参数包括登录 URL 和用户名参数。 • **登录 URL**：①URL 格式支持 host + uri-path + query-string；②输入 URL 内容时，不包含“http://”，后台处理时默认在 URL 前加上“http://”，若用户想要输入 HTTPS 的 URL，则必须在输入框中手动输入“https://”；③最多可输入 10 条 URL 信息。 • **用户名参数**：①最多输入 10 个用户名；②输入内容长度上限为 256 字节。

步骤 4 单击【确定】按钮，保存配置。

----结束

风险级别控制策略

在站点组树图中单击某一站点，在右侧该站点管理页面中选择“风险级别控制”页签，进入风险级别控制策略配置界面，如图 4-31 所示。

图 4-30 风险级别控制策略

加载风险级别控制策略

加载风险级别控制策略的具体操作如下：

步骤 1 在所示的风险级别控制策略配置页面，单击风险级别策略右侧的下拉框显示图标，在显示的所有当前类型的风险级别控制策略中选择策略，如图 4-32 所示。

图 4-31 选择风险级别控制策略

步骤 2 选择策略后，单击【确定】按钮，完成配置。

----结束

取消已选风险级别控制策略

取消风险级别控制策略的具体操作如下：

步骤 1 在如图 4-32 所示的风险级别控制策略配置页面，单击风险级别策略右侧的下拉框显示图标，在显示的所有当前类型的风险级别控制策略中单击【取消已选策略】按钮，取消已选择的风险级别控制策略。

步骤 2 单击【确定】按钮，完成配置。

----结束

新建风险级别控制策略

单击图 4-32 中的“新建策略”链接，弹出新建风险级别控制策略对话框，新建风险级别控制策略。有关新建风险级别控制策略的详细介绍请参见 4.7.5.3 配置风险级别策略。

配置 Web 解码

通过配置 Web 解码，WAF 可以对请求的 URL 中经过 Base64 编码的参数值进行解码，进而对该类攻击进行攻击识别和防护。

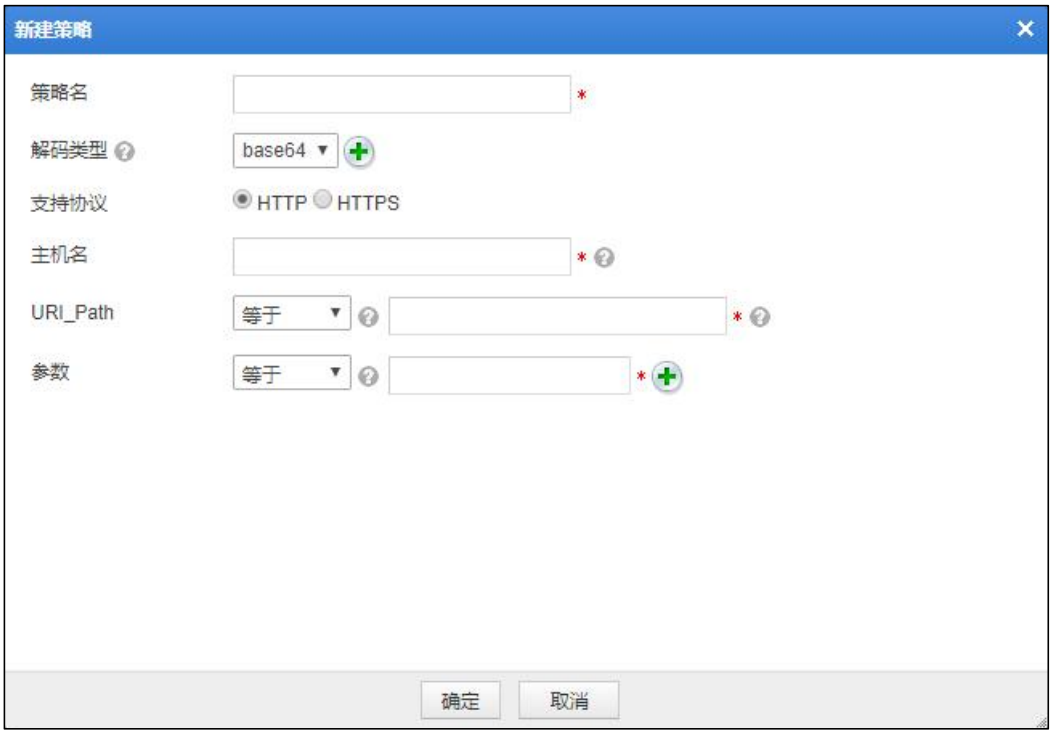
在站点组树图中单击某一站点组，在右侧该站点组管理页面中选择“Web 解码”页签，进入 Web 解码管理界面，如图 4-33 所示。

图 4-32 Web 解码

新建 Web 解码策略

步骤 1 单击图 4-33 中的【新建】按钮，弹出新建 Web 解码策略对话框，如图 4-34 所示。

图 4-33 新建 Web 解码



步骤 2 配置 Web 解码策略参数，参数详细说明如表 4-13 所示。

表 4-12 Web 解码策略参数说明

配置项	描述
策略名	Web 解码策略名称。
解码类型	WAF 解码的编码类型及层数。 在下拉框中选择编码类型，单击图标添加解码层数，单击图标减少解码层数。 解码顺序从左至右，从上至下。
支持协议	解码支持的协议，包括 HTTP 和 HTTPS。
主机名	解码对象主机的名称。
URI_Path	解码对象主机所在的 URI 路径。可通过等于、包含、正则匹配三种方式进行配置。
参数	解码的关键参数，可通过等于、包含、正则匹配三种方式进行配置。 单击图标添加参数，单击图标减少参数。

步骤 3 单击【确定】按钮，保存配置。

----结束

Web 解码策略其他操作

管理员可以在图 4-33 所示 Web 解码策略列表中，对 Web 解码策略进行以下操作：

- 编辑策略

  单击某 Web 解码策略相应“操作”栏中的图标，可以重新编辑该 Web 解码策略的参数。

- 删除策略

  单击某 Web 解码策略相应“操作”栏中的图标，在弹出的确认删除窗口中单击【确定】按钮，删除该策略。

配置误报分析

误报分析是指，通过日志分析发现 WAF 策略与业务冲突导致的误报。

误报分析基于某个站点组，分为手动分析和自动分析。自动分析和手动分析均可开启策略自动调整，以调用“自动调整配置项”中的配置。

在站点组树图中单击某一站点组，在右侧该站点组管理页面中选择“误报分析”页签，进入误报分析管理界面，如图 4-35 所示。

图 4-34 误报分析

手动分析

手动分析配置区域如图 4-36 所示。

图 4-35 手动分析

步骤 1 配置分析条件。

- 用户可以对指定时间范围内的日志进行分析。默认的可选时间范围包括：10 分钟、30 分钟、1 小时、6 小时、12 小时、1 天、3 天、7 天。除了默认的时间范围之外，也可以单击 自定义时间范围。
- 选择是否开启“自动调整”，开启后，将直接调用“自动调整配置项”中的配置。

步骤 2 单击【分析】按钮，弹出执行成功提示框后，单击【确定】按钮，下发误报分析任务。

分析任务完成后，在右侧该站点组管理页面中选择“误报分析结果”页签，可以查看分析结果。

----结束

自动分析

自动分析配置区域如图 4-37 所示。

图 4-36 自动分析

步骤 1 配置分析条件。

- 开启自动分析。
- 选择是否开启“自动调整”，开启后，将直接调用“自动调整配置项”中的配置。

- 配置自动分析的频率。
- 配置自动分析的开始时间。

步骤 2 单击【保存】按钮，WAF 将按照配置自动进行误报分析。

在站点组树图中单击某一站点组，在右侧该站点组管理页面中选择“误报分析结果”页签，可以查看分析结果。

----结束

自动调整配置项

自动调整是指，WAF 根据配置对策略进行优先修改策略或者优先添加例外的调整。

手动分析和自动分析中开启“自动调整”后，将调用自动调整配置项的配置进行修改策略或者添加例外的调整。

自动调整配置项区域如图 4-38 所示。

图 4-37 **自动调整配置项**

步骤 1 配置误报判定方式和阈值。

- 误报判定方式包括：告警 IP 数、告警比例。
  - 告警 IP 数：根据安全日志中的不同告警 IP 数量进行误报判定。
  - 告警比例：根据“安全日志中的不同告警 IP 数量/访问日志中的不同告警 IP 数量”进行误报判定。
- 误报判定阈值。
  - 告警 IP 数阈值：告警 IP 数达到或超过阈值，将根据设定进行修改策略或添加例外操作。

- 告警比例阈值：告警 IP 比例达到或超过阈值，将根据设定进行修改策略或添加例外操作。

步骤 2 调整策略选项。

选择策略类型后，设置该类型策略分析到误报后的自动调整方案：优先修改策略或优先添加例外。

- 优先修改策略：当策略触发了误报且满足修改策略条件，将优先修改策略。

  根据分析结果的告警原因修改策略，可修改策略参数或取消某检测项。

  修改策略的具体方式为复制当前策略，修改参数或取消某检测项后，再应用修改后的策略。

  当所有检测项都取消后，调整方式为“取消策略”。
- 优先添加例外：当策略触发了误报且满足添加例外条件，将优先将其添加到例外策略。

  添加例外包括：添加例外策略和添加例外规则。

  - 添加例外策略：对整个策略添加例外；
  - 添加例外规则：对该策略中的某个规则添加例外。

  算法型策略只能使用前者，规则型策略可以两者都使用（详细情况请参见分析结果中“手动添加例外”的说明）。

说明	• 若某策略分析到误报，且该类策略设置优先修改策略，但告警原因分析或规则分析不满足修改策略条件，此时 WAF 将进行添加例外的条件检查，若满足添加例外条件，WAF 将进行添加例外操作。 • 反之，若某策略分析到误报，且该策略设置优先添加例外，但 URL 分析不满足添加例外条件，此时 WAF 将进行修改策略的条件检查，若满足修改策略条件，WAF 将进行修改策略操作。

步骤 3 单击【保存】按钮，保存自动调整配置。

----结束

查看误报分析结果

WAF 进行误报分析后，无论是手动分析还是自动分析，都将生成误报分析结果，这些分析结果将集中展示在误报分析结果页签中。

在站点组树图中单击某一站点组，在右侧该站点组管理页面中选择“误报分析结果”页签，进入误报分析结果管理界面，如图 4-39 所示。

图 4-38 **误报分析结果**

查看分析结果

在分析结果列表的操作栏中，单击图标，查看分析结果详情，如图 4-40 所示。

图 4-39 分析结果详情

在分析结果详情中单击“类型”前的⊞/⊟，可一键展开或一键收起站点/站点组/虚拟站点的策略名、告警原因分析/URL 分析/规则分析；

在分析结果详情中单击站点/站点组/虚拟站点前的⊞/⊟，可依次展开站点/站点组/虚拟站点的策略名、告警原因分析/URL 分析/规则分析。

- 单击策略名后的策略名称蓝色链接，查看策略详情；
- 单击告警原因分析/规则分析后的图标，可以手动修改策略；
- 单击 URL 分析/规则分析后的图标，可以手动添加例外。
  - URL 分析的“添加例外”是对整个策略添加例外；
  - 规则分析的“添加例外”是对该策略中的某个规则添加例外。

查看调整详情

在如图 4-39 所示的分析结果列表的自动调整栏中，单击蓝色链接文字“详情”，查看调整详情，包括防护对象、调整方式、策略类型、原策略、新策略/例外策略、调整内容、调整状态，如图 4-41 所示。

图 4-40 调整详情

防护对象	调整方式	策略类型	原策略	新策略/例外策略	调整内容	调整状态
虚拟站点 :default	修改策略	Web通用防护	default_medium	Add_by_false_alarm_analyse_2359299	取消规则: 18612240	调整成功
站点组 :default	例外策略	HTTP访问控制	站点组-HTTP访问控制	Add_by_false_alarm_analyse_4718593	例外URL: 10.67.10.220:82/py/	调整成功
站点 :default_v4	修改策略	内置协议校验	内置协议校验		URI报文过长: 不检测 HTTP请求头部过长: 不检测 HTTP版本字段不合规: 不检测 HTTP 0.9未知的请求方法: 不检测 多余的请求头部: 不检测	调整成功

删除分析结果

在分析结果列表的操作栏中，单击图标，在弹出的确认删除对话框中单击【确定】按钮，删除相应的分析结果。

4.3.2.5 删除站点

单击站点组树图中的根目录“root”，进入站点组列表页面，或者单击站点组树图中的某一站点组，进入该站点组管理页面，均可对站点进行删除操作。

单击某站点相应的图标，弹出确认删除对话框，单击【确定】按钮，删除该站点。

4.3.3 管理虚拟站点

管理员可以对虚拟站点进行如下操作：

- 新建虚拟站点
- 启用/停用虚拟站点
- 配置虚拟站点
- 删除虚拟站点
- 批量操作

4.3.3.1 新建虚拟站点

步骤 1 在站点组树图中，鼠标移动到某个站点组时，显示新建虚拟站点图标，单击该图标，弹出新建虚拟站点对话框。

串联/旁路模式下新建虚拟站点对话框如图 4-42 所示，反向代理模式下新建虚拟站点对话框如图 4-43 所示。

图 4-41 新建虚拟站点 – 串联/旁路模式

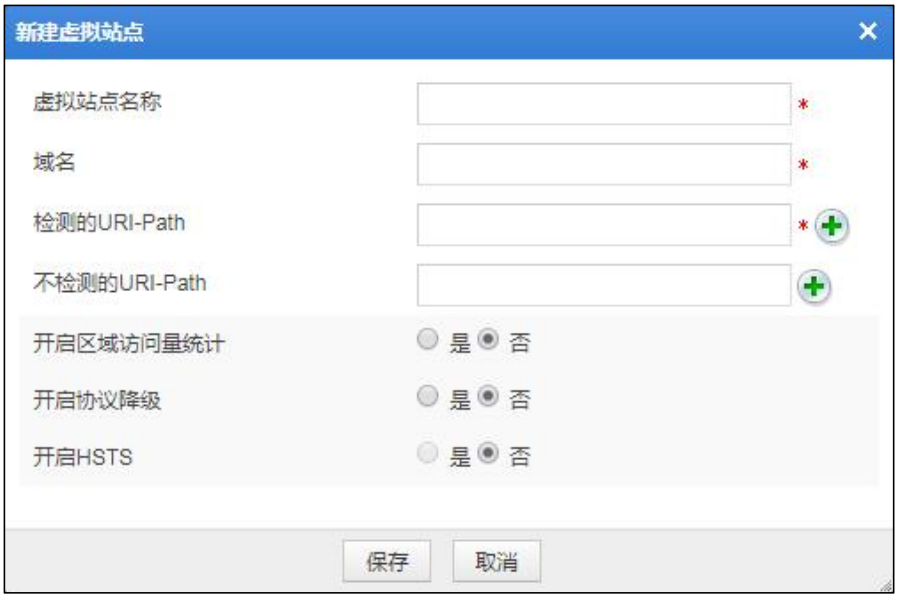
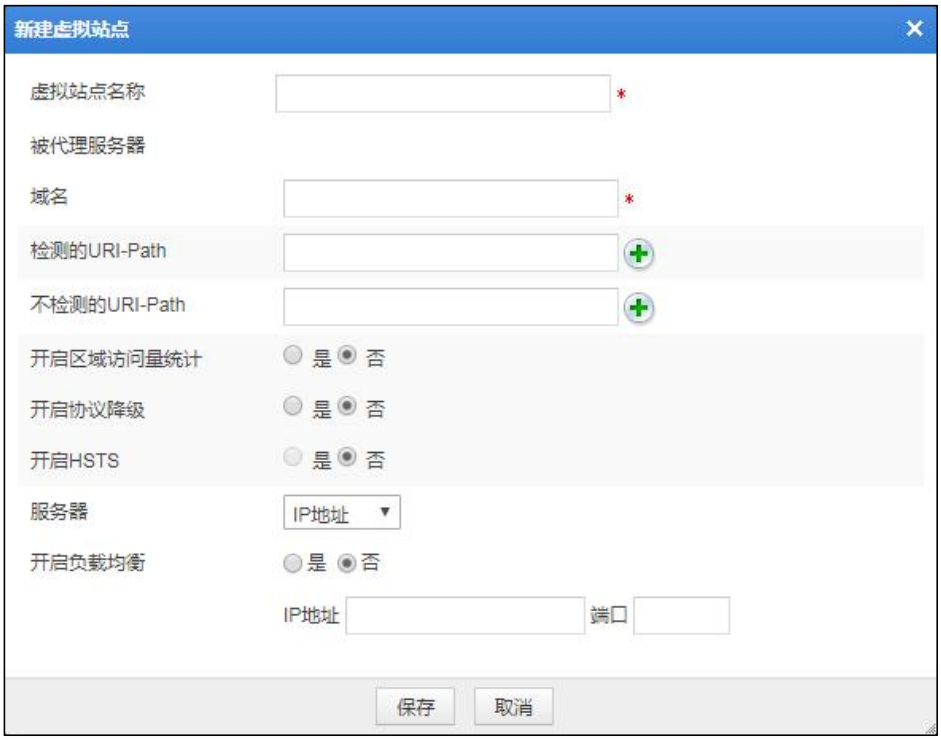


图 4-42 新建虚拟站点 – 反向代理模式



步骤 2 配置虚拟站点参数，参数说明如表 4-14 所示。

表 4-13 虚拟站点参数说明

配置项	描述
虚拟站点名称	虚拟站点的名称。
域名	虚拟站点的域名。
检测的 URI-Path	进行检测的 URL 地址。
不检测的 URI-Path	不进行检测的 URL 地址。
开启区域访问量	虚拟站点是否开启区域访问量统计功能。
开启协议降级	虚拟站点是否开启协议降级功能。 开启后，将 HTTP 的长连接变为短连接。
开启 HSTS	防护站点是否开启 HSTS（HTTP Strict Transport Security）。 开启 HSTS，max-age 为必配参数，表示 HSTS Header 的过期时间，首次访问该站点时，手动在 URL 栏中输入 https://*IPor 域名*，强制使用 HTTPS 协议访问目标网站，第二次访问如果在 max-age 配置的时间范围内，则可不用输入 https，直接输入站点 IP 或域名，浏览器将自动使用 HTTPS 协议访问目标网站，且浏览器的 HSTS Header 时间自动刷新为 max-age 配置的时间，重新开始计时；若第二次访问超过 max-age 配置的时间范围，则需手动输入 https，浏览器不会自发使用 HTTPS 协议访问站点。 若当前域名未加入入 Google 发起的 Preload List，为保证 HSTS 功能生效，服务器需要提供将 HTTP 协议重定向到 HTTPS 协议的跳转功能。可在 WAF 上配置相同 IP 段的 HTTP 协议站点，并配置数据安全传输策略，即可实现 http 重定向到 https 的功能。

配置项	描述
	说明 • 国内版 WAF 默认关闭，表示透传服务器响应报文中的 HSTS 字段。 • 国际版 WAF 默认开启，表示采用 WAF 上配置的 HSTS 响应头字段。
max-age	开启 HSTS 后必需配置该参数。 HSTS Header 在浏览器中的缓存时间。 初次开启时，建议设置较短时间。 说明 因为 HSTS Header 存在于每个 HTTPS 协议的响应中，随着用户和网站的交互，该有效时间在随时刷新。例：max-age 设置为 180s，第一次手动输入 https://*IPor 域名*访问 https 网站，120s 后再次访问，访问前浏览器计时剩余 60s，访问后计时被重置成 180s。
includeSubDomain	仅开启 HSTS 后可配置该参数。 是否包含子域名。 开启后，需确保当前域名的所有子域名都已支持 HTTPS 协议，否则会导致访问不通。
preload	仅开启 HSTS 后可配置该参数。 是否申请将该域名加入 Google 发起的 Preload List。 开启即表示申请加入。申请加入 Preload List 需满足以下条件： • max-age 不得少于 18 周（126 天） • 必须开启 includeSubDomains 字段 • 必须开启 preload 字段但 Google 不会判定申请人的合法性，请谨慎开启此字段。
服务器	仅当反向代理部署模式下新建虚拟站点时需要配置。 • 选择 **IP 地址**：需要输入被代理服务器的 IP 地址和端口号，同时可选择是否开启负载均衡。其中 IP 地址支持 Ipv4 和 Ipv6。 • 选择**真实域名**：需要被代理服务器的真实域名和端口号，并单击【获取 IP 地址】，获取服务器的 IP，其中 IP 地址支持 Ipv4 和 Ipv6。
开启负载均衡	是否开启负载均衡功能，仅当反向代理部署模式下新建虚拟站点时需要配置。 开启负载均衡后，还需要配置负载均衡组中其他 WAF 设备的 IP 地址及端口。
高级选项	若站点组中有服务器类型为 HTTPS 的站点，还可以为虚拟站点配置以下高级选项： • 证书文件：证书文件的导入方法，可选方式有**选择已有证书**和**上传证书**； • 选择已有证书：选择已有的证书文件； • SSL 版本支持：WAF 支持的 SSL 版本； • 加密算法：默认为**客户端**。

步骤 3 单击【保存】按钮，保存配置。

----结束

4.3.3.2 启用/停用虚拟站点

新建的虚拟站点默认为启用状态。

单击站点组树图中的根目录“root”，进入站点组列表页面，或者单击站点组树图中的某一站点组，进入该站点组管理页面，均可对虚拟站点进行启用/停用操作。

- 单击某个未启用虚拟站点“操作”栏中的图标，对应虚拟站点状态变为，表示该虚拟站点已启用。
- 单击某个已启用虚拟站点“操作”栏中的图标，对应虚拟站点状态变为，表示该虚拟站点已停用。

4.3.3.3 配置虚拟站点

在站点组树图中，单击某一虚拟站点，进入虚拟站点配置页面，串联/旁路模式下配置虚拟站点页面如图 4-44 所示，反向代理模式下配置虚拟站点页面如图 4-45 所示。

图 4-43 虚拟站点配置 – 串联/旁路模式

图 4-44 虚拟站点配置 – 反向代理模式

编辑虚拟站点参数

在图 4-44、图 4-45 中编辑参数后单击【保存】按钮，保存配置。

配置虚拟站点策略

在图 4-44、图 4-45 中选择“策略配置”页签，进入虚拟站点策略配置页面，如图 4-46 所示。

图 4-45 虚拟站点策略配置

配置虚拟站点的策略可以选择如下三种方式：

- 快速配置：单击【选择虚拟站点模板】，可选择默认模板和其他模板。
- 引用策略：在各类策略对应的下拉框中，一一选择相应的策略。
- 应用站点策略：在各类策略对应的“应用站点组配置的对应类型策略”的复选框中勾选，该虚拟站点自动应用所属站点组的对应策略。

配置虚拟站点后，单击【确定】按钮，完成配置。

新建策略

在图 4-46 所示页面，单击“新建策略”链接，进入新建当前策略的配置页面，新建该类型的新策略。有关新建策略的详细介绍请参见 4.7 策略管理。

导出为虚拟站点模板

在图 4-46 所示页面，单击【导出为虚拟站点模板】按钮，在弹出的如图 4-47 所示页面中输入虚拟站点模板的名称，单击【确定】，页面提示“导出成功”，表示成功导出当前策略选择的配置为虚拟站点模板。导出后的模板可以在虚拟站点模板中查看和管理。有关虚拟站点模板的介绍，请参见 4.8.2 虚拟站点模板。

图 4-46 导出为虚拟站点模板

4.3.3.4 删除虚拟站点

删除虚拟站点有两种方法。

- 在站点组树图中，单击站点组前的图标⊞，显示所有站点组中的虚拟站点，鼠标移动到某个虚拟站点时，显示删除图标✖，单击该图标，并在确认删除对话框中单击【确定】按钮，删除对应的虚拟站点。
- 单击站点组树图中的根目录“root”，进入站点组列表页面，或者单击站点组树图中的某一站点组，进入该站点组管理页面，单击某虚拟站点相应的图标，弹出确认删除对话框，单击【确定】按钮，删除该虚拟站点。

4.3.3.5 批量操作

管理员可以批量对多个站点组及站点组下的虚拟站点进行批量开启/关闭区域访问量、删除、启用、停用操作。

区域访问量是指，站点资源中所有虚拟站点 IP 范围内的访问量统计数据。

开启区域访问量统计功能后，在菜单 **日志报表> 区域访问量统计报表**中可以按照区域查看区域访问量统计数据。

虚拟站点批量操作和站点批量操作一致，具体操作请参见 4.3.2.3 批量操作。

4.4 自学习策略

自学习系统，是通过学习用户对被保护站点的正常流量的数据信息，总结出站点保护对象的正常模型，并生成相应的白名单策略，加载到白名单规则引擎中对异常流量进行检测和防护。自学习策略是配置进行统计的内容。

用户可以按照站点组对自学习策略进行以下操作：

- 新建自学习策略
- 编辑自学习策略
- 删除自学习策略
- 启用自学习策略
- 停用自学习策略
- 跳转到指定站点组管理界面
- 跳转到自学习结果页面

4.4.1 新建自学习策略

新建自学习策略的具体操作如下所示：

步骤 1 选择菜单 **安全管理** > **自学习策略**，进入自学习策略配置页面，如图 4-48 所示。

图 4-47 自学习策略配置页面

步骤 2 单击自学习策略树中某一站点组后，在该站点组自学习策略管理页面中单击【新建】按钮，弹出新建自学习策略对话框；或者鼠标指向自学习策略树中某一站点组，显示图标，单击该图标，弹出新建自学习策略对话框，如图 4-49 所示。

图 4-48 新建自学习策略

步骤 3 配置自学习策略参数。

步骤 4 单击【确定】按钮，保存配置并返回到自学习策略列表界面。

----结束

4.4.2 编辑自学习策略

编辑自学习策略的具体操作如下所示：

步骤 1 在如图 4-48 所示的自学习策略树中单击某一站点组，右侧显示该站点组的站点信息以及自学习策略表，单击自学习策略表中某自学习策略相应“操作”栏中的图标；或者在自学习策略树中单击某个自学习策略，都可以编辑该自学习策略的参数，编辑页面如图 4-50 所示。

图 4-49 编辑自学习策略

步骤 2 编辑自学习策略参数。

步骤 3 单击【确定】按钮，完成编辑保存配置，返回自学习策略列表界面。

在编辑过程中，单击【重置】，自学习策略配置页面的参数即可自动返回上一次保存的修改状态。

----结束

4.4.3 删除自学习策略

启用中的自学习策略不能删除，请在删除自学习策略前停用该策略。不同自学习策略组的自学习策略不能同时删除。

用户可以删除单个自学习策略，也可以批量删除同一站点组下的多个自学习策略。具体有如下三种方法：

- 在图 4-48 所示界面中，单击某个自学习策略“操作”栏中的图标，进入删除确认窗口，然后单击该窗口中的【确定】按钮，删除该自学习策略。
- 在图 4-48 所示界面中，单击自学习策略树中某一站点组下的一个或多个自学习策略左侧的复选框，然后单击该自学习策略组列表右下方的【删除】按钮，进入删除确认窗口，单击该窗口中的【确定】按钮，删除被选中的自学习策略。
- 在图 4-48 所示界面中，鼠标指向自学习策略树中某个站点组下的自学习策略，显示删除图标，单击该图标，删除对应站点下的自学习策略。

4.4.4 启用自学习策略

新建的自学习策略默认为启用状态。当自学习策略被停用时，自学习策略状态显示为 ；此时需要启用后，才能继续使用。

用户可以启用单个自学习策略，也可以批量启用同一站点组内的多个自学习策略。不同自学习策略组的自学习策略不能同时启用。具体有如下三种方法：

- 在图 4-48 所示界面中，单击某个自学习策略“操作”栏中的图标 ，对应自学习策略状态变为 ，表示该自学习策略已启用。
- 在图 4-48 所示界面中，单击某一站点组下的一个或多个自学习策略左侧的复选框，然后单击该站点组列表右下方的【启用】按钮，对应自学习策略状态为 ，表示该自学习策略已启用。
- 在图 4-48 所示界面中，鼠标指向自学习策略树中某个站点组下的自学习策略，显示图标 ，单击该图标，启用对应站点下的自学习策略。

4.4.5 停用自学习策略

用户可以停用单个自学习策略，也可以批量停用同一站点组内的多个自学习策略。不同站点组的自学习策略不能同时停用。具体有如下三种方法：

- 在图 4-48 所示界面中，单击某个自学习策略“操作”栏中的图标 ，对应自学习策略状态变为 ，表示该自学习策略已停用。
- 在图 4-48 所示界面中，单击某一站点组下的一个或多个自学习策略左侧的复选框，然后单击该站点组列表右下方的【停用】按钮，对应自学习策略状态为 ，表示该自学习策略已停用。
- 在图 4-48 所示界面中，鼠标指向自学习策略树中某个站点组下的自学习策略，显示图标 ，单击该图标，停用对应站点下的自学习策略。

4.4.6 其他操作

用户还可以对自学习策略进行以下操作：

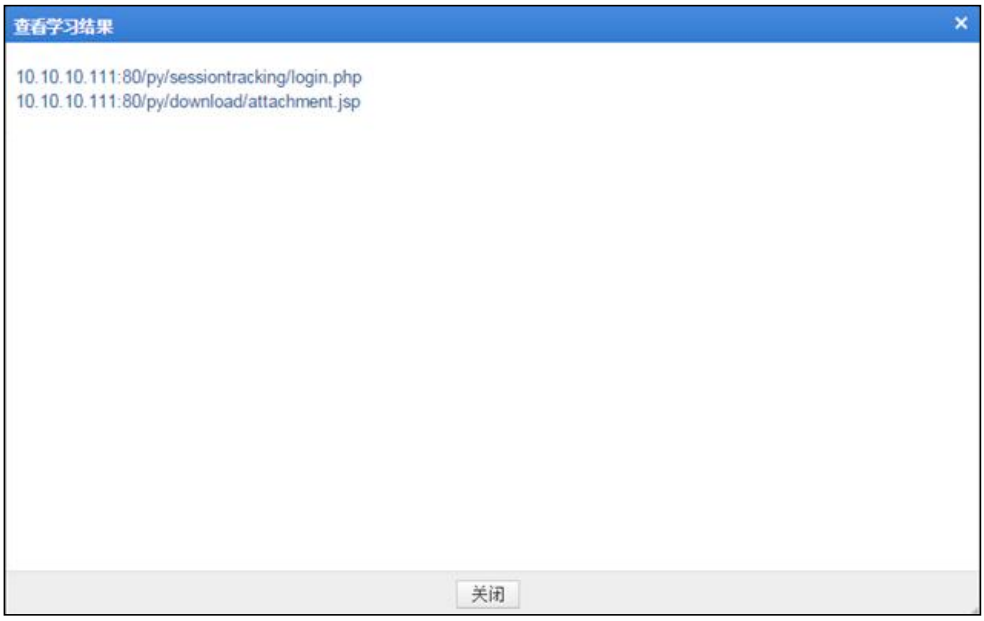
- 跳转到指定站点组管理界面

  在如图 4-48 所示的自学习策略树中单击某一站点组，右侧显示该站点组的站点信息以及自学习策略表，单击站点信息列表“操作”栏中的图标 并选择“组管理”，跳转到该自学习策略对应的站点组管理界面，如图 4-13 所示。

- 跳转到自学习结果链接页面

  在如图 4-48 所示的自学习策略树中单击某一站点组，右侧显示该站点组的站点信息以及自学习策略表，单击站点信息列表“操作”栏中的图标 并选择“自学习结果”，跳转到该自学习策略对应的站点的自学习结果链接界面，如图 4-51 所示。单击图中链接，即可打开对应的自学习结果。

图 4-50 跳转到自学习结果链接页面



4.5 自学习结果

选择菜单 **安全管理** > **自学习结果**，进入查看自学习结果页面，如图 4-52 所示。在左侧的站点组树图中，展开某站点组，图标为“”即为该站点组下自学习策略的学习结果。

图 4-51 查看自学习结果

4.6 规则库管理

在配置策略时，需要选择使用的规则。WAF 规则库分为系统内置的通用防护规则库和用户可以自定义的特征库。

4.6.1 查询通用防护规则

通用防护规则是系统内置的规则集，用户无编辑权限，只能查看相应的规则详情。

步骤 1 选择菜单 **安全管理** > **规则库管理** > **通用防护** > **Web 服务器漏洞**，进入 Web 服务器漏洞规则列表，右侧规则列表为该类型下的规则集合，如图 4-53 所示。

图 4-52 Web 服务器漏洞规则

步骤 2 设置规则查询条件，条件说明如表 4-15 所示。

表 4-14 查询规则参数说明

配置项	描述
ID	规则的 ID 号码。
名称	规则的名称。
描述	描述规则信息的关键字。
危险等级	规则的危险级别，分为**高**、**中**、**低**三种级别，**未选择**表示不对规则的危险级别进行限制。
准确度	规则的准确度级别，分为**高**、**中**、**低**三种级别，**未选择**表示不对规则的准确度级别进行限制。

步骤 3 单击【查询】按钮，查看符合条件的规则。

步骤 4 单击规则列表右侧的“操作”栏中的图标，打开某条规则的详细信息，如图 4-54 所示。

图 4-53 Web 服务器漏洞规则详情

----结束

4.6.2 配置自定义特征库

WAF 内置的防护规则，都是针对已知漏洞的防护；而 Web 应用通常是定制化的，完全通过内置规则的防护往往不够有效。此时，用户可以自定义特征规则，并在策略中引用该条规则，使之生效。

自定义特征规则的告警类型分为其他多种类型（如 Web 服务器漏洞、Web 插件漏洞等等）和自定义类型。新建策略引用自定义特征规则时，自定义特征规则的告警类型决定了可被引用的情况：

- 自定义特征规则的告警类型为**自定义**时，仅可在新建自定义策略时引用该自定义特征规则；
- 自定义特征规则的告警类型为**其他多种类型**时，不仅可以在新建自定义策略时引用，创建其他类型策略时也可引用该自定义特征规则。

4.6.2.1 新建自定义特征

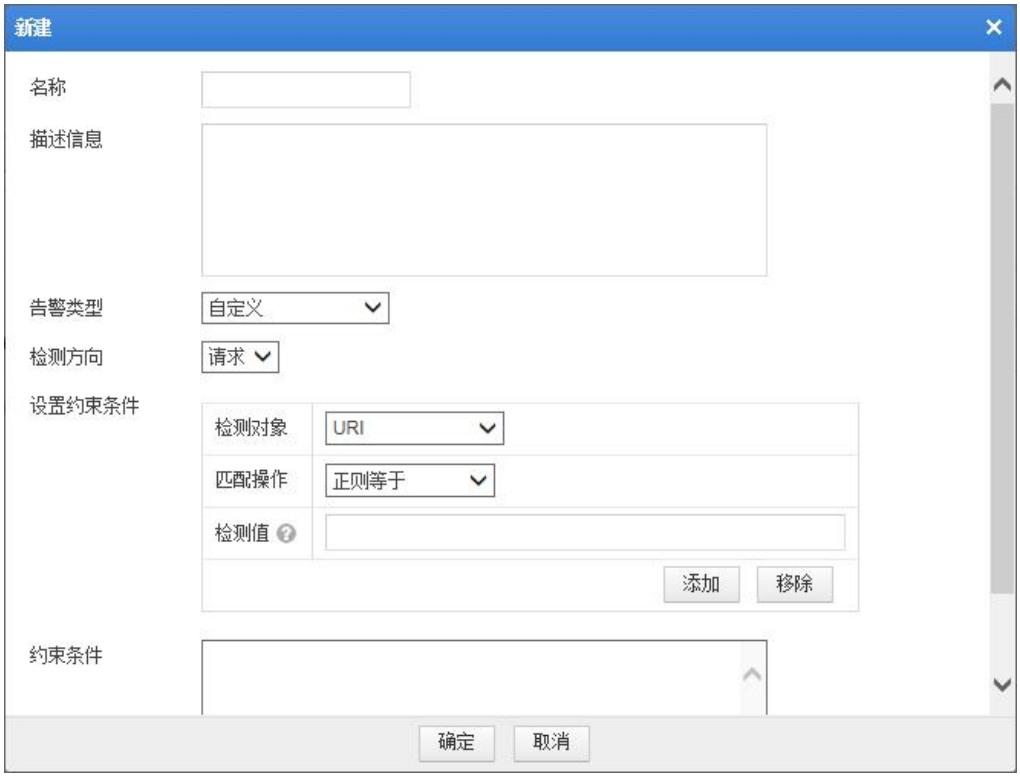
新建自定义规则的具体操作如下：

步骤 1 选择菜单 **安全管理** > **规则库管理** > **自定义特征** > **自定义**，进入自定义规则列表，如图 4-55 所示。

图 4-54 自定义规则列表

步骤 2 单击【新建】按钮，弹出新建自定义规则对话框，如图 4-56 所示。

图 4-55 新建自定义规则



步骤 3 参数配置完成后，单击【确定】按钮保存配置。

----结束

4.6.2.2 编辑自定义规则

自定义规则配置完成后，管理员可以重新编辑其参数，具体操作如下所示：

步骤 1 在图 4-55 所示自定义规则列表中，单击某个自定义规则“操作”栏中的图标，重新编辑该自定义规则的参数。

步骤 2 编辑完成后，单击【确定】按钮，保存配置并返回到自定义规则列表界面。

----结束

4.6.2.3 删除自定义规则

WAF 支持删除单条自定义规则。

在图 4-55 所示自定义规则列表中，单击某条自定义规则“操作”栏中的图标，进入删除确认窗口，然后单击该窗口中的【确定】按钮，即可删除该自定义规则。

4.7 策略管理

WAF 提供多种策略来防护网络常见的 Web 攻击。策略只有被站点组加载后，才能生效。同一个策略可以被多个站点组加载。

WAF 为用户提供如下 5 类配置策略：

- 协议校验：提供 HTTP 协议校验。
- 基础防护：一般网络环境中常见的防护策略。
- 高级防护：需要根据具体的网络环境选择的配置策略。
- 精准防护：根据自学习策略的学习结果进行的更精确的防护策略。
- 其他防护：需要根据用户的实际情况自定义配置策略、例外策略和风险级别策略。

在本节中，介绍了所有策略的新建、编辑、复制和删除操作。而策略管理也可以通过站点防护进行新建或编辑，相关介绍请参见配置数据安全传输策略。

此外，系统在部分策略中还提供默认的策略，如 default_low，default_medium 和 default_high。每类策略可能包含一个或多个默认策略，默认策略不能被删除、修改，但是可以被复制后另存为新的策略。

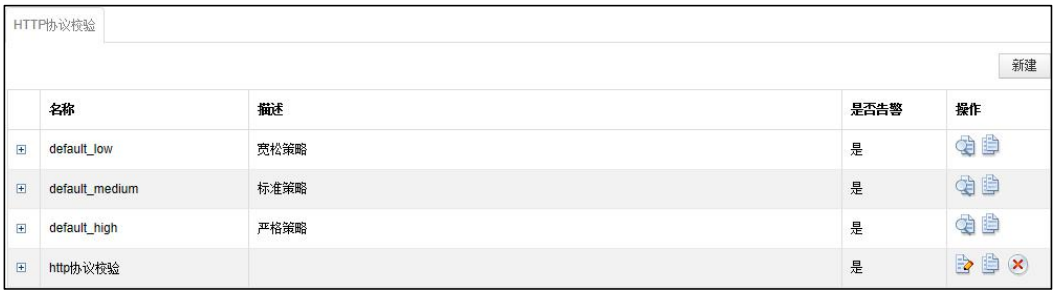
4.7.1 协议校验

HTTP 是超文本传输协议（Hypertext Transfer Protocol）的简称。它用来在 Internet 上传递 Web 页面信息。如果大量畸形的 HTTP 协议数据包攻击服务器，会影响服务器对正常请求的反应速度，严重的会造成服务器缓冲区溢出或者服务器瘫痪。配置 HTTP 协议校验后，WAF 会阻断不符合协议校验策略检查项的 HTTP 访问。

4.7.1.1 新建 HTTP 协议校验策略

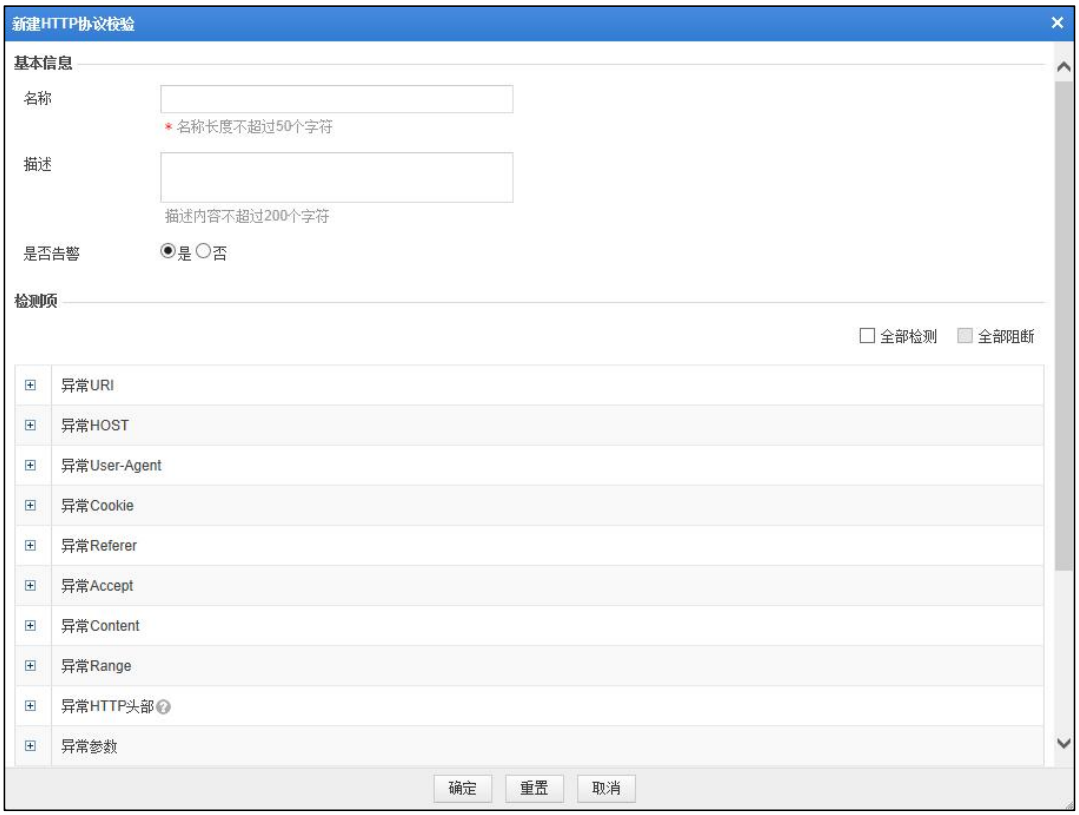
步骤 1 选择菜单 **安全管理** > **策略管理** > **协议校验** > **HTTP 协议校验**，进入 HTTP 协议校验策略列表，如图 4-57 所示。

图 4-56 HTTP 协议校验策略列表



步骤 2 单击【新建】按钮，弹出新建 HTTP 协议校验策略对话框，如图 4-58 所示。

图 4-57 HTTP 协议校验策略配置



步骤 3 配置 HTTP 协议校验策略参数，参数详细信息如表 4-16 所示。

表 4-15 添加 HTTP 协议校验策略参数信息

配置项	描述
名称	HTTP 协议校验策略的名称。
描述	HTTP 协议校验策略的描述说明。
是否告警	是否产生告警日志。
检测项	设置 Http 协议包头各字段的参数值、异常参数或异常编码。

配置项	描述
	除“异常 HTTP 头部”中的**禁止重复 HTTP 头部**之外，新建的每条检测项默认都是进行检测的，如果勾选页面右上角的全部检测，此时所有的检测项仍然是全部检测的状态，若再次取消勾选，则全部检测项都不进行检测。 除“异常 HTTP 头部”中的**禁止重复 HTTP 头部**之外，新建的每条检测项默认都是进行阻断的，如果勾选页面右上角的全部阻断，此时所有的检测项仍然是全部阻断的状态，若再次取消勾选，则全部检测项的动作都为接受。
HTTP 解码控制	WAF 在进行 HTTP 解码时，是否清除异常符号“%”或空字符。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.1.2 编辑 HTTP 协议校验策略

HTTP 协议校验策略配置完成后，管理员可以重新编辑其参数，具体操作如下所示：

步骤 1 在图 4-57 所示 HTTP 协议校验策略列表中，单击某个 HTTP 协议校验策略“操作”栏中的图标，编辑该 HTTP 协议校验策略的参数。

步骤 2 编辑完成后，单击【确定】按钮，保存配置并返回到 HTTP 协议校验策略列表界面。

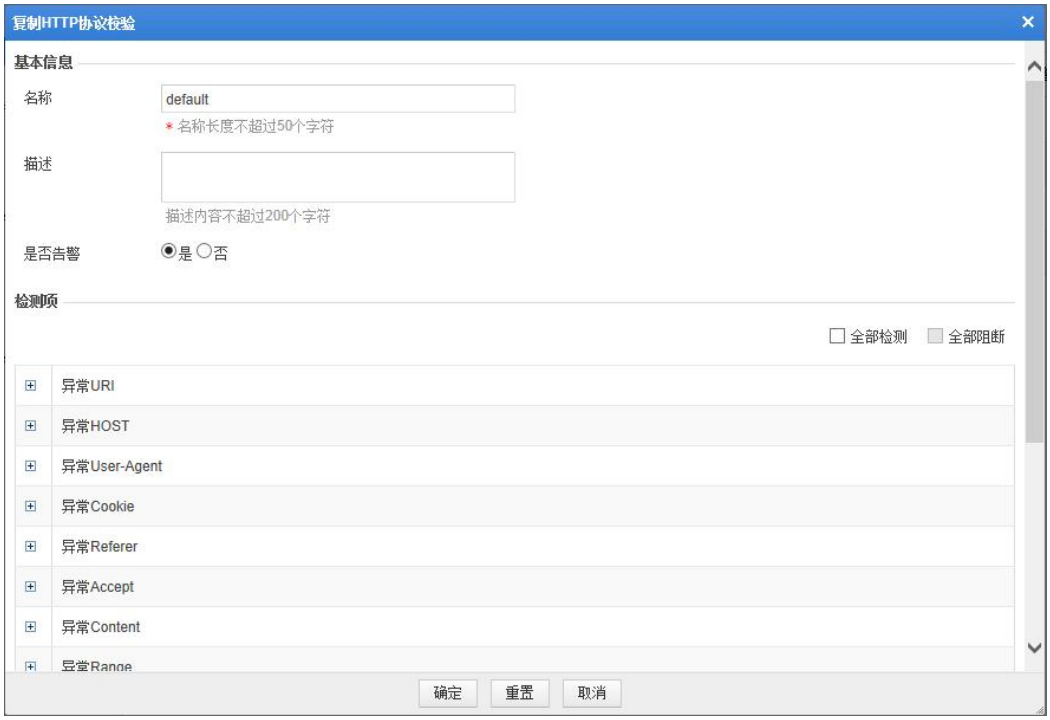
----结束

4.7.1.3 复制 HTTP 协议校验策略

当需要新的 HTTP 协议校验策略时，管理员除了新建策略之外，还可以利用复制功能，将已有的策略复制，在此基础上进行参数修改后另存为新的策略。具体操作如下所示：

步骤 1 在图 4-57 所示 HTTP 协议校验策略列表中，单击某条 HTTP 协议校验策略“操作”栏中的图标，弹出复制 HTTP 协议校验策略对话框，如图 4-59 所示。

图 4-58 复制 HTTP 协议校验策略



步骤 2 修改参数。

根据实际需要修改 HTTP 协议校验策略参数，参数说明如表 4-16 所示。

步骤 3 单击【确定】按钮，保存为新的策略。

----结束

4.7.1.4 删除 HTTP 协议校验策略

WAF 支持删除单条 HTTP 协议校验策略。

在图 4-57 所示 HTTP 协议校验策略列表中，单击某条 HTTP 协议校验策略“操作”栏中的图标，进入删除确认窗口，然后单击该窗口中的【确定】按钮，即可删除该 HTTP 协议校验策略。

4.7.2 基础防护

基础防护是指网络环境中常见的防护策略，分为以下几类：

- Web 服务器/插件防护
- HTTP 访问控制
- 爬虫防护
- Web 通用防护
- 文件非法上传防护
- 非法下载限制

- 信息泄露防护

4.7.2.1 配置 Web 服务器/插件防护策略

Web 服务器/插件是指 Web 服务器以及运行在服务器上的业务逻辑。Web 服务器/插件防护针对已有的服务器漏洞和业务处理逻辑漏洞设置的规则，主要检测非法请求以及非法回应内容。WAF 的 Web 服务器/插件防护策略，可根据 Web 服务器和服务器上的业务处理逻辑，灵活地选择对应的防护规则。

在 Web 服务器/插件防护页面，可以进行新建、编辑、复制和删除 Web 服务器/插件防护策略的操作。下面介绍如何新建 Web 服务器/插件防护策略，有关如何编辑、复制和删除 Web 服务器/插件防护策略与对 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建 WEB 服务器/插件防护策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **基础防护** > **Web 服务器/插件防护**，进入 Web 服务器/插件防护策略列表，如图 4-60 所示。

图 4-59 Web 服务器/插件防护策略配置

步骤 2 单击【新建】按钮，弹出新建 Web 服务器/插件防护策略对话框，如图 4-61 所示。

图 4-60 新建 Web 服务器/插件防护策略

步骤 3 配置 Web 服务器/插件防护策略参数，参数详细信息如表 4-17 所示。

表 4-16 Web 服务器/插件防护策略参数信息

配置项	描述
名称	Web 服务器/插件防护策略的名称。
描述	Web 服务器/插件防护策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。

配置项	描述
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
匹配原则	匹配原则有两种： • 匹配中即结束，是匹配一条规则后就不进行后续规则的匹配； • 匹配中仍继续，是匹配一条规则后仍要进行策略中后续规则的匹配。
规则筛选	根据规则类型、ID、危险等级、操作系统、Web 服务器、名称、准确度、数据库、编程语言其中的一项或多项过滤条件，对规则列表进行筛选。单击图 4-61 所示页面的【筛选】按钮后，下方的规则列表将显示根据指定条件过滤后的规则列表。
规则列表	默认显示全部规则，当进行规则筛选后，仅显示指定条件的规则列表。 至少选择一个规则。要将某个规则加入规则集，只需勾选规则对应的复选框。

步骤 4 单击【确定】按钮保存配置。

----结束

4.7.2.2 配置 HTTP 访问控制策略

HTTP 访问控制策略是指对来自客户端的 HTTP 请求协议进行检测，根据配置的动作对不满足条件的数据包进行相应的处理。在一个“站点”中，用户可以配置多条 HTTP 访问控制策略。这些策略根据界面所展示的顺序被依次匹配，只要其中一条策略被匹配，则不会继续匹配后续的策略。

在 HTTP 访问控制策略页面，可以进行新建、编辑、复制和删除 HTTP 访问控制策略的操作。下面介绍如何新建 HTTP 访问控制策略，有关如何编辑、复制和删除 HTTP 访问控制策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

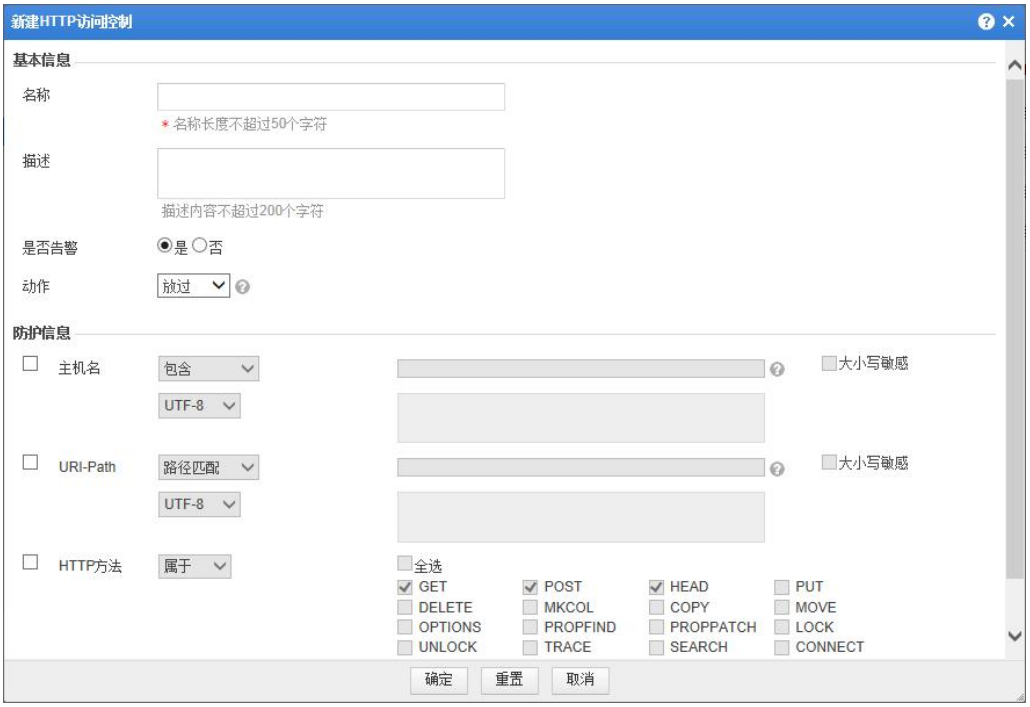
新建 HTTP 访问控制策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **基础防护** > **HTTP 访问控制**，进入 HTTP 访问控制策略列表，如图 4-62 所示。

图 4-61 HTTP 访问控制策略列表

步骤 2 单击【新建】按钮，弹出新建 HTTP 访问控制策略对话框，如图 4-63 所示面。

图 4-62 新建 HTTP 访问控制策略



步骤 3 配置 HTTP 访问控制策略参数，参数详细信息如表 4-18 所示。

表 4-17 HTTP 访问控制策略参数信息

配置项	描述
名称	HTTP 访问控制策略的名称。
描述	HTTP 访问控制策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。

配置项	描述
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
防护信息	HTTP 访问控制策略通过主机名、URI-Path、HTTP 方法以及客户端 IP 等多个条件实现对 HTTP 请求的组合控制。在策略中若选择多个条件，则表示这些条件必须同时匹配才能触发策略；若不选择任何条件则表示任意条件均匹配策略。关于配置参数的详情请参见界面在线帮助的介绍。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.2.3 配置爬虫防护策略

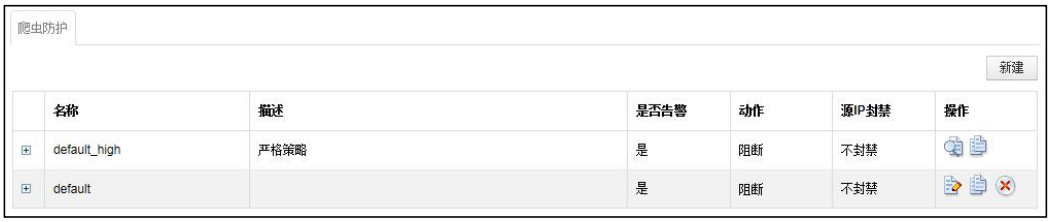
网络爬虫，是一种按照一定的规则，自动抓取万维网信息的程序或者脚本。网络上有很多搜索引擎，如百度，雅虎等，都使用爬虫提供最新的数据。但如果恶意使用爬虫爬取大量的网站页面，不但占用网站带宽，而且影响服务器性能，WAF 通过设置该策略，可以防止信息被搜索引擎获取。

在爬虫防护策略页面，可以进行新建、编辑、复制和删除爬虫防护策略的操作。下面介绍如何新建爬虫防护策略，有关如何编辑、复制和删除爬虫防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建爬虫防护策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **基础防护** > **爬虫防护**，进入爬虫防护策略列表，如图 4-64 所示。

图 4-63 爬虫防护策略配置



步骤 2 单击【新建】按钮，弹出新建爬虫防护策略对话框，如图 4-65 所示。

图 4-64 新建爬虫防护策略

步骤 3 配置爬虫防护策略参数，参数详细信息如表 4-19 所示。

表 4-18 爬虫防护策略参数信息

配置项	描述
名称	爬虫防护策略的名称。
描述	爬虫防护策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。

配置项	描述
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
匹配原则	匹配原则有两种： • 匹配中即结束，是匹配一条规则后就不进行后续规则的匹配； • 匹配中仍继续，是匹配一条规则后仍要进行策略中后续规则的匹配。
规则筛选	根据规则类型、ID、危险等级、名称和准确度中的一项或多项过滤条件，对规则列表进行筛选。单击图 4-65 所示页面的【筛选】按钮后，下方的规则列表将显示根据指定条件过滤后的规则列表。
规则列表	默认显示全部规则，当进行规则筛选后，仅显示指定条件的规则列表。 至少选择一个规则。要将某个规则加入规则集，只需勾选规则对应的复选框。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.2.4 配置 Web 通用防护策略

WEB 通用防护策略主要针对：SQL（Structured Query Language）注入防护、命令行注入攻击防护和跨站脚本攻击防护等几类防护。

SQL 注入，是指通过把 SQL 命令作为数据的一部分提交到服务器，并最终达到欺骗服务器执行这些 SQL 命令的过程。SQL 注入产生的原因往往是因为服务器的代码本身存在的缺陷，例如当服务器的应用程序未经校验而直接使用客户端提交的数据来构造动态 SQL 语句以访问数据库时，就会可能发生 SQL 注入攻击。

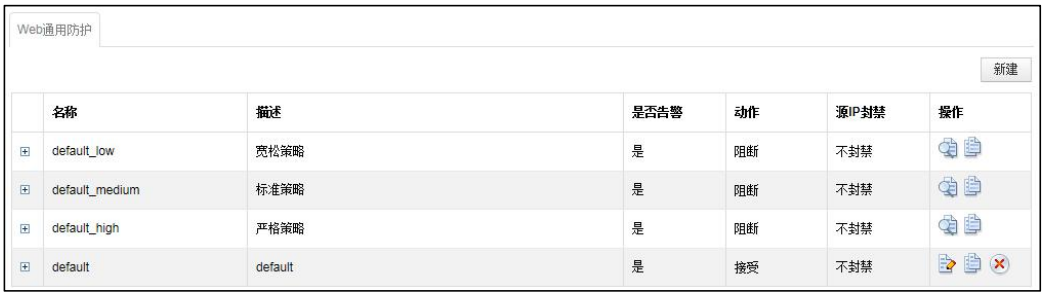
跨站脚本攻击，也称 XSS/CSS(Cross Site Scripting)，是指利用网站漏洞从用户那里恶意盗取信息。用户在浏览网站、使用即时通讯软件、甚至在阅读电子邮件时，通常会单击其中的链接。攻击者通过在链接中插入恶意代码，就能够盗取用户信息。

在 Web 通用防护策略页面，可以进行新建、编辑、复制和删除 Web 通用防护策略的操作。下面介绍如何新建 Web 通用防护策略，有关如何编辑、复制和删除 Web 通用防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建 Web 通用防护策略步骤如下：

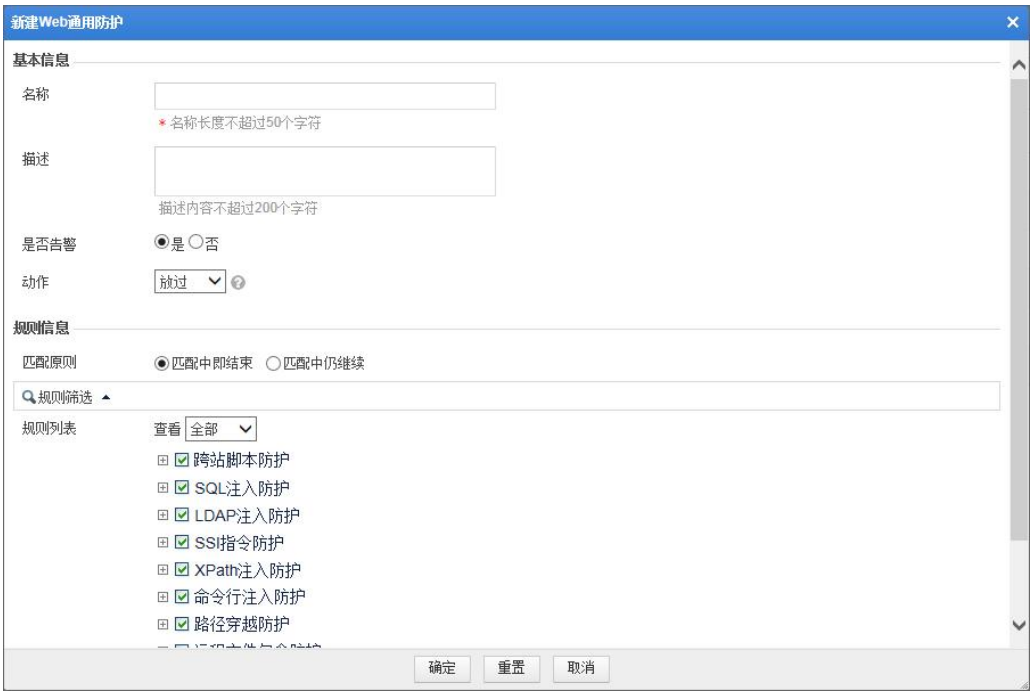
步骤 1 选择菜单 **安全管理** > **策略管理** > **基础防护** > **Web 通用防护**，进入 Web 通用防护策略列表，如图 4-66 所示。

图 4-65 Web 通用防护策略配置



步骤 2 单击【新建】按钮，弹出新建 Web 通用防护对话框，如图 4-67 所示。

图 4-66 新建 Web 通用防护策略



步骤 3 配置 Web 通用防护策略参数，参数详细信息如表 4-20 所示。

表 4-19 Web 通用防护策略参数信息

配置项	描述
名称	Web 通用防护策略的名称。
描述	Web 通用防护策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它

配置项	描述
	安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
匹配原则	匹配原则有两种： • 匹配中即结束，是匹配一条规则后就不进行后续规则的匹配； • 匹配中仍继续，是匹配一条规则后仍要进行策略中后续规则的匹配。
规则筛选	根据规则类型、ID、危险等级、操作系统、Web 服务器、名称、准确度、数据库、编程语言中的一项或多项过滤条件，对规则列表进行筛选。单击图 4-67 所示页面的【筛选】按钮后，下方的规则列表将显示根据指定条件过滤后的规则列表。
规则列表	默认显示全部规则，当进行规则筛选后，仅显示指定条件的规则列表。 至少选择一个规则。要将某个规则加入规则集，只需勾选规则对应的复选框。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.2.5 配置文件非法上传防护策略

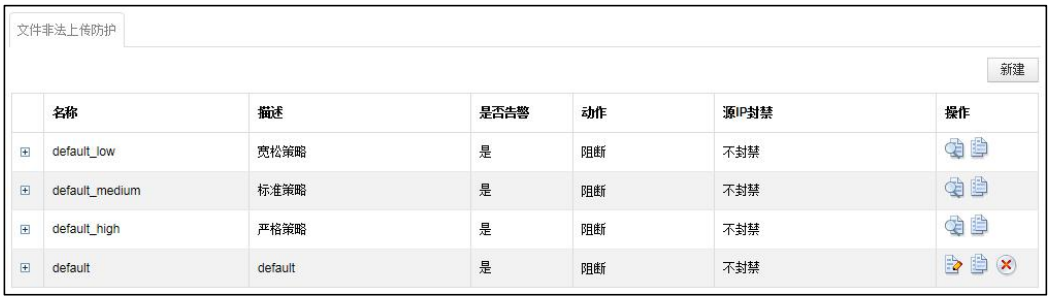
当客户端用户向服务器上传数据时，WAF 可以对上传的文件类型进行防护，当有非法上传策略中配置的文件类型上传时，WAF 会根据策略中配置的动作允许或阻断该数据的上传，并记录告警日志。

在文件非法上传防护策略页面，可以进行新建、编辑、复制和删除文件非法上传防护策略的操作。下面介绍如何新建文件非法上传防护策略，有关如何编辑、复制和删除文件非法上传防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建文件非法上传防护策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **基础防护** > **文件非法上传防护**，进入文件非法上传防护策略列表，如图 4-68 所示。

图 4-67 文件非法上传防护策略配置



步骤 2 单击【新建】按钮，弹出新建文件非法上传防护策略对话框，如图 4-69 所示。

图 4-68 新建文件非法上传防护策略

步骤 3 配置文件非法上传防护策略参数，参数详细信息如表 4-21 所示。

表 4-20 文件非法上传防护策略参数信息

配置项	描述
名称	文件非法上传防护策略的名称。

配置项	描述
描述	文件非法上传防护策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
输入文件扩展名	支持用户自定义输入待检测的文件扩展名。
Shell 类型	需要检查的上传文件类型。勾选指定文件类型后，上传该类型文件时将根据配置的策略及动作，WAF 做出相应响应。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.2.6 配置非法下载限制策略

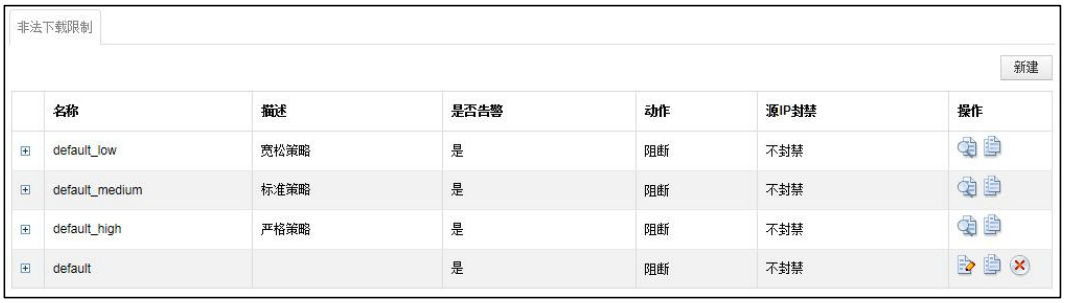
当客户端用户从服务器端下载数据时，WAF 可以对下载的文件类型进行防护，当有非法下载策略中配置的文件类型下载时，WAF 会根据策略中配置的动作允许或阻断该数据的下载，并记录告警日志。

在非法下载限制策略页面，可以进行新建、编辑、复制和删除非法下载限制策略的操作。下面介绍如何新建非法下载限制策略，有关如何编辑、复制和删除非法下载限制策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建非法下载限制策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **基础防护** > **非法下载限制**，进入非法下载限制策略列表，如图 4-70 所示。

图 4-69 非法下载限制策略配置



步骤 2 单击【新建】按钮，弹出新建非法下载限制策略对话框，如图 4-71 所示。

图 4-70 新建非法下载限制策略

步骤 3 配置非法下载限制策略参数，参数详细信息如表 4-22 所示。

表 4-21 非法下载限制策略参数信息

配置项	描述
名称	非法下载限制策略的名称。
描述	非法下载限制策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作：

配置项	描述
	• **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。 当响应码大于等于 200 小于 400 时，才会触发防护，产生安全告警事件。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
文件大小检测	是否开启文件大小检测。如需开启，勾选该项并输入文件大小，当客户端下载超过设定值的文件时，触发此条策略，WAF 根据设置的动作采取相应操作。
文件扩展名检测	是否开启扩展名检测。如需开启，勾选该项并输入文件扩展名，当客户端下载设定的扩展名文件时，触发此条策略，WAF 根据设置的动作采取相应操作。
MIME 类型检测	是否开启 MIME 类型检测。如需开启，勾选该项并选择文件的 MIME，当客户端下载设定的 MIME 类型文件时，触发此条策略，WAF 根据设置的动作采取相应操作。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.2.7 配置信息泄露防护策略

服务器对不同的客户端请求会有不同的处理结果，用不同的状态码返回给客户端。有时状态码会泄露重要的服务器信息给攻击者，使攻击者进行更有效的网络攻击。因此阻断服务器返回的状态码给客户端，是很必要的防范措施。

WAF 通过信息过滤，将敏感数据直接丢弃，防止信息泄露。

在信息泄露防护策略页面，可以进行新建、编辑、复制和删除信息泄露防护策略的操作。下面介绍如何新建信息泄露防护策略，有关如何编辑、复制和删除信息泄露防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建信息泄露防护策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **基础防护** > **信息泄露防护**，进入信息泄露防护策略列表，如图 4-72 所示。

图 4-71 信息泄露防护策略列表

步骤 2 单击【新建】按钮，弹出新建信息泄露防护策略对话框，如图 4-73 所示。

图 4-72 新建信息泄露防护策略

步骤 3 配置信息泄露防护策略参数，参数详细信息如表 4-23 所示。

表 4-22 信息泄露防护策略参数信息

配置项	描述
名称	信息泄露防护策略的名称。
是否告警	是否产生告警日志。
修改服务器名为	信息泄露的服务器名称，有助于区分被保护服务器；填写后所有 HTTP 响应的该服务器名都将被替换为所填写的内容。不填写时表示不修改服务器名称。
描述	信息泄露防护策略的描述说明。
动作	有四种类型的动作：

配置项	描述
	• **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接。 • **重定向**：对符合条件的请求，WAF 构造一个重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
响应状态	选择状态码。状态码对应信息类型的详细描述请参考表 4-24。
重定向路径/响应替换内容	如果动作选择**重定向**，需要在此处配置重定向路径。 重定向路径长度范围：1～2048。 如果动作选择**伪装**，需要在此处配置响应码及响应文件等。 如果动作选择**放过**或**阻断**，不需要配置该项。

一些常见的状态码信息如表 4-24 所示。

表 4-23 状态码信息

状态码	描述
200（成功）	服务器已成功处理了请求。通常，这表示服务器提供了请求的网页。
201（已创建）	请求成功并且服务器创建了新的资源。
202（已接受）	服务器已接受请求，但尚未处理。
203（非授权信息）	服务器已成功处理了请求，但返回的信息可能来自另一来源。
204（无内容）	服务器成功处理了请求，但没有返回任何内容。
205（重置内容）	服务器成功处理了请求，但没有返回任何内容。与 204 响应不同，此响应要求请求者重置文档视图（例如，清除表单内容以输入新内容）。
206（部分内容）	服务器成功处理了部分 GET 请求。
300（多种选择）	针对请求，服务器可执行多种操作。服务器可根据请求者 (user agent) 选择一项操作，或提供操作列表供请求者选择。
301（永久移动）	请求的网页已永久移动到新位置。服务器返回此响应（对 GET 或 HEAD 请求的响应）时，会自动将请求者转到新位置。
302（临时移动）	服务器目前从不同位置的网页响应请求，但请求者应继续使用原有位置来响应以后的请求。此代码与响应 GET 和 HEAD 请求的 301 代码类似，会自动将请求者转到不同的位置。
303（查看其他位置）	请求者应当对不同的位置使用单独的 GET 请求来检索响应时，服务器返回此代码。对于除 HEAD 之外的所有请求，服务器会自动转到其他位置。
304（未修改）	自从上次请求后，请求的网页未修改过。服务器返回此响应时，不会返回网页内容。 如果网页自请求者上次请求后再也没有更改过，您应将服务器配置为返回此响应（称为 If-Modified-Since HTTP 标头）。
305（使用代理）	请求者只能使用代理访问请求的网页。如果服务器返回此响应，还表示请求者应使用代理。

状态码	描述
307（临时重定向）	服务器目前从不同位置的网页响应请求，但请求者应继续使用原有位置来响应以后的请求。
400（错误请求）	服务器不理解请求的语法。
401（未授权）	请求要求身份验证。对于登录后请求的网页，服务器可能返回此响应。
403（禁止）	服务器拒绝请求。
404（未找到）	服务器找不到请求的网页。例如，对于服务器上不存在的网页经常会返回此代码。
405（方法禁用）	禁用请求中指定的方法。
406（不接受）	无法使用请求的内容特性响应请求的网页。
407（需要代理授权）	如果服务器返回此响应，还表示请求者应当使用代理。
408（请求超时）	服务器等候请求时发生超时。
409（冲突）	服务器在完成请求时发生冲突。服务器必须在响应中包含有关冲突的信息。服务器在响应与前一个请求相冲突的 PUT 请求时可能会返回此代码，以及两个请求的差异列表。
410（已删除）	如果请求的资源已永久删除，服务器就会返回此响应。该代码与 404（未找到）代码类似，但在资源以前存在而现在不存在的情况下，有时会用来替代 404 代码。如果资源已永久移动，您应使用 301 指定资源的新位置。
411（需要有效长度）	服务器不接受不含有效内容长度标头字段的请求。
412（未满足前提条件）	服务器未满足请求者在请求中设置的其中一个前提条件。
413（请求实体过大）	服务器无法处理请求，因为请求实体过大，超出服务器的处理能力。
414（请求的 URI 过长）	请求的 URI（通常为网址）过长，服务器无法处理。
415（不支持的媒体类型）	请求的格式不受请求页面的支持。
416（请求范围不符合要求）	如果页面无法提供请求的范围，则服务器会返回此状态码。
417（未满足期望值）	服务器未满足"期望"请求标头字段的要求。
500（服务器内部错误）	服务器遇到错误，无法完成请求。
501（尚未实施）	服务器不具备完成请求的功能。例如，服务器无法识别请求方法时可能会返回此代码。
502（错误网关）	服务器作为网关或代理，从上游服务器收到无效响应。
503（服务不可用）	服务器目前无法使用（由于超载或停机维护）。通常，这只是暂时状态。
504（网关超时）	服务器作为网关或代理，但是没有及时从上游服务器收到请求。
505（HTTP 版本不受支持）	服务器不支持请求中所用的 HTTP 协议版本。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3 高级防护

高级防护是指需要根据具体的网络环境选择的配置策略，分为以下几类：

- 盗链防护
- 跨站请求伪造防护
- 扫描防护
- Cookie 安全
- 内容过滤
- 敏感信息过滤
- 暴力破解防护
- XML 攻击防护
- 智能引擎检测

4.7.3.1 配置盗链防护策略

盗链行为通常是指在未经许可的情况下，通过内嵌代码、在线播放等手段直接引用其他内容服务提供商的资源（如图片、语音或视频等）的行为。网站盗链还可能会大量消耗被盗链网站的带宽资源（而此时被盗链网站真实的访问量可能并不大），甚至可能导致站点无法正常对外提供服务，严重损害了被盗链网站的利益。

通过 WAF 配置的盗链防护，可以有效阻止一些资源（如图片、语音、视频和软件等）在未经许可的情况下被引用。

在盗链防护策略页面，可以进行新建、编辑、复制和删除盗链防护策略的操作。下面介绍如何新建盗链防护策略，有关如何编辑、复制和删除盗链防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

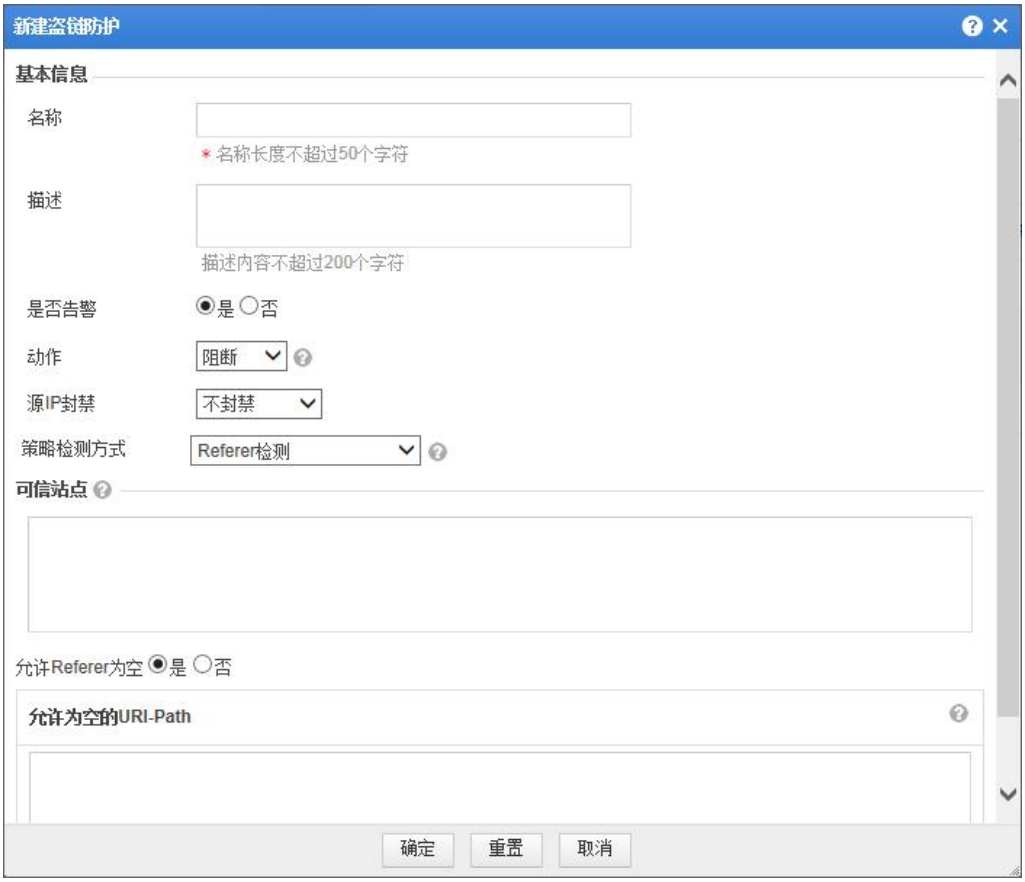
新建盗链防护策略步骤如下：

步骤 1 选择菜单 **安全管理 > 策略管理 > 高级防护 > 盗链防护**，进入盗链防护策略列表，如图 4-74 所示。

图 4-73 盗链防护策略

步骤 2 单击【新建】按钮，弹出新建盗链防护策略对话框，如图 4-75 所示。

图 4-74 新建盗链防护策略



步骤 3 配置盗链防护策略参数，参数详细信息如表 4-25 所示。

表 4-24 盗链防护策略参数信息

配置项	描述
名称	盗链防护策略的名称。
描述	盗链防护策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对指定源 IP 进行封禁；

配置项	描述
	• **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对指定源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
策略检测方式	算法有两种： • **Referer 检测**：只验证用户的 http 请求中 Referer 字段。如果该 Referer 字段与信任域的 URL 地址匹配，则认为是普通行为；反之，则认为是盗链访问行为。 • **Referer+Cookie 结合算法**： 验证用户 http 请求中的 Referer 字段和 cookie ID 值。如果该 Referer 字段与信任域的 URL 匹配且 cookie ID 为 WAF 授权，则认为是普通访问行为；反之，则认为是盗链行为。
可信站点	可以理解为保护对象 URL 的访问入口页面，也就是必须先访问 Referer URL，然后从 Referer URL 跳转到保护对象 URL，才认为是合法的，对保护对象 URL 的其他访问方式均认为是盗链行为。 信任域为 url 地址。支持*通配符，但不包括任何 URL 参数。格式如：*.example.com/。 注意：每行一个 url 地址。当不配置信任域时，来自同一站点的 referer 地址总是可信的。
允许 referer 为空	是否允许 Referer URL 地址为空。
允许为空的 URI-Path	当不配置此路径时，所有 URL 均允许 referer 为空。反之，如果配置了 URL，则只有配置的 URL 才允许 referer 为空。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3.2 配置跨站请求伪造防护策略

跨站请求伪造 CSRF（Cross-site request forgery）， 是一种盗用合法用户的身份，以用户的名义发送恶意请求的攻击。常见的 CSRF 攻击有：以用户名义发送邮件、发消息，盗取用户帐号，甚至于购买商品，虚拟货币转账等，造成个人隐私泄露和财产的不安全。

在跨站请求伪造防护策略页面，可以进行新建、编辑、复制和删除跨站请求伪造防护策略的操作。下面介绍如何新建跨站请求伪造防护策略，有关如何编辑、复制和删除跨站请求伪造防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

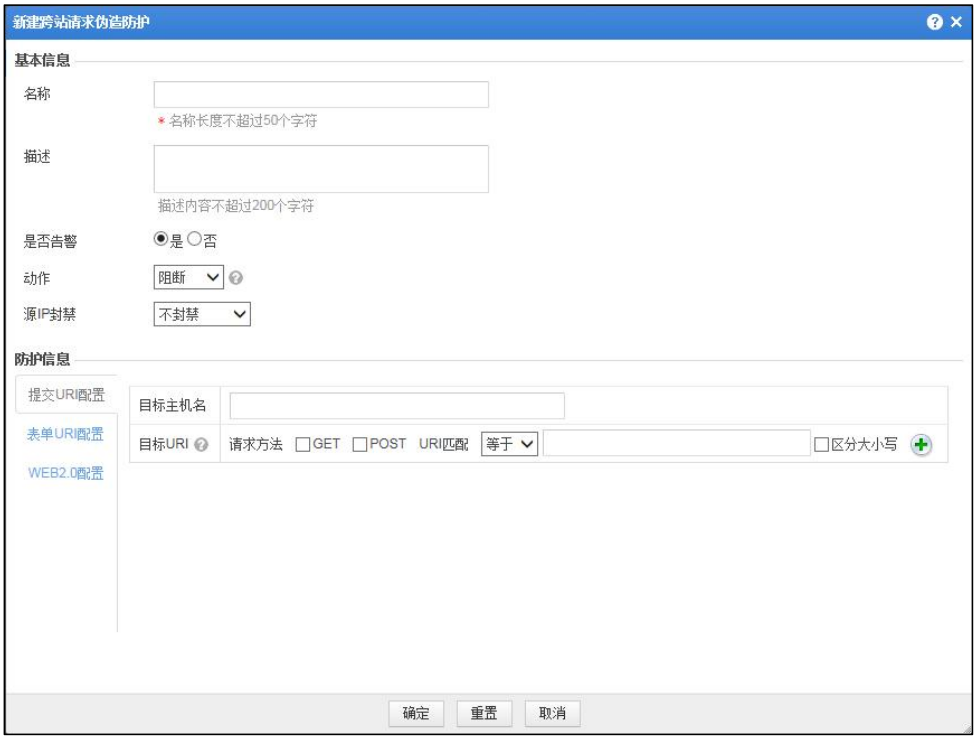
新建跨站请求伪造防护策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **高级防护** > **跨站请求伪造防护**，进入跨站请求伪造防护策略列表，如图 4-76 所示。

图 4-75 跨站请求伪造防护策略

步骤 2 单击【新建】按钮，弹出新建跨站请求伪造防护策略对话框，如图 4-77 所示。

图 4-76 新建跨站请求伪造防护策略



步骤 3 配置跨站请求伪造防护策略参数，参数详细信息如表 4-26 所示。

表 4-25 跨站请求伪造防护策略参数信息

配置项	描述
名称	跨站请求伪造防护策略的名称。
描述	跨站请求伪造防护策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前

配置项	描述
	TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
提交 URI 配置	该部分设置的路径就是要保护的 URL，客户端访问该 URL 时必须携带访问 Referer URL 时 WAF 分配的哈希值，如果没有哈希值，WAF 会阻断访问。 WAF 上配置目标主机名时，非 80 端口的主机名需要填写端口号，例如：www.test.com:808
表单 URI 配置	该部分设置的路径就是要保护 URL 的合法入口 URL，客户端访问 Referer URL 时，WAF 会随机产生一个哈希值返回给客户端，客户端访问防护目标的 URL 时会携带哈希值，WAF 检测到哈希值认为合法放行，如果没有检测到哈希值，则访问都被阻断。
WEB2.0 配置	启用 web2.0 防护之后，安全引擎动态生成的密钥会同时下发到表单和 cookie 中，有效时间参照配置项，密钥验证过一次之后就失效。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3.3 配置扫描防护策略

攻击者通常会利用各种工具扫描网站，探测网站漏洞，给网站的安全带来极大隐患。WAF 可以通过识别扫描工具的数据特征值，阻断扫描工具的探测。

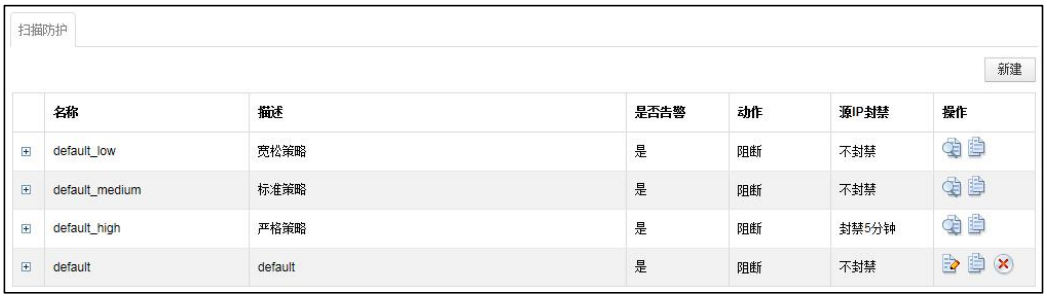
WAF 系统自带对 pagolin、webinspect 和 appscan 等工具的防护规则，其他扫描工具的防护，可通过配置的特征数据进行识别。

在扫描防护策略页面，可以进行新建、编辑、复制和删除扫描防护策略的操作。下面介绍如何新建 Cookie 安全策略，有关如何编辑、复制和删除扫描防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建扫描防护策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **高级防护** > **扫描防护**，进入扫描防护策略列表，如图 4-78 所示。

图 4-77 扫描防护策略



步骤 2 单击【新建】按钮，弹出新建扫描防护策略对话框，如图 4-79 所示。

图 4-78 新建扫描防护策略

步骤 3 配置扫描防护策略参数，参数详细信息如表 4-27 所示。

表 4-26 扫描防护策略参数信息

配置项	描述
名称	扫描防护策略的名称。
描述	扫描防护策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP

配置项	描述
	连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问 • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
规则库匹配	是否启用规则库匹配。
请求量统计	• 是否启用：是否启用请求量统计。请求量统计一个统计周期内的 HTTP 请求的数量。 • 最小样本数：有效统计次数，数值大于等于 2 小于等于 20，当统计的有效次数达到这个数目时，将进行统计算法分析。 • 请求离散率：取值范围为：0～1 之间的小数。在统计周期内，如果请求离散率越小，统计数据越具有规律性，可认定为是扫描器操作。 • 最大请求量：最大请求量用来设置 5 秒钟内允许的最大 HTTP 请求量。  请求离散率和最大请求量两个参数需至少填写一项。当只填写最大请求量时，系统会默认请求离散率为 0。
应答分布统计	• 是否启用：是否启用应答分布统计。应答分布统计了在统计时间段内，HTTP 响应码的分布情况。 • 成功应答比例：统计时间段内的 http 协议成功状态码的比例。如 100(Continue)，200(OK)，302(Found)的统计比例，取值范围为 0～1 之间的小数。 • 失败应答比例：统计时间段内的 http 协议失败状态码的比例。 • 如 404(Not Found)，500(Internal Server Error)等的统计比例，取值范围为 0～1 之间的小数。  成功应答比和失败应答比至少填写一项。当只填写一项时，失败应答比默认为 1，成功应答比默认为 0。 • 最小统计量：在统计周期内，必须统计的最小统计量。只有统计次数达到设定的最小统计量，才进行统计比例计算。 • 统计时间：扫描防护统计的时间范围。
阈值告警	• 是否启用：是否启用阈值告警。 • 最大告警数：统计时间段内针对指定源 IP 的告警数量的最大值。 • 统计时间：设置扫描防护统计的时间范围。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3.4 配置 Cookie 安全策略

Cookie 是由服务器发送给客户端浏览器，让浏览器保存并在后续的访问中一同提交给服务器的一段数据，通常用来保存客户信息及会话状态等内容。当客户机访问服务器时，一些重要的信息会保留在 Cookie 里，可能会被他人利用，导致信息泄露或其他安全问题。另外 WEB 应用程序对 Cookie 值进行处理中可能存在漏洞，攻击者可以通过修改提交的 Cookie 内容构造恶意请求进行攻击。

WAF 进行 Cookie 安全防护的方式有如下两种：

- Cookie 签名

  在不改变原 Cookie 内容的前提下对指定的 Cookie 值进行签名并将签名内容作为 Cookie 内容一部分一同发送给客户端，由于 Cookie 内容为明文，客户端可以查看到 Cookie 内容，但对 Cookie 已签名字段的修改将可以被 WAF 识别，并作出相应动作。

- Cookie 加密

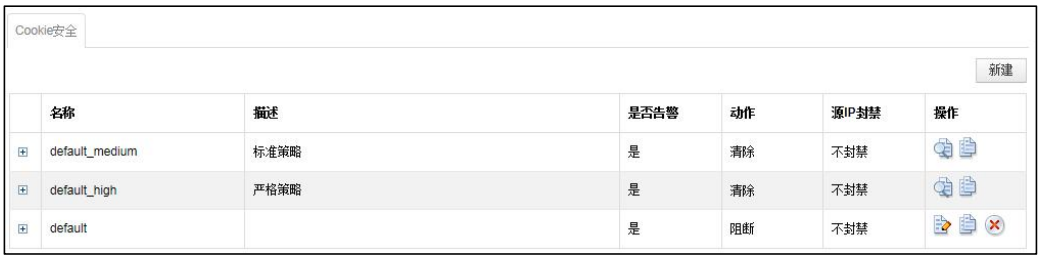
  对 Cookie 进行加密，使用自有的加密算法对指定的 Cookie 值进行加密，使用加密后的 Cookie 值替换原 Cookie 值，在客户端将 Cookie 提交给服务器时 WAF 再对 Cookie 进行解密，将 Cookie 的明文发送给服务器端。防止攻击者查看 Cookie 值或修改 Cookie 内容。

在 Cookie 安全策略页面，可以进行新建、编辑、复制和删除 Cookie 安全策略的操作。下面介绍如何新建 Cookie 安全策略，有关如何编辑、复制和删除 Cookie 安全策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建 Cookie 安全策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **高级防护** > **Cookie 安全**，进入 Cookie 安全策略列表，如图 4-80 所示。

图 4-79 Cookie 安全策略



步骤 2 单击【新建】按钮，弹出新建 Cookie 安全策略对话框，如图 4-81 所示。

图 4-80 新建 Cookie 安全策略

步骤 3 配置 Cookie 安全策略的详细信息，如表 4-28 所示。

表 4-27 Cookie 安全策略参数信息

配置项	描述
名称	Cookie 安全策略的名称
描述	Cookie 安全策略的描述说明。
是否告警	是否产生告警日志。
动作	有 6 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。 • **清除**：当检测到非法 Cookie 时，WAF 不阻断 HTTP 会话，而是删除它们后再将数据发送给后端服务器。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问；

配置项	描述
	• **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
主机名称	防护的目标主机名称。
启用 HTTPOnly	是否启用 HTTPOnly。 使用 HTTPOnly 属性后，Cookie 只对浏览器（主流浏览器 IE/Firefox/Chrome 均已支持）可见，客户端的脚本无法获取 Cookie，从而可以更好地保护 Cookie 不被盗用。
防护算法	有 Cookie 加密和 Cookie 签名两类，必须选择一类防护方法。
启用源 IP 校验	是否启用源 IP 校验。 将客户端 IP 作为 Cookie 加密或签名的算法的一部分，加密或签名后的 Cookie 只有从相同的 IP 提交给服务器才被 WAF 认为有效，以此防止 Cookie 的盗用及由此引发的会话支持，从而能更好地保证 Cookie 安全。
Cookie 兼容时间	在启用 Cookie 安全策略前，Web 客户端可能已经存留了未经加密或签名的 Cookie，为了保证启用策略前后的 Cookie 兼容性，WAF 提供“Cookie 兼容时间”选项，在定义的这个时间之前，WAF 执行以下动作： • 对服务器端新下发的 Cookie 执行策略所定义的加密或签名动作； • 对从客户端所接收到的 Cookie，尝试进行解密或签名校验。若是加密、签名正确的 Cookie，则解密或去除签名后再提交给服务器；否则保持原样不变。
Cookie 名称	输入要保护的 Cookie 名称；其中 Cookie 名称可输入多个，每行输入一个 Cookie。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3.5 配置内容过滤策略

在内容过滤策略页面，可以进行新建、编辑、复制和删除内容过滤策略的操作。下面介绍如何新建内容过滤策略，有关如何编辑、复制和删除内容过滤策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建内容过滤策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **高级防护** > **内容过滤**，进入内容过滤策略列表，如图 4-82 所示。

图 4-81 内容过滤策略

步骤 2 单击【新建】按钮，弹出新建内容过滤策略对话框，如图 4-83 所示。

图 4-82 新建内容过滤策略

步骤 3 配置内容过滤策略参数，参数详细信息如表 4-29 所示。

表 4-28 内容过滤策略参数信息

配置项	描述
名称	内容过滤策略的名称。
描述	内容过滤策略的描述说明。
是否告警	是否产生告警日志。
动作	有五 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP

配置项	描述
	连接。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
匹配原则	匹配原则有两种： • 匹配中即结束，是匹配一条规则后就不进行后续规则的匹配； • 匹配中仍继续，是匹配一条规则后仍要进行策略中后续规则的匹配。
规则筛选	根据规则类型、ID、危险等级、名称和准确度中的一项或多项过滤条件，对规则列表进行筛选。单击图 4-83 所示页面的【筛选】按钮后，下方的规则列表将显示根据指定条件过滤后的规则列表。
规则列表	至少选择一个规则。要将某个规则加入规则集，只需勾选规则对应的复选框。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3.6 配置敏感信息过滤策略

敏感信息过滤策略主要针对指定的隐私信息如个人身份证、社会安全号码等进行过滤，对涉及敏感信息内容的访问进行阻断或者替换为指定字符，从而避免泄露用户隐私。

在敏感信息过滤策略页面，可以进行新建、编辑、复制和删除敏感信息过滤策略的操作。下面介绍如何新建敏感信息过滤策略，有关如何编辑、复制和删除敏感信息过滤策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建敏感信息过滤策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **高级防护** > **敏感信息过滤**，进入敏感信息过滤策略列表，如图 4-84 所示。

图 4-83 敏感信息过滤策略

步骤 2 单击【新建】按钮，弹出新建敏感信息过滤策略对话框，如图 4-85 所示。

图 4-84 新建敏感信息过滤策略

步骤 3 配置敏感信息过滤策略参数，参数详细信息如表 4-30 所示。

表 4-29 敏感信息过滤策略参数信息

配置项	描述
名称	敏感信息过滤策略的名称。
描述	敏感信息过滤策略的描述说明。
是否告警	是否产生告警日志。
动作	有 4 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **替换**：对符合条件的请求，WAF 将响应体中匹配到的特征替换为指定字符，然后结束本次策略检测，但还会对其进行其他安全检测。
替换方式	如果动作选择**替换**，则该项必须设置。即 WAF 保留匹配特征前 n 个字符和匹配特征后 n 个字符的内容，将其余字符替换为用户配置的内容，其中替换字符只能为英文字符或数字。
匹配原则	匹配原则有两种： • 匹配中即结束，是匹配一条规则后就不进行后续规则的匹配； • 匹配中仍继续，是匹配一条规则后仍要进行策略中后续规则的匹配。 如果动作选择为替换，则匹配原则只能默认选匹配中仍继续，匹配中即结束置灰不可选；如果动作为除替换外的其它动作，则匹配原则两个选项均可任选。

配置项	描述
规则筛选	根据规则类型、ID、危险等级、名称和准确度中的一项或多项过滤条件，对规则列表进行筛选。单击图 4-85 所示页面的【筛选】按钮后，下方的规则列表将显示根据指定条件过滤后的规则列表。
规则列表	至少选择一个规则。要将某个规则加入规则集，只需勾选规则对应的复选框。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3.7 配置暴力破解防护策略

暴力破解是指，攻击者通过收集互联网上已经泄露的用户名和密码信息，生成对应的字典表，并依据该表进行批量登陆其他网站的尝试，从而得到一系列可以登陆的用户名及密码信息。

暴力破解防护策略的主要作用就是验证登录行为是否为暴力破解攻击，从而防止攻击者利用已知库，进行暴力破解攻击盗取用户信息。

WAF 进行暴力破解防护主要依赖于统计检测：正常的普通用户登录一个站点，提交的验证请求在短时间内不会重复多次；如果在设定的检测周期内重复请求多次，则有可能是利用工具或脚本的自动登录。据此，WAF 可以判断其为暴力破解。

若设置动作为验证码，当在一个检测周期内提交的验证请求超过阈值，WAF 将返回一个包含验证码的验证页面，用户需要输入正确的验证码后才能继续对目标 URL 发起请求，否则将继续进行验证码验证。

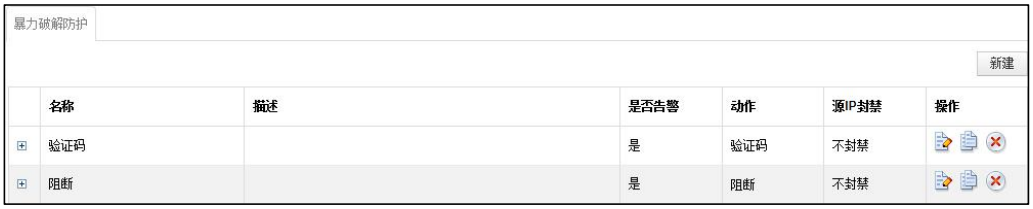
配置暴力破解防护策略时，WAF 默认使用统计检测进行暴力破解防护，用户可根据需要选择是否开启验证码。

在暴力破解防护策略页面，可以进行新建、编辑、复制和删除暴力破解防护策略的操作。下面介绍如何新建暴力破解防护策略，有关如何编辑、复制和删除暴力破解防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建暴力破解防护策略步骤如下：

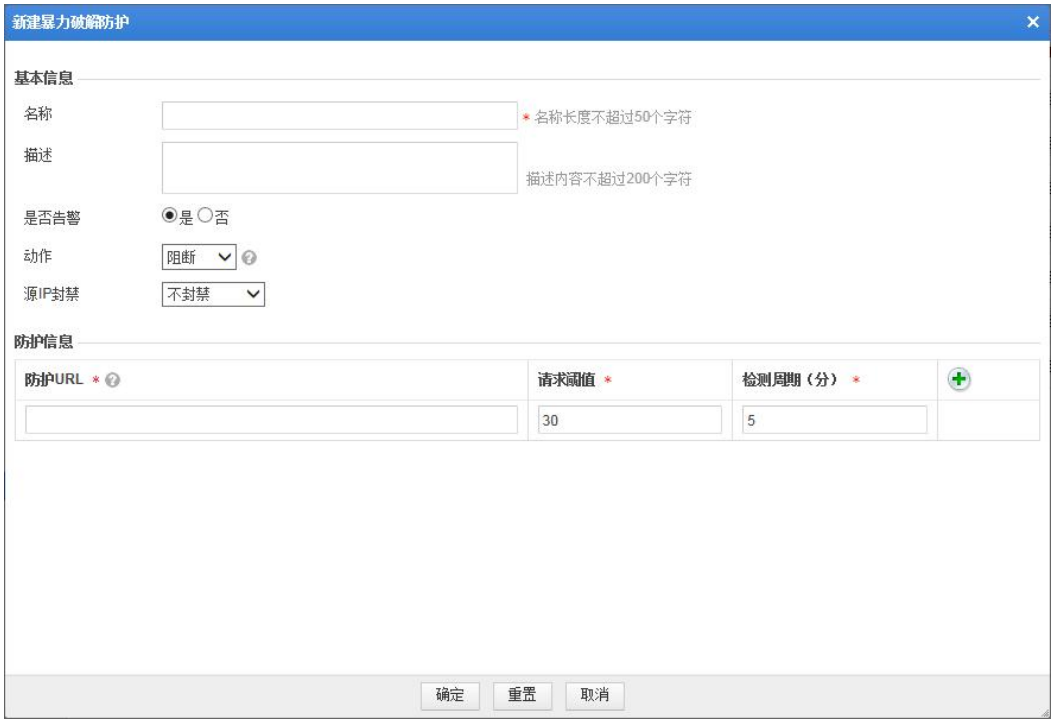
步骤 1 选择菜单 **安全管理** > **策略管理** > **高级防护** > **暴力破解防护**，进入暴力破解防护策略列表，如图 4-86 所示。

图 4-85 暴力破解防护策略



步骤 2 单击【新建】按钮，弹出新建暴力破解防护策略对话框，如图 4-87 所示。

图 4-86 新建暴力破解防护策略



步骤 3 配置暴力破解防护策略参数，参数详细信息如表 4-31 所示。

表 4-30 暴力破解防护策略参数信息

配置项		描述
基本信息	名称	暴力破解防护策略的名称。名称长度不超过 50 字符。
	描述	暴力破解防护策略的描述说明。
	是否告警	触发暴力破解防护策略时，是否进行告警。
	动作	对于符合条件的请求，WAF 采取怎样的动作。动作选项包括： • **放过**：WAF 不再作任何安全检测而直接转发给服务器； • **接受**：WAF 结束本次策略检测，但还会对其作其它安全检测； • **阻断**：WAF 结束本次策略检测，并直接关闭当前 TCP 连接； • **重定向**：WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接； • **伪装**：WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。 • **验证码**：对符合条件的请求，WAF 用验证码回应客户端。
	源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
	重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
	响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。

配置项		描述
	响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
防护信息	防护 URL	需要 WAF 防护的提交登录信息的目标 URL。
	请求阈值	GET/POST 方式下，判定是否为暴力破解攻击的单个检测周期内的最大登录次数。范围为 1~300 次，默认 30 次。
	检测周期（分）	判定是否为暴力破解攻击的单个检测周期。范围为 1~360，默认 5，单位：分。
	登录验证方式	当动作选择**验证码**时需要配置该配置项。 客户端向服务器发起登录请求时，服务器对其进行验证的方式。可选方式有：Form、Ajax、Jsonp。
	登录 Referer	当动作选择**验证码**时需要配置该配置项。 登录提交 URL 对应的 Referer URL。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3.8 配置 XML 攻击防护策略

WAF 进行 XML 攻击防护主要依赖于以下 3 种校验方式：

- XML 基础校验

  通过对 XML 文档的基础元素进行校验，判断是否存在 XML 攻击。基础元素包括：树深度、元素、属性、CDATA（Unparsed Character Data，不由 XML 解析器进行解析的文本数据）、DTD（Documnet Type Definition，文件类型定义）等。

- Schema 校验

  通过用一个指定的 XML Schema 来校验 XML 文档，以检查该 XML 文档是否符合其要求，判断是否存在 XML 攻击。

  XML Schema 描述了 XML 文档的结构。一个 XML Schema 会定义：文档中出现的元素、文档中出现的属性、子元素、子元素的数量、子元素的顺序、元素是否为空、元素和属性的数据类型、元素或属性的默认和固定值等。

- SOAP 校验

  SOAP 校验，即使用 WSDL（Web Services Description Language）在 WebService 应用部署之前对 SOAP 消息进行验证，从而判断是否存在 XML 攻击。

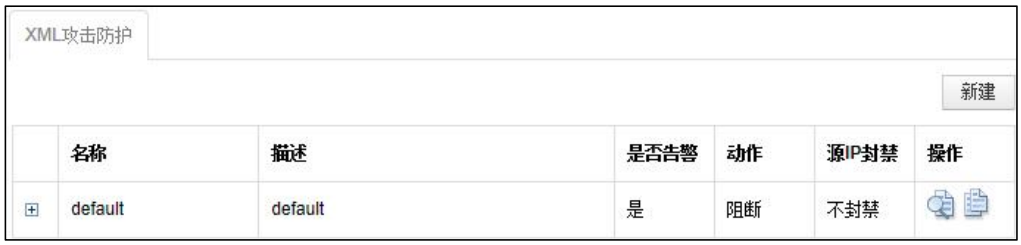
  SOAP、WSDL、UDDI(UniversalDescriptionDiscovery andIntegration)是 WebService 三要素，SOAP 用来描述传递信息的格式，WSDL 用来描述如何访问具体的接口，UDDI 用来管理、分发、查询 WebService。

在 XML 攻击防护策略页面，可以进行新建、编辑、复制和删除 XML 攻击防护策略的操作。下面介绍如何新建 XML 攻击防护策略，有关如何编辑、复制和删除 XML 攻击防护策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建 XML 攻击防护策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **高级防护** > **XML 攻击防护**，进入 XML 攻击防护策略列表，如图 4-88 所示。

图 4-87 XML 攻击防护策略



步骤 2 单击【新建】按钮，弹出新建 XML 攻击防护策略对话框，如图 4-89 所示。

图 4-88 新建 XML 攻击防护策略

步骤 3 配置 XML 攻击防护策略参数，参数详细信息如表 4-32 所示。

表 4-31 XML 攻击防护策略参数信息

配置项		描述
基本信息	名称	XML 攻击防护策略的名称。名称长度不超过 50 字符。
	描述	XML 攻击防护策略的描述说明。
	是否告警	触发 XML 攻击护策略时，是否进行告警。
	动作	对于符合条件的请求，WAF 采取怎样的动作。动作选项包括：

配置项			描述
			• **放过**：WAF 不再作任何安全检测而直接转发给服务器； • **接受**：WAF 结束本次策略检测，但还会对其作其它安全检测； • **阻断**：WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）； • **重定向**：WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接（当动作为“重定向”时，需要设置重定向路径的完整 URL）； • **伪装**：WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接（当动作为“伪装”时，还需要设置响应码、响应文件，其中，响应文件可以选择已有，也可以上传）。
	源 IP 封禁		如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
	重定向路径		如果动作选择**重定向**，则该项必选，设置重定向的 URL。
	响应码		如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
	响应文件		如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
检测项	XML 基础校验	开启 XML 基础校验	是否开启 XML 攻击防护基础校验。 选择“是”还需要对以下校验参数进行配置。
		最大树深度	XML 树结构的最大深度。
		最大元素名长度	XML 元素名的最大长度。
		最多元素个数	XML 元素的最大个数。
		最多子节点个数	XML 节点可包含的最大子节点个数。
		最多属性个数	XML 元素可包含属性的最大个数。
		最大属性名长度	XML 元素属性名称的最大长度。
		最大属性值长度	XML 元素属性值的最大长度。
		最大 CDATA 长度	XML 中 CDATA 的最大长度。
		最大文档大小	最大 XML 文档不能超过的字节数。
		最小文档大小	最小 XML 文档不能少于的字节数。
		禁止包含处理指令	是否禁止 XML 包含处理指令。默认禁止。
		禁止包含 DTDs	是否禁止 XML 包含 DTDs。默认禁止。
		禁止引用外部实体	是否禁止 XML 引用外部实体。默认禁止。
	Schema 校验	开启 Schema 校验	是否开启 Schema 校验。选择“是”，每个策略可以配置 10 组 schema 校验参数，每组校验参数分别由 schema 文件和目标 URL 组成，则还需要对以下校验参数进行配置。
		Schema 文件	即 XSD 文件，选择 Schema 文件，或者从本地上传 Schema 文件。每组校验参数，只能选择或上传 1 个 Schema 文件。

配置项			描述
			各组之间的 Schema 文件不允许重复。 管理 XSD 文件的操作请参见 4.11.2 XSD/WSDL 文件管理。
		目标 URL	每个 Schema 文件最多可配置 10 个目标 URL，只对符合目标 URL 的 XML 流量进行 Schema 校验。 输入目标 URL 时注意以下几点： • URL 不支持通配符； • URL 格式支持：host + uri-path + query-string； • 输入 URL 时可不包含“http://”，后台处理时将自动在 URL 前加上“http://”； • 界面默认只支持 HTTP 协议，若用户想要输入 HTTPS 的 URL，则输入框中必须加上“https://”； • URL 的最大长度为 2048 字符。
	SOAP 检验	开启 SOAP 校验	是否开启 SOAP 校验。选择“是”，每个策略可以配置 10 组 SOAP 校验参数，每组校验参数分别由 wsdl 文件和目标 URL 组成，则还需要对以下校验参数进行配置。
		WSDL 文件	选择 WSDL 文件，或者从本地上传 WSDL 文件。每组 SOAP 校验参数，只能选择或者上传 1 个 WSDL 文件。各组之间的 WSDL 文件不允许重复。 管理 WSDL 文件的操作请参见 4.11.2 XSD/WSDL 文件管理。
		目标 URL	每个 WSDL 文件最多可配 10 个目标 URL。输入目标 URL 的注意事项与 Schema 文件的 URL 一致。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.3.9 配置智能引擎检测

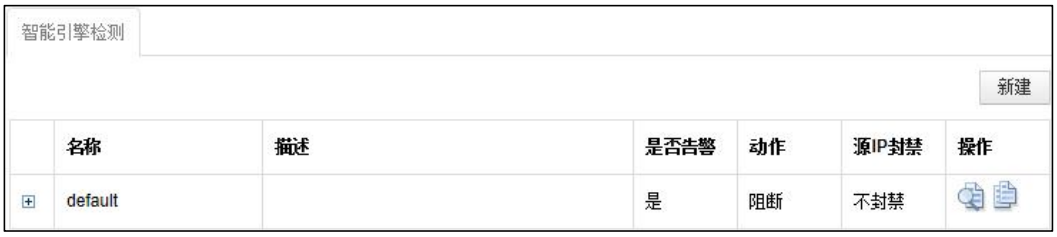
智能引擎是基于机器学习的新一代 Web 攻击检测引擎，在传统规则检测的基础上，加入了语法分析与统计算法，从而实现更高的检测率和更低的误报率。目前，WAF 设备支持智能引擎检测的攻击类型有 4 类：跨站脚本攻击、SQL 注入攻击、命令行注入攻击、路径穿越攻击。

在智能引擎检测页面，可以进行新建、编辑、复制和删除智能引擎检测策略的操作。下面介绍如何新建智能引擎检测策略，有关如何编辑、复制和删除智能引擎检测与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建智能引擎检测策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **高级防护** > **智能引擎检测**，进入智能引擎检测策略列表，如图 4-90 所示。

图 4-89 智能引擎检测策略



步骤 2 单击【新建】按钮，弹出新建智能引擎检测策略对话框，如图 4-91 所示。

图 4-90 新建智能引擎检测策略

步骤 3 配置智能引擎检测策略参数，参数详细信息如表 4-33 所示。

表 4-32 智能引擎检测策略参数信息

配置项	描述
名称	智能引擎检测策略的名称。
描述	智能引擎检测滤策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接。

配置项	描述
	• **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
响应码	如果动作选择**伪装**，则该项必选，选择 HTTP 响应码。
响应文件	如果动作选择**伪装**，则该项必选，可以自行上传响应文件或选择已有响应文件。
检测攻击	智能引擎可检测的攻击类型，包括：**跨站脚本攻击**、**SQL 注入攻击**、**命令行注入攻击**、**路径穿越攻击**。
检测内容	智能引擎可检测的内容，包括：**URI**、**参数**、**Cookie**。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.4 精准防护

精准防护是 WAF 特有的防护策略。WAF 通过自学习策略获取的自学习结果，记录了被保护服务器的实际访问信息统计数据，根据该类规则配置的策略可以为用户提供精准的防护。

在白名单策略页面，可以进行新建、编辑、复制和删除白名单策略的操作。下面介绍如何新建白名单策略，有关如何编辑、复制和删除白名单策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建白名单策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **精准防护** > **白名单**，进入白名单策略配置列表，如图 4-92 所示。

图 4-91 配置白名单策略

步骤 2 单击【新建】按钮，弹出新建白名单策略对话框，如图 4-93 所示。

图 4-92 新建白名单策略

步骤 3 配置白名单策略参数，参数详细信息如表 4-34 所示。

表 4-33 白名单策略参数信息

配置项	描述
名称	白名单策略的名称。
描述	白名单策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。

配置项	描述
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。
可选学习结果对象	可选择的自学习结果规则。 当站点包含的目录层次太深或子目录太多时，不推荐在整个站点或该目录上使用全选功能，这可能导致浏览器响应缓慢。

步骤 4 单击【提交】按钮，保存配置。

----结束

4.7.5 其他防护

其他防护包括例外策略、自定义策略以及风险级别策略。下面介绍这三类策略的配置方法。

4.7.5.1 配置例外策略

例外策略通常用来对已经配置的基础防护或高级防护策略的防护内容进行补充或其他限定。

在例外策略页面，可以进行新建、编辑、复制和删除例外策略的操作。下面介绍如何新建例外策略，有关如何编辑、复制和删除例外策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建例外策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **其他防护** > **例外策略**，进入例外策略配置列表，如图 4-94 所示。

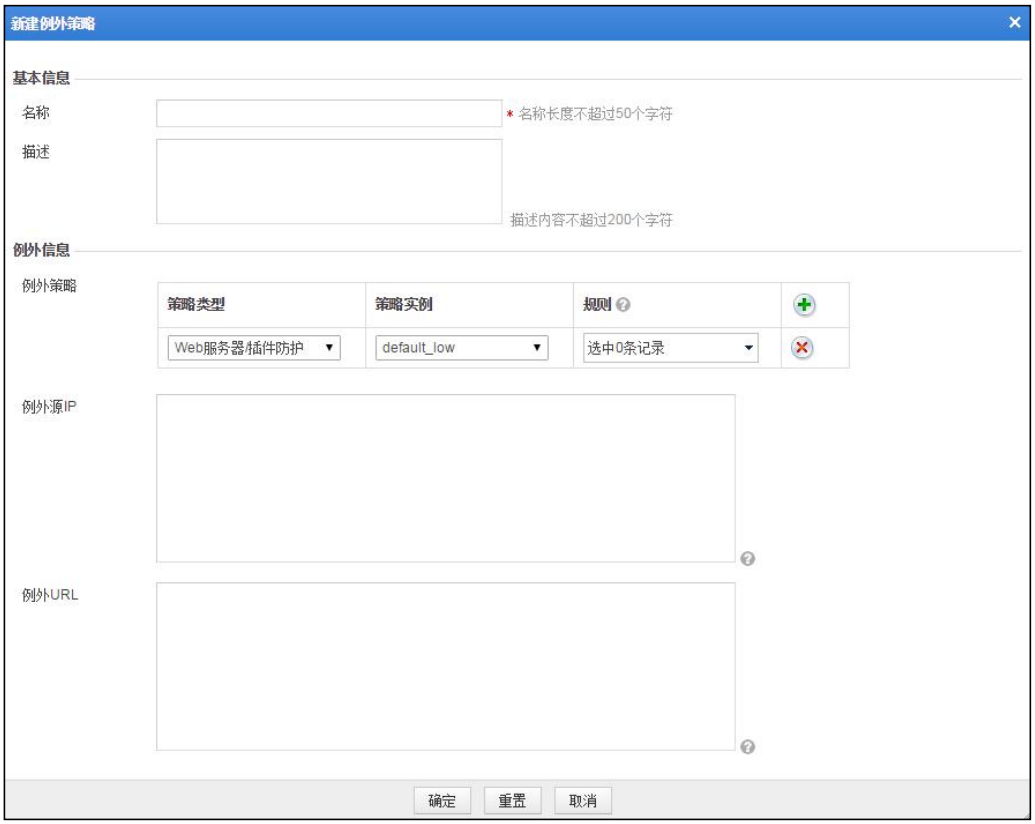
说明	也可以在站点防护例外控制中，直接新建并编辑例外策略，相关介绍请参见配置例外策略。

图 4-93 例外策略列表

步骤 2 单击【新建】按钮，弹出新建例外策略对话框，如图 4-95 所示。

用户可以在一个例外策略中配置多个策略的例外策略。

图 4-94 新建例外策略



步骤 3 配置例外策略参数，参数详细信息如表 4-35 所示。

表 4-34 例外策略参数信息

配置项	描述
名称	例外策略的名称。
描述	例外策略的描述说明。
例外信息	
策略类型	选择新建例外策略的策略类型。
策略实例	使用例外策略进行补充配置的策略实例。
规则	如果选中的防护策略实例下没有规则集合，则该项显示“无规则”，此时 WAF 会将该策略添加到例外中； 如果选中的防护策略实例下存在规则集，此时： • 如果不选中任何规则，则 WAF 会将该策略添加到例外； • 如果选中任一规则，则 WAF 只将该条规则添加到例外。
例外源 IP	适用该例外策略的源 IP 地址。支持单个 IP 地址或者 IP 地址段，如：10.66.9.1，192.168.1.1-192.168.1.255。 如果不填写则表示任意 IP 地址段。
例外 URL	适用该例外策略的源 URL 地址。 每行输入一条 url 路径，格式为:[$]域名[:端口]/路径/文件，以$开头表示正则表达式匹配，否则是完全匹配。

配置项	描述
	例：www.example1.com:8080/login.jsp，$www.example2.com:80/.*，如果不填写则表示任意 URL 地址。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.5.2 配置自定义策略

自定义策略为用户提供了自定义配置策略的功能。用户可以选择多条内置规则或自定义规则实现多角度的网络安全防护。

在自定义策略页面，可以进行新建、编辑、复制和删除自定义策略的操作。下面介绍如何新建自定义策略，有关如何编辑、复制和删除自定义策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

新建自定义策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **其他防护** > **自定义策略**，进入自定义策略配置列表，如图 4-96 所示。

图 4-95 自定义策略列表

步骤 2 单击【新建】按钮，弹出新建自定义策略对话框，如图 4-97 所示。

用户可以在规则列表中选择多个自定义规则。

图 4-96 新建自定义策略

步骤 3 配置自定义策略参数，参数详细信息如表 4-36 所示。

表 4-35 自定义策略参数信息

配置项	描述
名称	自定义策略的名称。
描述	自定义策略的描述说明。
是否告警	是否产生告警日志。
动作	有 5 种类型的动作： • **放过**：对符合条件的请求，WAF 不再作任何安全检测而直接转发给服务器。 • **接受**：对符合条件的请求，WAF 结束本次策略检测，但还会对其作其它安全检测。 • **阻断**：对符合条件的请求，WAF 结束本次策略检测，并直接关闭当前 TCP 连接（当动作为“阻断”时，WAF 还提供“源 IP 封禁”选项）。 • **重定向**：对符合条件的请求，WAF 构造一个 302 重定向页面回应客户端，并关闭当前 TCP 连接。 • **伪装**：对符合条件的请求，WAF 使用用户自定义的 HTTP 响应码及响应文件的内容回应客户端，并关闭当前 TCP 连接。
源 IP 封禁	如果动作选择**阻断**，则该项为必选。 • **不封禁**：不对源 IP 进行封禁； • **永久封禁**：永久阻断该源 IP 的访问； • **自定义封禁**：在设定时间内对源 IP 进行封禁。封禁时间可以配置为秒、分钟、小时。
重定向路径	如果动作选择**重定向**，则该项必选，设置重定向的 URL。

配置项	描述
匹配原则	匹配原则有两种： • 匹配中即结束，是匹配一条规则后就不进行后续规则的匹配； • 匹配中仍继续，是匹配一条规则后仍要进行策略中后续规则的匹配。
规则筛选	根据规则类型、ID、名称中的一项或多项过滤条件，对规则列表进行筛选。单击图 4-97 所示页面的【筛选】按钮后，下方的规则列表将显示根据指定条件过滤后的规则列表。
规则列表	至少选择一个规则。要将某个规则加入规则集，只需勾选规则对应的复选框。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.7.5.3 配置风险级别策略

风险级别策略用于对防护策略进行风险级别自定义，通过风险级别对站点进行防护。

WAF 能够读取并保存用户配置的风险级别策略信息，并根据风险级别配置信息检测来自客户端的 http 请求，判断该请求是否属于自定义风险级别集。

- 如果属于，则返回用户自定义的风险级别；
- 如果不属于，则返回空，并按原有事件告警级别写进日志。

在风险级别策略页面，可以进行新建、编辑、复制和删除风险级别策略的操作。下面介绍如何新建风险级别策略，有关如何编辑、复制和删除风险级别策略与 HTTP 协议校验策略相同，详情请参考 HTTP 协议校验策略的相关介绍，此处不再赘述。

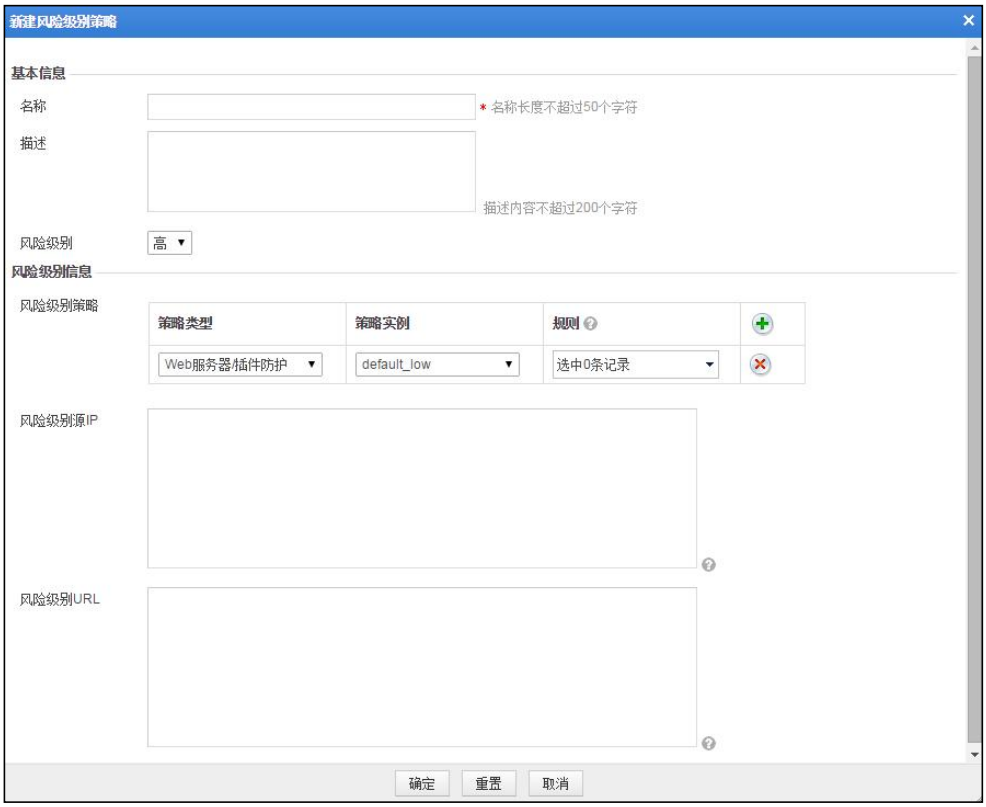
新建风险级别策略步骤如下：

步骤 1 选择菜单 **安全管理** > **策略管理** > **其他防护** > **风险级别策略**，进入风险级别策略配置列表，如图 4-98 所示。

图 4-97 风险级别策略列表

步骤 2 单击【新建】按钮，弹出新建风险级别策略对话框，如图 4-99 所示。

图 4-98 新建风险级别策略



步骤 3 配置风险级别策略参数，参数详细信息如表 4-37 所示。

表 4-36 风险级别策略参数信息

配置项	描述
名称	风险级别策略的名称。
描述	风险级别策略的描述说明。
风险级别	风险级别策略的风险等级。 可选级别有：高、中、低。
风险级别信息	
风险级别策略	风险级别策略的防护策略类型、策略实例、规则。单击图标可新建多条风险级别策略，单击图标可删除风险级别策略。 • **策略类型**：在下拉列表中选择防护策略类型。 • **策略实例**：在下拉列表中选择防护策略类型对应的策略实例。 • **规则**：在下拉列表中选择防护策略类型对应的规则。 说明 • 如果该防护策略下不存在规则集合，则显示**无规则**，WAF 会将该策略添加到风险级别策略中； • 如果该防护策略下存在规则集合，有如下两种情况： 1、如果未选中任何规则，WAF 会将该策略添加到风险级别策略中；

配置项	描述
	2、如果选中任一规则，WAF 只将该规则添加到风险级别策略中。
风险级别源 IP	适用该风险级别策略的 HTTP 请求的源 IP。支持单个 IP 地址或者 IP 地址段，如：10.66.9.1，192.168.1.1-192.168.1.255。 如果不填写则表示任意 IP 地址段。
风险级别 URL	适用该风险级别策略的 URL 地址。 每行输入一条 url 路径，格式为:[$]域名[:端口]/路径/文件，以$开头表示正则表达式匹配，否则是完全匹配。 例:www.example1.com:8080/login.jsp，$www.example2.com:80/.*,如果不填写则表示任意 URL 地址。

步骤 4 单击【确定】按钮，保存配置。

----结束

4.8 模板管理

WAF 为用户提供如下三类的策略模板，用户无需新建策略，只需新建一个策略模板，并在相应策略下选择不同级别的策略，并应用到站点，即可开始防护。WAF 自带有如下三种级别的默认策略：

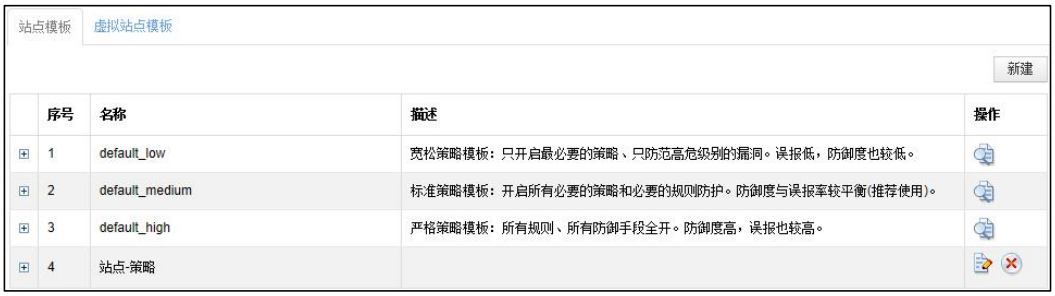
- default_low（宽松策略模板）：只开启最必要的策略、只防范高危级别的漏洞。误报低，防御度也较低。
- default_medium（标准策略模板）：开启所有必要的策略和必要的规则防护。防御度与误报率较平衡(推荐使用)。
- default_high（严格策略模板）：所有规则、所有防御手段全开。防御度高，误报也较高。

模板分为站点模板和虚拟站点模板，下面分别进行介绍。

4.8.1 站点模板

选择菜单 **安全管理** > **模板管理** > **站点模板**，进入站点模板的配置界面，如图 4-100 所示。

图 4-99 站点模板列表

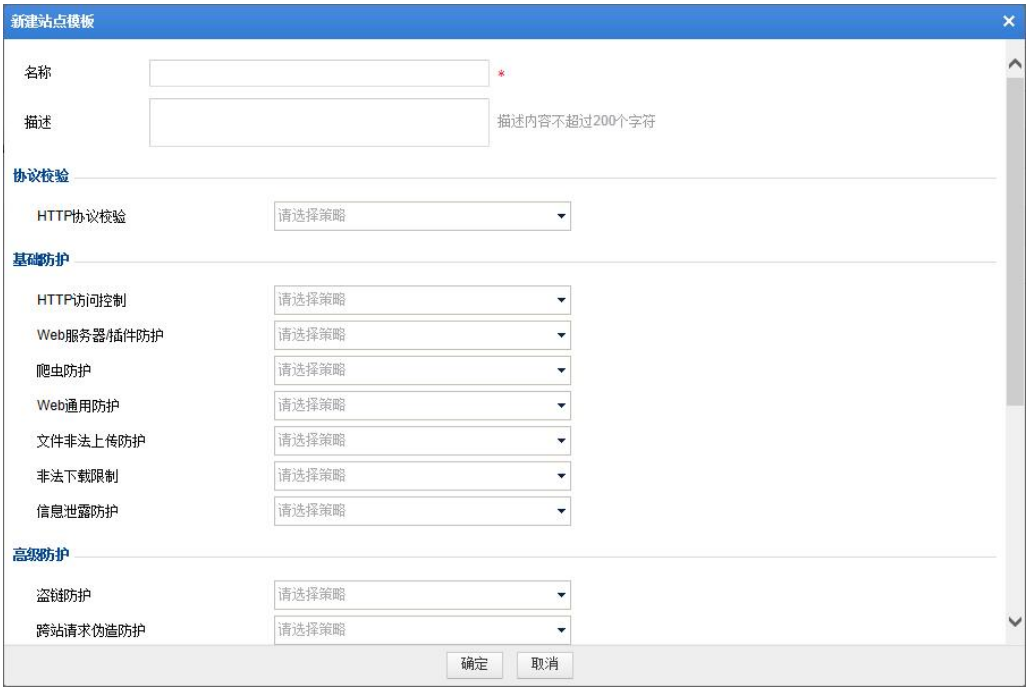


4.8.1.1 新建站点模板

新建站点模板的步骤如下：

步骤 1 单击图 4-100 中的【新建】按钮，弹出新建站点模板对话框，如图 4-101 所示。

图 4-100 新建站点模板



步骤 2 配置站点模板参数，参数信息如表 4-38 所示。

表 4-37 配置站点模板参数信息

配置项	描述
名称	站点模板的名称。
描述	站点模板的描述说明。
选择策略	选择需要进行防护的相应策略。单击某个策略右侧下拉框进行选择。 说明 • 选择策略后，WAF 自动根据策略顺序自上而下进行匹配，单击图标或可向上或向下调整策略顺序。 • 也可直接单击蓝色链接“新建策略”，新建一条策略。

步骤 3 单击【确定】，完成配置。

----结束

4.8.1.2 其他操作

新建站点模板后，在为站点配置 Web 安全防护时，即可在策略模板中，选择相应的站点模板，进行策略的快速配置，详情请参见配置 Web 安全防护策略。

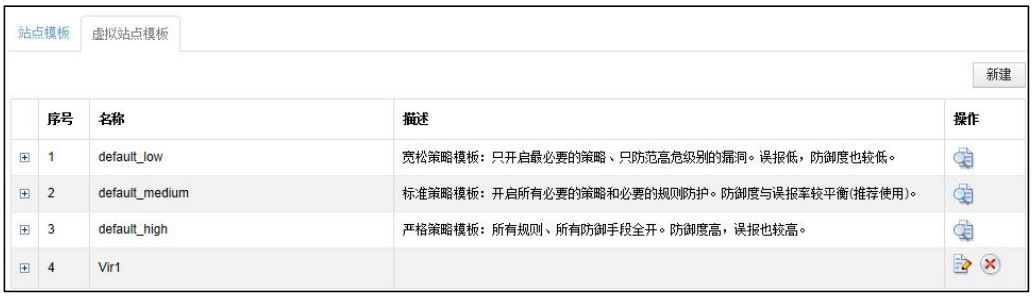
除新建站点模板外，在图 4-100 所示页面，管理员还可进行如下操作：

- 查看模板：单击图标，即可查看对应的模板详情。只有系统自带的站点模板才能进行查看操作。
- 编辑模板：单击图标，即可编辑对应的模板。只有管理员新建的模板才能进行编辑操作。
- 删除模板：单击图标，即可删除对应的模板。只有管理员新建的模板才能进行删除操作。

4.8.2 虚拟站点模板

选择菜单 **安全管理** > **模板管理** > **虚拟站点模板**，进入虚拟站点模板的配置界面，如图 4-102 所示。

图 4-101 虚拟站点模板列表



4.8.2.1 新建虚拟站点模板

新建虚拟站点模板的步骤如下：

步骤 1 单击图 4-102 中的【新建】按钮，弹出新建虚拟站点模板对话框，如图 4-103 所示。

图 4-102 新建虚拟站点模板

步骤 2 配置虚拟站点模板参数，参数信息如表 4-39 所示。

表 4-38 配置虚拟站点模板参数信息

配置项	描述
名称	虚拟站点模板的名称。
描述	虚拟站点模板的描述说明。
选择策略	选择需要进行防护的相应策略。单击某个策略右侧下拉框，选择已有策略。 说明 • 选择策略后，WAF 自动根据策略顺序自上而下进行匹配，单击图标或可向上或向下调整策略顺序。 • 也可直接单击蓝色链接“新建策略”，新建一条策略。

步骤 3 单击【确定】按钮，完成配置。

----结束

4.8.2.2 其他操作

新建虚拟站点模板后，在为虚拟站点配置 Web 安全防护时，即可在策略模板中，选择相应的虚拟站点模板，进行策略的快速配置，详情请参见 4.3.3.3 配置虚拟站点。

除新建虚拟站点模板外，在图 4-102 所示页面，管理员还可进行如下操作：

- 查看模板：单击图标  ，即可查看对应的模板详情。只有系统自带的虚拟站点模板才能进行查看操作。
- 编辑模板：单击图标  ，即可编辑对应的模板。只有管理员新建的模板才能进行编辑操作。
- 删除模板：单击图标  ，即可删除对应的模板。只有管理员新建的模板才能进行删除操作。

4.9 代理信息配置

为了避开互联网上可能影响数据传输速度、传输稳定性的瓶颈和环节，给用户体验更快更稳定的数据传输，越来越多的网站为自己的 Web 服务器购买 CDN（Content Delivery Network，内容分发网络）代理服务。

使用 CDN 代理服务后，客户端向 Web 服务器发起的访问请求首先到达离用户最近的 CDN 服务器节点，如果请求内容已存在于该 CDN 服务器节点的缓存，CDN 的缓存服务器会直接将响应数据返回给客户端；如果请求内容还不存在于该 CDN 服务器节点的缓存中，那么，CDN 服务器节点会做一个反向代理，将请求转发给网站的真实 Web 服务器。

如果网站的真实 Web 服务器前部署了 WAF，那么，CDN 节点服务器反向代理后到达 WAF 的请求 IP 实际上是 CDN 节点的 IP，CDN 服务器节点一般会将真实的客户端 IP 放入请求头部中进行发送，比如较通用的 X-Forwarded-For 头部，以及一些老的代理服务器使用的 Client-IP 首部等。

在这种情况下，如果 WAF 以网络层 IP 做为策略的检测依据，就会造成误阻断情况。WAF 从 V6.0R05F00 版本开始，能够根据配置的代理信息（如 HTTP 头部信息等），解析出真实客户端 IP 作为策略的检测依据，避免误阻断从而适应使用 CDN 代理服务网站的业务场景。

下面介绍代理信息配置的具体方法。

步骤 1 选择菜单 **安全管理** > **代理信息配置**，进入代理信息配置页面，如图 4-116 所示。

图 4-103 代理信息配置

步骤 2 配置代理信息参数。

代理信息参数说明如表 4-44 所示。

表 4-39 代理信息参数

配置项	描述
代理模式	WAF 支持以下三种代理模式。 • **完全忽略**：不解析代理信息；日志详情中“代理信息”字段内容为空；Web 安全日志、Web 访问日志中的“客户端 IP”记录为网络层 IP；安全策略检测/加密算法、IP 封禁动作中使用的源 IP 为网络层 IP。 • **记录代理信息**：解析代理信息；日志详情中“代理信息”字段内容显示从 HTTP 头部字段中解析出的代理信息；Web 安全日志、Web 访问日志中的“客户端 IP”记录为网络层 IP；安全策略检测/加密算法、IP 封禁动作中使用的源 IP 为网络层 IP。 • **策略中使用真实客户端 IP**：解析代理信息；日志详情中“代理信息”字段内容显示从 HTTP 头部字段中解析出的代理信息；Web 安全日志、Web 访问日志中的“客户端 IP”记录为从代理信息中分析得到的客户端源 IP；安全策略检测/加密算法、IP 封禁动作中使用的源 IP 为代理信息分析到的客户端源 IP。
Http-Headers	代理信息的 HTTP 头部名称。触发 Web 安全防护告警的 HTTP 请求中如果包含设置的 HTTP 头部名称，则头部名称字段将作为代理信息记录到 Web 安全日志的日志详情中。 最多可输入 10 个头部名称，名称之间用回车换行进行分隔；所有名称的长度不能超过 256 字节，其中，每个换行符占 1 个字节。

配置项	描述
	说明 • 如果有多个头部字段匹配，则均会被记录。 • 解析客户端真实 IP 时，选择优先级最高的头部字段进行解析。 • HTTP 头部字段优先级按照输入顺序，依次递减。
最大代理深度	代理信息 HTTP 头部的最大深度。代理信息 HTTP 头部的深度不得超过配置的最大代理深度，若超过则很可能是伪造头部，WAF 将不信任该代理信息。 深度范围为 0~10，当深度为 0 时，表示不对代理信息头部进行代理深度检查。
服务端信任 IP	服务器端的信任 IP（支持 IPv4 以及 IPv6）。 最多可输入 10 个 IP 地址或 IP 地址段，多个地址或地址段用英文逗号分隔；所有信任 IP 的长度不能超过 1023 字节。

步骤 3 单击【保存】按钮，保存配置。

----结束

4.10 上传文件管理

上传文件管理包括 SSL 证书管理、XSD/WSDL 文件管理和伪装响应文件管理。

4.10.1 SSL 证书管理

在新建 https 站点时，必须上传或选择已有 SSL 证书，管理员可以在该页面上传、查看或删除 SSL 证书。

4.10.1.1 导入证书

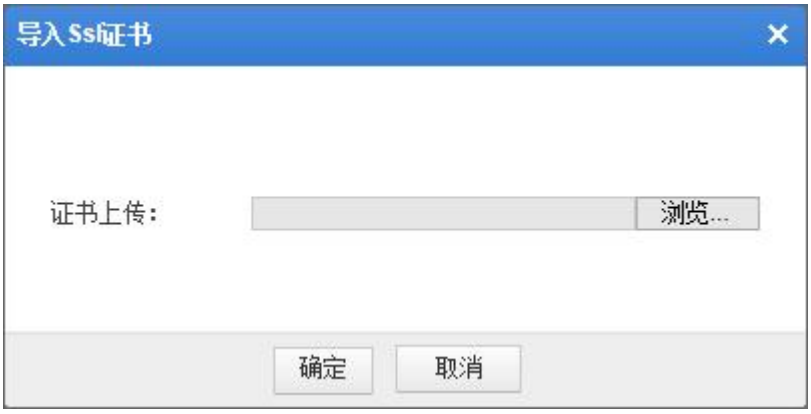
导入 SSL 证书的步骤如下：

步骤 1 选择菜单 **安全管理** > **上传文件管理** > **SSL 证书管理**，进入 SSL 证书管理配置页面，如图 4-117 所示。

图 4-104 SSL 证书管理配置

步骤 2 在图 4-117 所示页面，单击【导入证书】按钮，弹出导入 SSL 证书对话框，如图 4-118 所示。

图 4-105 导入 SSL 证书



步骤 3 单击【浏览】，选择待导入的 SSL 证书，并单击【确定】按钮，完成导入。

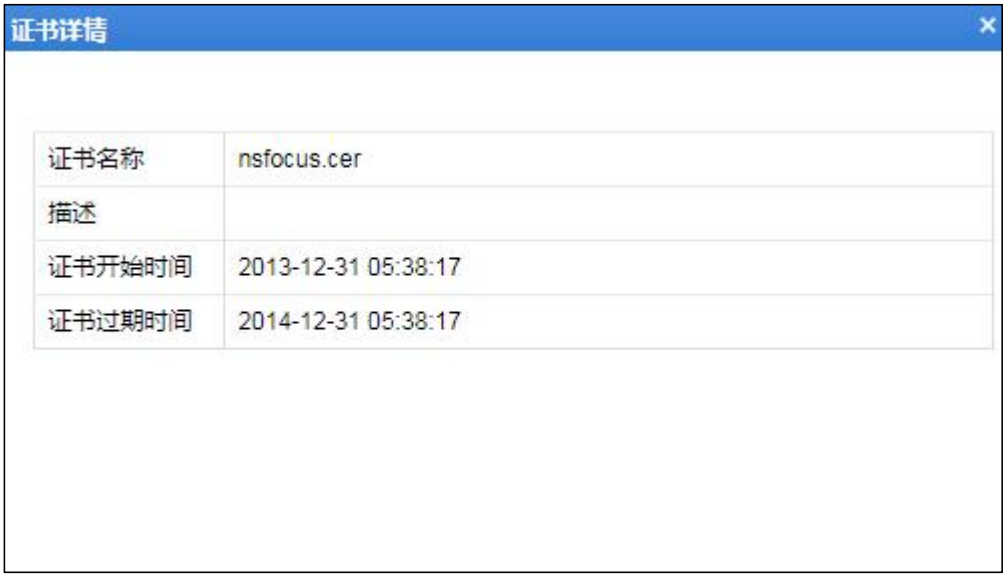
----结束

除导入证书外，管理员还可以进行查看、删除证书的操作。

4.10.1.2 查看证书

单击操作栏中的图标，弹出证书详情对话框，如图 4-119 所示。

图 4-106 证书详情



单击对话框右上角的图标，关闭证书详情。

4.10.1.3 删除证书

在证书列表中勾选需要删除的证书，单击【批量删除】按钮，确认删除后，删除相应证书。

4.10.2 XSD/WSDL 文件管理

新建/编辑 XML 攻击防护策略时，上传或选择的已有 XSD/WSDL 文件，都会在该页面显示。管理员也可以在该页面上上传或管理 XSD/WSDL 文件。

XSD 文件和 WSDL 文件分别支撑 WAF 设备进行 XML 攻击防护时的 Schema 校验和 SOAP 校验。

- XSD 文件

  XML Schema 语言也就是 XSD（XML Schemas Definition，XML 结构定义）。XML Schema 描述了 XML 文档的结构，可以用一个指定的 XML Schema 来验证某个 XML 文档，以检查该 XML 文档是否符合其要求。

- WSDL 文件

  WSDL（Web Services Description Language）作为 WebService 三要素之一，用于描述如何访问具体的接口。通常在 WebService 应用部署之前对 SOAP 消息进行验证，从而判断是否存在 XML 攻击。

下面详细介绍如何进行 XSD/WSDL 文件管理。

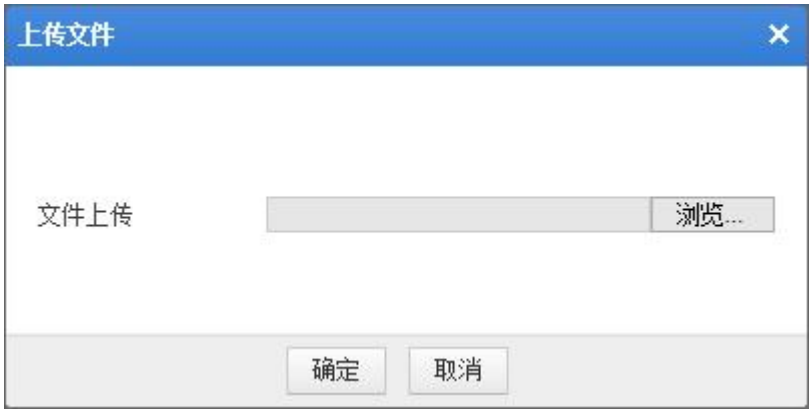
4.10.2.1 上传文件

步骤 1 选择菜单 **安全管理** > **上传文件管理** > **XSD/WSDL 文件管理**，进入 XSD/WSDL 文件管理页面，如图 4-120 所示。

图 4-107 XSD/WSDL 文件管理

步骤 2 单击【上传文件】按钮，弹出上传文件对话框，如图 4-121 所示。

图 4-108 上传 XSD/WSDL 文件



步骤 3 单击【浏览…】按钮，从本地选择 XSD/WSDL 文件，单击【确定】按钮，上传文件。

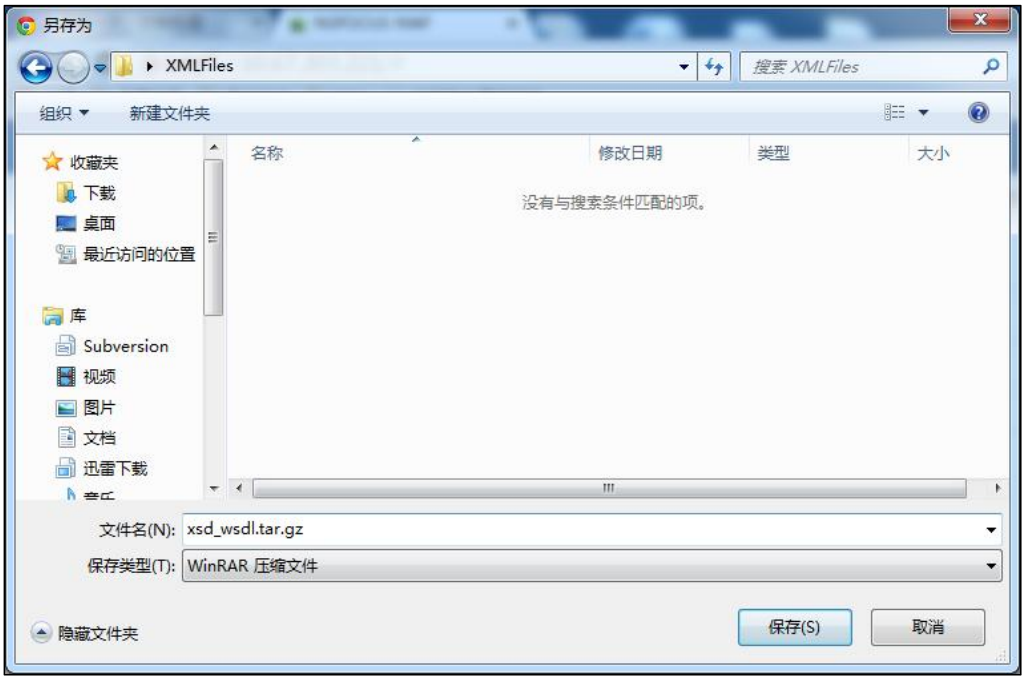
注意	上传 XSD/WSDL 文件时需注意以下几点： • 单个 XSD/WSDL 文件的大小不能超过 10M； • XSD/WSDL 文件的个数各不能超过 1000 个； • XSD/WSDL 文件的总大小不能超过 200M。

----结束

4.10.2.2 下载文件

单击图 4-120 中的【全部下载】按钮，WAF 会将文件列表中所有 XSD/WSDL 文件进行压缩后下载，默认文件名为：xsd_wsdl.tar.gz，如图 4-122 所示。

图 4-109 下载 XSD/WSDL 文件



注意	解压下载的文件时需要注意： • 若 XSD/WSDL 文件名为中文，请使用 tar 工具进行解压，否则会出现乱码； • 若 XSD/WSDL 文件名均为英文，则可以使用 WINRAR 工具解压。

4.10.2.3 删除文件

在删除文件前，建议做好备份工作，被删除的文件无法恢复，且策略也无法再引用该文件。

管理员可以删除已存在的且未被策略引用的 XSD/WSDL 文件，文件列表中“应用该文件的策略”一栏中显示有策略存在或“操作”一栏中没有图标，则表示该文件被策略引用不允许被删除，如图 4-120 所示。

- 单个删除

  单击文件列表“操作”一栏中的图标，删除相应的 XSD/WSDL 文件。

- 全部删除

  单击文件列表右上方的【全部删除】按钮，删除列表中所有未被策略引用的 XSD/WSDL 文件。

  全部删除功能只能删除未被策略引用的文件，即“应用该文件的策略”一栏中为空或操作一栏中有图标的文件。被策略引用的文件，即使单击【全部删除】按钮后，依然不会被删除。

4.10.3 伪装响应文件管理

配置策略时，动作选择“伪装”，需要选则已有的伪装响应文件或上传新的伪装响应文件。新上传的伪装响应文件和已有的伪装响应文件都在该页面中展示。管理员也可以在该页面上传或管理伪装响应文件。

4.10.3.1 上传文件

步骤 1 选择菜单 **安全管理** > **上传文件管理** > **伪装响应文件管理**，进入伪装响应文件管理页面，如图 4-123 所示。

图 4-110 伪装响应文件管理

步骤 2 单击【上传】按钮，弹出上传文件对话框。

步骤 3 单击【选择文件】按钮，从本地选择.gif 或.html 格式的伪装响应文件，单击【确定】按钮上传。

注意	上传伪装响应文件时需注意：.gif 格式的文件不能大于 20kb。

----结束

4.10.3.2 删除文件

在删除文件前，建议做好备份工作，被删除的文件无法恢复，且策略也无法再引用该文件。

管理员可以删除已存在的且未被策略引用的伪装响应文件，系统默认的伪装响应文件以及被策略引用的伪装响应文件不能被删除。

文件列表“操作”栏中显示“此文件已被应用于策略，不能删除”且“操作”栏中没有图标，则表示该文件被策略引用，如图 4-123 所示。

单击文件列表“操作”一栏中的图标，删除相应的伪装响应文件。

5 统计报表

本章介绍 WAF 提供的四类报表：

功能	描述
安全报表	介绍查看两种类型安全报表的方法。
流量报表	介绍查看流量报表的方法。
区域访问量统计报表	介绍查看区域访问量统计报表的方法。
PCI-DSS 合规报表	介绍查看 PCI-DSS 合规报表的方法。

5.1 安全报表

安全报表分为两种统计类型，分别是告警分类统计和告警时段统计。用户可通过选择站点、事件类型、统计周期和统计时间等条件获取需要的报表数据。

5.1.1 查看告警分类统计报表

步骤 1 选择菜单 **日志报表** > **安全报表** > **告警分类统计报表**，进入告警分类统计报表页面，如图 5-1 所示。

图 5-1 告警分类统计报表预览条件

步骤 2 配置告警分类统计报表参数，参数说明如表 5-1 所示。

表 5-1 告警分类统计报表参数说明

配置项	描述
站点	报表查看的目标站点。待选站点列表由系统根据用户的站点设置自动生成。 有关站点防护的详细操作请参见 4.3 站点防护。
周期类型	报表查看的时段，分为**日报**、**周报**和**月报**。

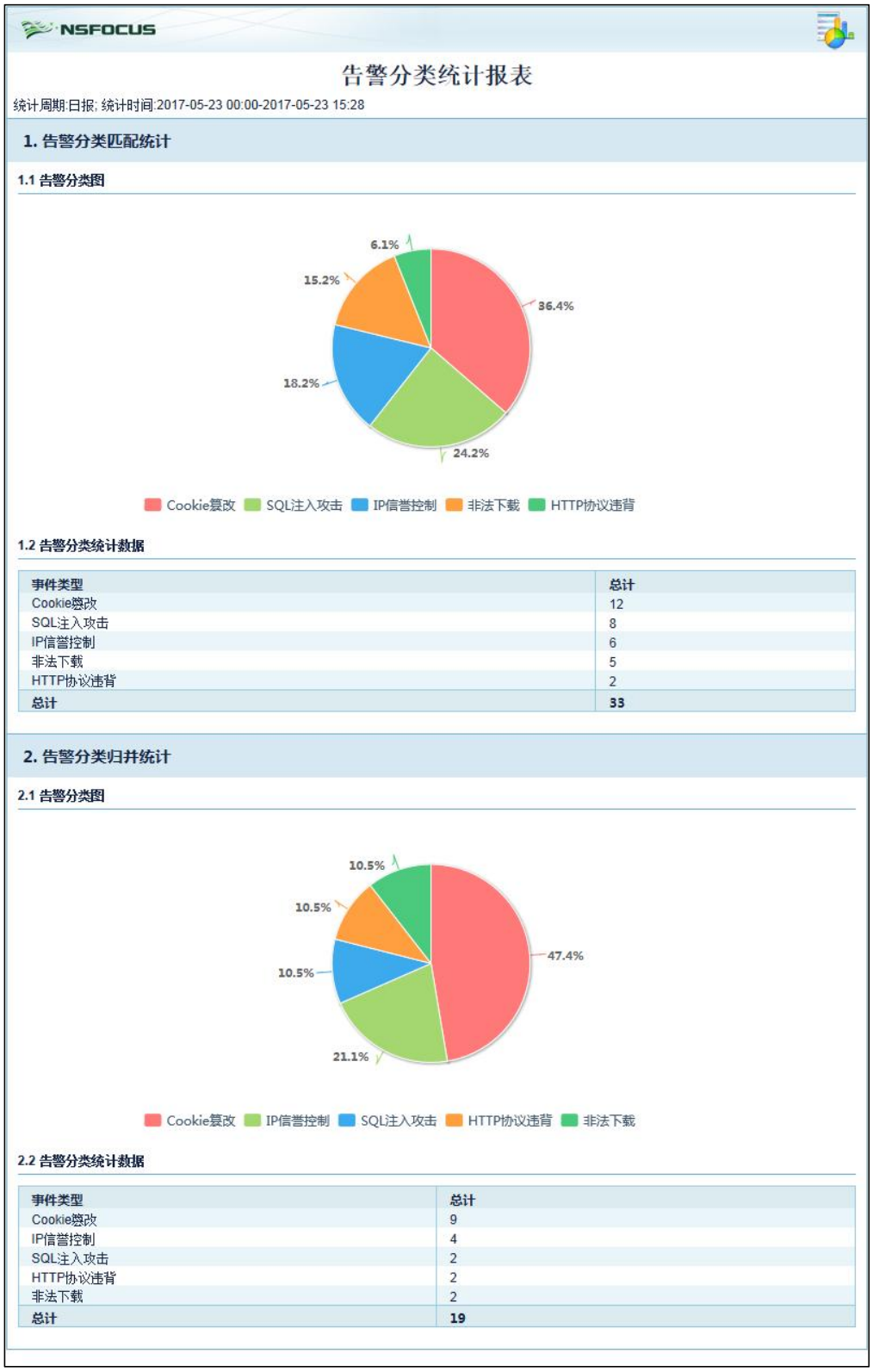
配置项	描述
日期	由用户自行设定与周期类型相对应的查看报表的时间段。

步骤 3 单击【生成】按钮，可得到目标站点在统计时间内受到的不同类型 Web 安全事件的统计信息。

以**全部站点**、**周报**为例，得到告警分类统计报表（包含告警分类匹配统计报表和告警分类归并统计报表），如图 5-2 所示。

- 告警分类匹配统计报表显示了统计时间内，不同类型 Web 安全事件的实际发生次数及其百分比。
- 告警分类归并统计报表中，WAF 每分钟对事件类型、服务器 IP、服务器端口、请求路径、客户端 IP、策略动作、告警级别、站点组均相同的 Web 安全事件归并一次，并在统计时间内累加，得到统计时间内不同类型 Web 安全事件归并后的次数及其百分比。

图 5-2 告警分类统计报表



NSFOCUS

告警分类统计报表

统计周期:日报; 统计时间:2017-05-23 00:00-2017-05-23 15:28

1. 告警分类匹配统计

1.1 告警分类图

1.2 告警分类统计数据

事件类型	总计
Cookie篡改	12
SQL注入攻击	8
IP信誉控制	6
非法下载	5
HTTP协议违背	2
总计	**33**

2. 告警分类归并统计

2.1 告警分类图

2.2 告警分类统计数据

事件类型	总计
Cookie篡改	9
IP信誉控制	4
SQL注入攻击	2
HTTP协议违背	2
非法下载	2
总计	**19**

步骤 4 （可选）单击图标，在弹出的报表导出对话框中设置报表参数，将 excel 格式的报表导出到本地。

步骤 5 （可选）单击图标，打印报表。

----结束

5.1.2 查看告警时段统计报表

步骤 1 选择菜单 **日志报表** > **安全报表** > **告警时段统计报表**，进入告警时段统计报表页面，如图 5-3 所示。

图 5-3 **告警时段统计报表预览条件**

步骤 2 配置告警时段统计报表参数，参数说明如表 5-2 所示。

表 5-2 **告警时段统计报表参数说明**

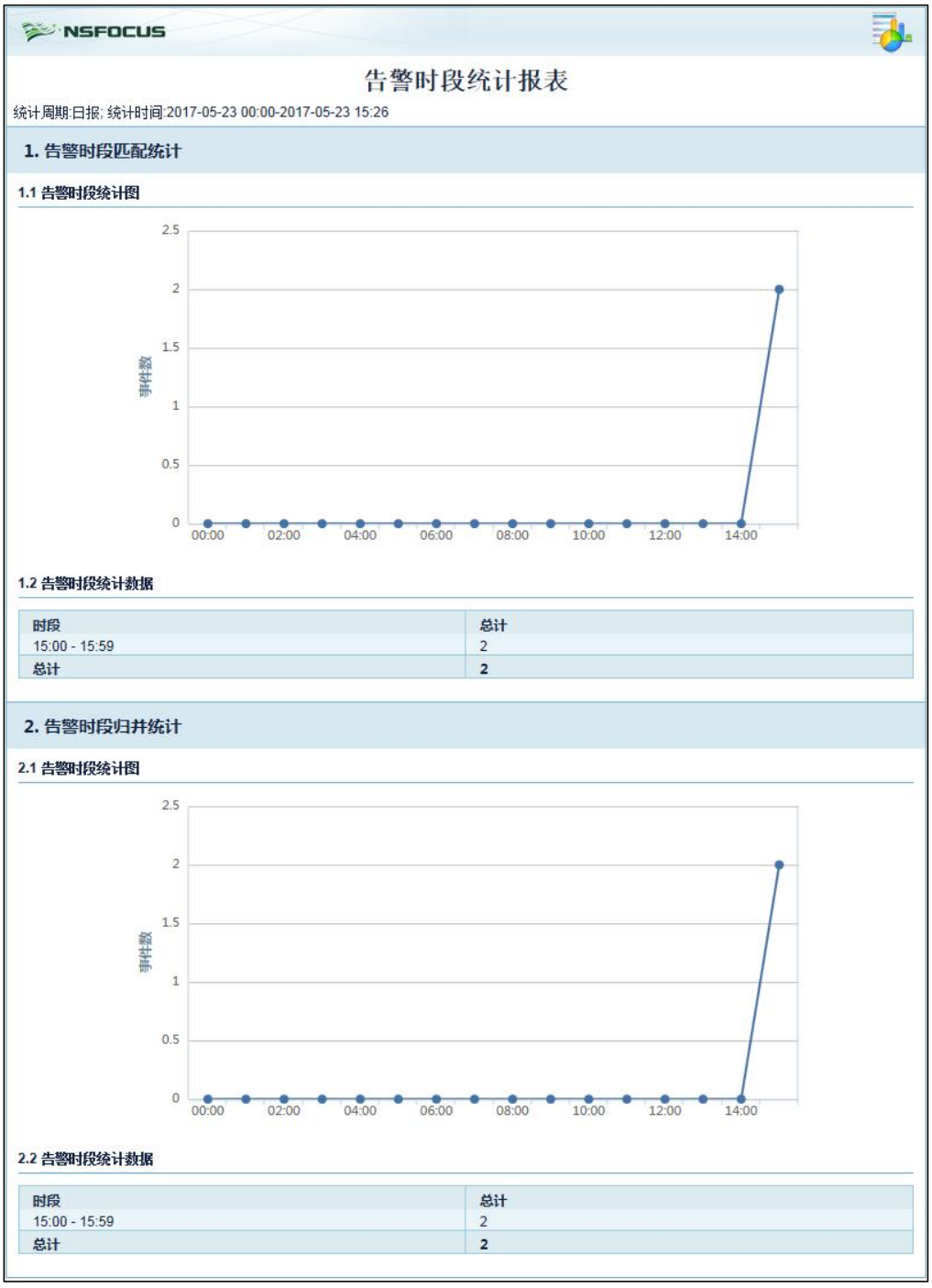
配置项	描述
事件类型	安全事件的类型，由系统内置。
周期类型	报表查看的时段，分为**日报**、**周报**和**月报**。
日期	由用户自行设定与周期类型相对应的查看报表的时间段。

步骤 3 单击【生成】按钮，即可得到在不同时间段内，不同类型的 Web 安全事件的统计信息。

以**全部事件类型**、**日报**为例，得到告警时段统计报表（告警时段匹配统计报表和告警时段归并统计报表），如图 5-4 所示。

- 告警时段匹配统计报表显示了不同时间段内不同类型 Web 安全事件的实际发生次数及其百分比。
- 告警时段归并统计报表中，WAF 每分钟对事件类型、服务器 IP、服务器端口、请求路径、客户端 IP、策略动作、告警级别、站点组均相同的 Web 安全事件归并一次，并分别在不同的时间段内累加，得到不同时间段内不同类型 Web 安全事件归并后的次数及其百分比。

图 5-4 告警时段统计报表



步骤 4 （可选）单击图标，在弹出的报表导出对话框中设置报表参数，将 excel 格式的报表导出到本地。

步骤 5 （可选）单击图标，打印报表。

----结束

5.2 流量报表

流量报表即流量趋势报表，按照设备引擎和接口流量统计信息。

步骤 1 选择菜单 **日志报表** > **流量报表** > **流量趋势报表**，进入流量趋势报表页面，如图 5-5 所示。

图 5-5 流量趋势报表预览条件

步骤 2 配置流量趋势报表参数，参数说明如表 5-3 所示。

表 5-3 流量趋势报表参数说明

配置项	描述
统计目标	流量趋势报表的统计目标，分为**引擎**和**接口**。 • **引擎**：统计客户端和服务器之间的流量。 • **接口**：统计流经所选接口的流量。
周期类型	报表查看的时段，分为**日报**、**周报**和**月报**。
日期	由用户自行设定与周期类型相对应的查看报表的时间段。

步骤 3 单击【生成】按钮，即可得到统计目标在一定时间段内的流量信息。

WAF 提供的流量统计有两种类型，分别是引擎流量统计和接口流量统计。

- 统计目标选择为“引擎”时，报表展示了客户端和服务器端的 Rx 和 Tx 两个方向的流量趋势图，并在数据列表中展示了具体的平均值、最大值、最小值，如图 5-6 所示。

图 5-6 引擎流量趋势报表

NSFOCUS

引擎流量趋势报表

统计周期:日报;统计时间:2017-05-23 00:00-2017-05-23 15:29;统计目标:引擎.

引擎流量趋势

1. 客户端 流量趋势图

2. 服务器端 流量趋势图

3. 引擎流量趋势数据

时间	客户端						服务器端					
	Rx(bps)			Tx(bps)			Rx(bps)			Tx(bps)		
	平均值	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值
13:00 - 13:59	0	0	0	0	0	0	0	0	0	0	0	0
14:00 - 14:59	31	150	0	49	419	0	49	419	0	12	74	0
15:00 - 15:59	33	145	0	3	16	0	3	16	0	8	39	0

- 统计目标选择为“接口”时，用户可以根据需要查看一个或多个接口，也可以选择查看所有接口的统计报表。报表展示所选接口的 Rx 和 Tx 方向的 bps 和 pps 趋势图，并在数据列表中列出了具体的平均值、最大值、最小值，如图 5-7 所示。

图 5-7 接口流量趋势报表

接口流量趋势报表

统计周期:日报;统计时间:2015-03-04 00:00-2015-03-04 16:50;统计目标(接口):G1/1.

接口流量趋势

1. bps趋势图

2. pps趋势图

3. 接口流量数据

时间	Rx						Tx					
	平均值		最大值		最小值		平均值		最大值		最小值	
	bps	pps	bps	pps	bps	pps	bps	pps	bps	pps	bps	pps
00:00 - 00:59	34.3K	19	297.3K	45	9.2K	15	1.6K	2	16.3K	20	0	0
01:00 - 01:59	10K	16	11.6K	18	8.9K	14	105	0	266	0	0	0
02:00 - 02:59	10.5K	16	13K	18	8.9K	14	81	0	284	0	0	0
03:00 - 03:59	11.1K	17	14.2K	20	9.5K	15	99	0	244	0	0	0
04:00 - 04:59	11.3K	18	15.4K	22	8.2K	14	101	0	375	0	0	0
05:00 - 05:59	11K	17	17.1K	21	9.2K	15	85	0	249	0	0	0
06:00 - 06:59	10.4K	16	12.8K	19	8.8K	14	92	0	248	0	0	0
07:00 - 07:59	10.1K	16	11.6K	17	8.8K	14	149	0	444	0	0	0
08:00 - 08:59	12.4K	18	17.4K	25	9.3K	15	90	0	251	0	0	0
09:00 - 09:59	21.2K	26	27.8K	33	13.5K	20	112	0	295	0	2	0
10:00 - 10:59	30.8K	36	45.8K	71	24.4K	26	131	0	376	0	18	0
11:00 - 11:59	43.6K	48	74.8K	112	25.2K	26	199	0	1.1K	2	9	0
12:00 - 12:59	39.2K	38	105.6K	164	20.3K	21	204	0	977	0	2	0
13:00 - 13:59	80.3K	51	336.4K	255	14.4K	20	589	0	3.7K	2	0	0
14:00 - 14:59	41.1K	33	48.8K	37	32.5K	29	271	0	326	0	224	0
15:00 - 15:59	66.3K	82	141.4K	236	31.5K	32	280	0	320	0	239	0
16:00 - 16:59	68.3K	95	111.3K	202	35.4K	29	289	0	346	0	212	0

步骤 4 （可选）单击图标，在弹出的报表导出对话框中设置报表参数，将 excel 格式的报表导出到本地。

步骤 5 （可选）单击图标，打印报表。

----结束

5.3 区域访问量统计报表

区域访问量统计报表的数据来源是虚拟站点，必须开启虚拟站点的区域访问量统计功能，统计报表才会有数据。开启虚拟站点的访问量统计操作请参见 4.3.3 管理虚拟站点。

步骤 1 选择菜单 **日志报表** > **区域访问量统计报表**，进入区域访问量统计报表页面，如图 5-8 所示。

图 5-8 区域访问量统计报表预览条件

步骤 2 配置区域访问量统计报表参数，参数说明如表 5-4 所示。

表 5-4 区域访问量统计报表参数说明

配置项	描述
站点资源	统计时间范围内已有统计数据的虚拟站点列表以及全局。
周期类型	报表查看的时段，分为**日报**、**周报**和**月报**。
日期	与周期类型相对应的查看报表的时间段。
区域范围	统计的区域范围，可选项为：**全球**、**大中华区**、**美国**和**日本**。

步骤 3 单击【生成】按钮，即可得到目标区域在一定时间段内的访问量统计信息。

以站点资源选择**全局**、周期类型选择**日报**、区域范围选择**大中华区**为例，得到的区域访问量统计报表如图 5-9 所示。

图 5-9 区域访问量统计报表

步骤 4 （可选）单击图标，在弹出的报表导出对话框中设置报表参数，将 excel 格式的报表导出到本地。

步骤 5 （可选）单击图标，打印报表。

----结束

5.4 PCI-DSS 合规报表

PCI-DSS 合规报表是 WAF 基于支付卡行业资料安全标准、对指定站点的配置进行 PCI-DSS 合规检验，将检验结果输出为 HTML 格式的 PCI-DSS 合规性报表，并对部分满足或不满足 PCI 要求的配置提供建议或解决方案。其中检验的主要内容有站点的防护状态及策略、WAF 工作口的状态及工作模式等。

当管理员为站点配置防护策略后，可通过生成 PCI-DSS 合规报表来查看不满足 PCI 合规的配置，以便管理员及时调整站点的配置，提升防护效果。

生成报表

WAF 最多支持存储 100 份 PCI-DSS 合规报表，超过 100 份时，必须删除现有报表，才能生成新的报表。WAF 执行完报表生成功能后，需要单击报表列表右上角的【刷新】，手动刷新当前页面展示的报表生成状态。

生成报表的操作如下：

步骤 1 选择菜单 **日志报表 > PCI-DSS 合规报表**，进入 PCI-DSS 合规报表页面，如图 5-10 所示。

图 5-10 PCI-DSS 合规报表预览条件

步骤 2 配置 PCI-DSS 合规报表参数，参数说明如表 5-5 所示。

表 5-5 PCI-DSS 合规报表参数说明

配置项	描述
报表名称	PCI-DSS 合规报表的名称，默认为 default。
选择站点	选择进行 PCI 合规检验的站点，可选择单个或多个。

步骤 3 单击【生成】按钮，WAF 自动在后台生成报表，并在图 5-10 所示的报表列表中自动生成对应的报表信息。

----结束

下载报表

在图 5-10 所示的报表列表的“操作”栏中，单击图标  ，在弹出的文件下载对话框中选择【保存】，下载 HTML 报表文件到本地。

查看报表

只有将 PCI-DSS 合规报表下载到本地后才能查看。在本地使用浏览器打开相应的报表文件，如图 5-11 所示。WAF 对部分满足或不满足 PCI 要求的配置提供了解决方案。

管理员可以根据该报表调整站点的配置，从而更有效的提升 WAF 对站点的防护。

图 5-11 查看 PCI-DSS 合规报表

WEB应用防护系统PCI-DSS合规性报表

报表生成时间: 2016-08-17 15:21:10

报表说明：本报表遵照《支付卡行业(PCI)资料安全标准》3.2版本。本报表只为您评估程序，它不能替代由资格认证机构QSA/ASV发布的PCI审计报告。

站点组名称: default
站点名称: default_v4
IP: 10.68.2.204-10.68.2.204
端口: 80
合规校验结果:

PCI 章节	PCI 要求	完全满足	部分满足	不满足	解决方案
2.3	使用强效加密对所有非主控台管理的存取进行加密。对于基于Web的管理和其他非控制台管理的存取使用诸如SSH、VPN、SSL/TLS等技术。			是	请确保站点的"服务器类型"配置为HTTPS。
3.3	显示PAN时予以掩盖（最多显示前六位和后四位数字），这样仅具有正当业务需要者方可看到完整的PAN。			是	请确保站点所在的站点组启用了"敏感信息过滤"策略，策略动作为阻断/替换；如果策略动作为替换，则策略配置需满足"最多显示前六位和后四位数字"的约束条件。
4.1	使用强效加密和安全协定（例如，SSL/TLS、IPSEC、SSH等）以便在开放的公用网络传输期间保护敏感的持卡人资料。			是	请确保站点的"服务器类型"配置为HTTPS。
6.1	制定一项程序，确定并指派新发现安全漏洞的风险排名。	是			WAF支持手动升级规则库功能，并且每条规则按照危害等级分为高、中、低，在WAF防护下的站点都符合此规范。
6.5.1	注入式漏洞，特别是 SQL 注入，同时还需考虑OS 指令注入、LDAP与Xpath注入式漏洞以及其他注入式漏洞。		是		请确保站点所在的站点组启用了通用防护策略，策略动作为阻断/重定向/伪装，策略覆盖了所有SQL注入防护、LDAP注入防护、Xpath注入防护、命令行注入防护规则。
6.5.2	缓冲区溢出		是		请确保站点所在的站点组启用了以下策略：（1）"HTTP协议校验"策略，（2）"Web服务器插件防护"策略。"HTTP协议校验"策略中配置了相关极限值（最大长度/最大个数）。"Web服务器插件防护"策略中需要从"Web服务器漏

删除报表

在图 5-10 所示 PCI-DSS 合规报表列表中，可以删除单个报表，也可以批量删除多个报表。

- 单个删除

  在图 5-10 所示界面中，单击某个报表“操作”一栏的删除图标，弹出删除确认窗口，然后单击该窗口中的【确定】按钮，即可删除该报表。

- 批量删除

  在图 5-10 所示界面中，选中一个或多个报表左侧的复选框，然后单击报表列表右上方的【批量删除】按钮，弹出删除确认窗口，单击该窗口中的【确定】按钮，即可删除被选中的所有报表。

说明	无论是开始生成、结束生成、下载、删除 PCI 合规报表均会记录操作日志，请使用审计员账户登录 WAF 的 Web 界面进行查看。

6 日志分析

本章介绍系统中各类日志的详细信息，其中登录日志和操作日志属于审计日志，只有审计员有权限查看；其他日志信息只有管理员和被管理员授权的普通用户可以查看。有关审计员、管理员的帐号初始信息请参见**错误!未找到引用源。错误!未找到引用源。**。

具体包括以下内容：

功能	描述
查看安全防护日志	查看 WAF 对被保护服务器的安全防护日志信息。包括网络层访问控制日志、DDoS 防护日志、Web 安全日志、高危 IP 阻断日志、Web 防篡改日志、ARP 防护日志、Web 访问日志以及会话追踪日志。
查看流量控制日志	查看 WAF 对流量控制对象限流的日志信息。
查看系统运行日志	查看系统运行状态的日志信息。
查看登录日志	查看管理员、审计员等各类用户的登录日志信息。
查看操作日志	查看管理员、审计员等各类用户的操作日志信息。
日志管理配置	配置系统日志的导出备份、发送等参数。

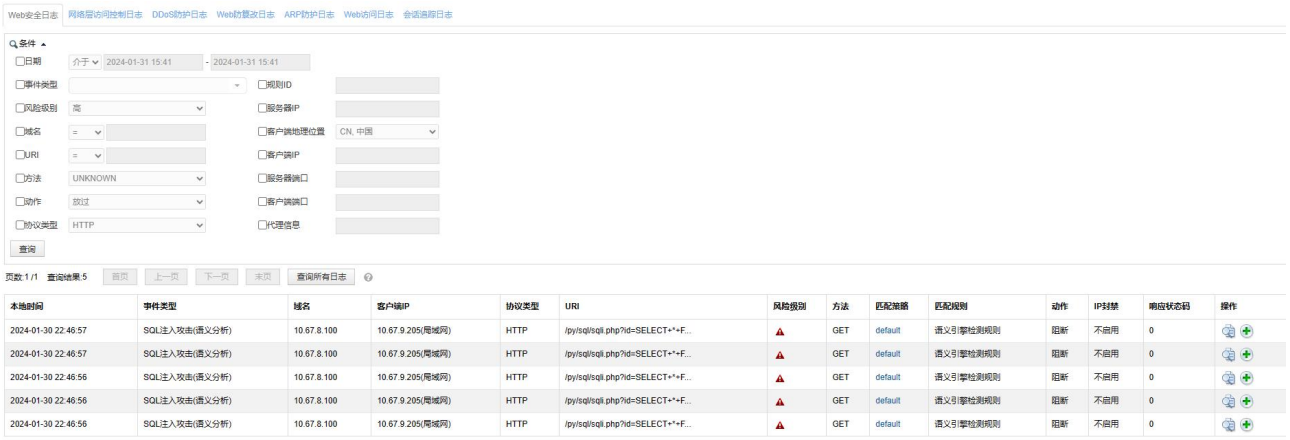
6.1 查看安全防护日志

安全防护日志包括 Web 安全日志、网络层访问控制日志、DDoS 防护日志、Web 防篡改日志、ARP 防护日志、Web 访问日志和会话追踪日志。

6.1.1 查看 Web 安全日志

步骤 1 选择菜单 **日志报表** > **安全防护日志** > **Web 安全日志**，进入 Web 安全日志页面，如图 6-1 所示。

图 6-1 Web 安全日志



默认情况下，Web 安全日志只显示最新的 1000 条符合查询条件的日志，如需查询所有日志，请单击【查询所有日志】按钮。

步骤 2 勾选并配置 Web 安全日志查询参数，参数说明如表 6-1 所示。

表 6-1 Web 安全日志参数说明

配置项	描述
日期	查询 Web 安全日志的时间段。 • <=：查询所设定时间之前的 Web 安全事件信息。 • >=：查询所设定时间至当前时间内的 Web 安全事件信息。 • **介于**：查询所设定起止时间内的 Web 安全事件信息。
事件类型	Web 安全事件类型，如 HTTP 协议校验、SQL 注入攻击等。
风险级别	Web 安全事件的风险级别，分为**高**、**中**、**低**三种级别。
域名	Web 安全事件对应的域名字段。域名同时支持精确查询和模糊查询： • =：表示精确查询； • >=：表示模糊查询； • !=：查询时不进行匹配的内容。
URI	Web 安全事件对应的 URL 路径字段。URI 同时支持精确查询和模糊查询： • =：表示精确查询； • >=：表示模糊查询； • !=：查询时不进行匹配的内容。
服务器/客户端 IP	Web 安全事件对应的服务器/客户端 IP。
服务器/客户端端口	Web 安全事件对应的服务器/客户端端口。
客户端地理位置	Web 安全事件对应的客户端所在的地理位置信息。
动作	WAF 针对 Web 安全事件采取的 HTTP 策略动作，分为**放过**、**阻断**、**接受**、**重定向**、**伪装**、**清除**、**替换**和**验证码**。。
方法	Web 安全事件的 HTTP 请求方法，如 GET、POST 等。
代理信息	根据代理信息进行查询，有关代理信息的介绍请参见 4.10 代理信息配置。
协议类型	Web 安全事件对应的协议类型。

步骤 3 单击【查询】按钮，即可得到符合条件的 Web 安全日志。

- 单击 Web 安全日志列表“匹配策略”栏中的策略名称，查看该通用防护策略的详情。
- 单击 Web 安全日志列表“匹配规则”栏中的规则名称，查看该通用防护策略引用的规则的详情。
- 单击 Web 安全日志列表“操作”栏中的图标，查看该条 Web 安全日志对应的站点 ID、HTTP 请求/响应信息等日志详情。
- 单击 Web 安全日志列表“操作”栏中的图标，选择“会话标识追踪”或“浏览器标识追踪”，跳转到会话追踪日志页面查看该条 Web 安全日志对应的会话追踪日志。会话追踪日志的查看操作请参见 6.1.7 查看会话追踪日志。

步骤 4 （可选）添加策略。

- 单击 Web 安全日志列表“操作”栏中的图标，选择“添加到例外策略”，弹出新建例外策略对话框，新建例外策略的详细步骤请参见 4.7.5.1 配置例外策略。
- 单击 Web 安全日志列表“操作”栏中的图标，选择“添加到风险级别策略”，弹出新建风险级别策略对话框，新建风险级别策略的详细步骤请参见 4.7.5.3 配置风险级别策略。

----结束

6.1.2 查看网络层访问控制日志

步骤 1 选择菜单 **日志报表** > **安全防护日志** > **网络层访问控制日志**，进入网络层访问控制日志页面，如图 6-2 所示。

图 6-2 网络层访问控制日志

步骤 2 配置网络层访问控制日志查询参数，参数说明如表 6-2 所示。

表 6-2 网络层访问控制日志参数说明

配置项	描述
日期	查询网络层访问控制日志的时间段。 • **<=**：查询所设定时间之前的网络层访问控制信息。 • **>=**：查询所设定时间至当前时间内的网络层访问控制信息。 • **介于**：查询所设定起止时间内的网络层访问控制信息。
服务器/客户端 IP	发生网络层访问控制事件的服务器/客户端 IP 地址，IP 地址支持 IPv4 和 IPv6。
服务器/客户端端口	发生网络层访问控制事件的服务器/客户端端口。
策略 ID	针对网络层访问的控制策略 ID。
匹配次数	与该条安全信息相匹配的网络层访问次数。
动作	WAF 对网络层访问控制事件的处理方式，分为**转发**、**阻断**、**接受**三种情况。 • **转发**：当前数据包不再经过后续检测，转发当前数据包。 • **阻断**：丢弃当前数据包，同时关闭当前的 TCP 连接。 • **接受**：不采取任何处理使当前数据包继续后续检测。
协议	网络层访问采用的协议，可选项为**不限**、**ICMP**、**ICMPV6**、**TCP** 和 **UDP**。

步骤 3 单击【查询】按钮，即可得到符合条件的网络层访问控制信息。

----结束

6.1.3 查看 DDoS 防护日志

步骤 1 选择菜单 **日志报表** > **安全防护日志** > **DDoS 防护日志**，进入 DDoS 防护日志页面，如图 6-3 所示。

图 6-3 DDoS 防护日志

步骤 2 配置 DDoS 防护日志查询参数，参数说明如表 6-3 所示。

表 6-3 DDoS 防护日志参数说明

配置项	描述
日期	查询 DDoS 防护日志的时间段。 • **<=**：查询所设定时间之前的 DDoS 防护信息。 • **>=**：查询所设定时间至当前时间内的 DDoS 防护信息。 • **介于**：查询所设定起止时间内的 DDoS 防护信息。
事件类型	DDoS 攻击类型，包括 **SYN Flood**、**ACK Flood**、**HTTP Flood** 和**联动事件**
动作	WAF 针对 DDoS 攻击采取的处理方式，分为**进入防护状态**、**退出防护状态**、**触发牵引阈值**、**ADS 启用防护**、**WAF 启用防护**
服务器 IP/端口	发生 DDoS 攻击的服务器 IP 地址/端口，IP 地址支持 IPv4 和 IPv6。

步骤 3 单击【查询】按钮，即可得到符合条件的 DDoS 防护日志。

----结束

6.1.4 查看 Web 防篡改日志

步骤 1 选择菜单 **日志报表** > **安全防护日志** > **Web 防篡改日志**，进入 Web 防篡改日志页面，如图 6-4 所示。

图 6-4 Web 防篡改日志

步骤 2 配置 Web 防篡改日志查询参数，参数说明如表 6-4 所示。

表 6-4 Web 防篡改日志参数说明

配置项	描述
日期	查询 Web 防篡改日志的时间段，可选项有<=、>=和**介于**。 <=：查询所设定时间之前的 Web 防篡改事件信息。 >=：查询所设定时间至当前时间内的 Web 防篡改事件信息。 • **介于**：查询所设定起止时间内的 Web 防篡改事件信息。
URL	Web 防篡改事件对应的 URL 路径字段。URL 同时支持精确查询和模糊查询： • =：表示精确查询； • >=：表示模糊查询； • !=：查询时不进行匹配的内容。
服务器 IP/端口	Web 防篡改事件对应的服务器 IP 地址/端口，IP 地址支持 IPv4 和 IPv6。

步骤 3 单击【查询】按钮，即可得到符合条件的 Web 防篡改日志。

----结束

6.1.5 查看 ARP 防护日志

步骤 1 选择菜单 **日志报表** > **安全防护日志** > **ARP 防护日志**，进入 ARP 防护日志页面，如图 6-5 所示。

图 6-5 ARP 防护日志

步骤 2 配置 ARP 防护日志查询参数，参数说明如表 6-5 所示。

表 6-5 ARP 防护日志参数说明

配置项	描述
日期	查询 ARP 防护日志的时间段。 • **<=**：查询所设定时间之前的 ARP 防护事件信息。 • **>=**：查询所设定时间至当前时间内的 ARP 防护事件信息。 • **介于**：查询所设定起止时间内的 ARP 防护事件信息。
攻击类型	有三种攻击类型：**非法 ARP 包**、**MAC 冲突**、**网关型 ARP 欺骗**。
源/目标 IP	ARP 请求的源/目标 IP 地址。
源/目标 MAC	ARP 请求的源/目标 MAC 地址。
绑定 IP/MAC	绑定的被代理服务器或网关的 IP/MAC 地址。有关绑定 IP/MAC 的操作请参见 4.2.4 配置 ARP 欺骗防护。
冲突 MAC	ARP 攻击中与系统自学习 MAC 表或绑定 MAC 相冲突的 MAC 地址，即 ARP 攻击来源主机或服务器的 MAC 地址。
匹配次数	与该条安全信息相匹配的 ARP 攻击次数。
动作	WAF 针对 ARP 攻击采取的处理方式，分为**放过**、**阻断**、**接受**和**重定向**四种方式。
状态	ARP 攻击状态，分为**正在尝试**和**攻击成功**。

步骤 3 单击【查询】按钮，即可得到符合条件的 ARP 防护日志。

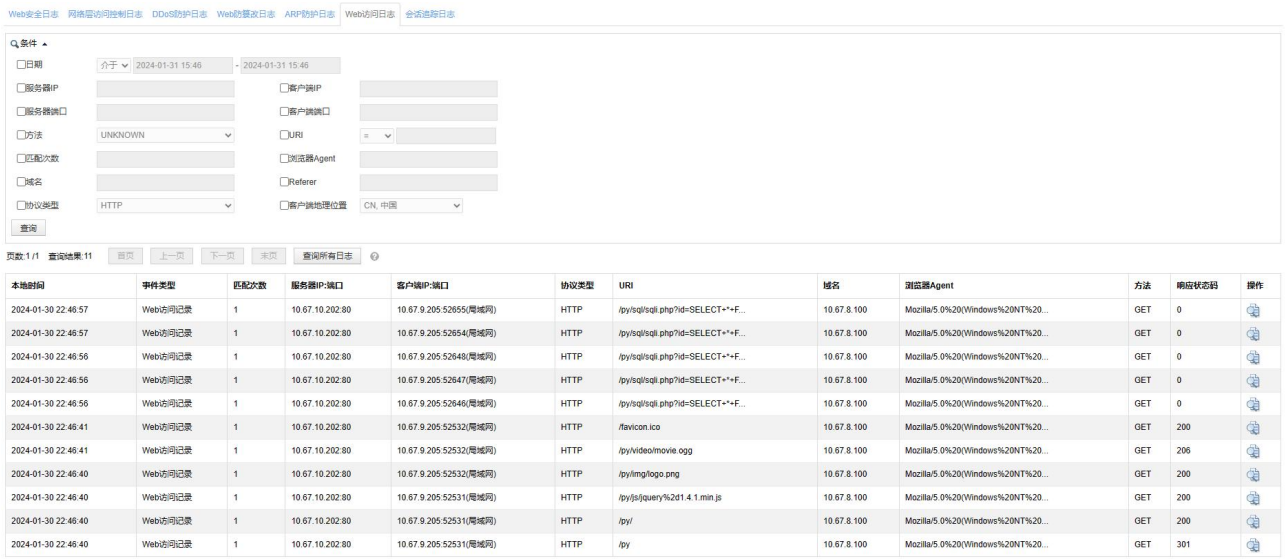
----结束

6.1.6 查看 Web 访问日志

只有站点开启了 Web 访问日志功能，才能在 Web 访问日志中查看对应站点的 Web 访问日志。有关开启 Web 访问日志的介绍请参见 4.3.1.1 新建站点组。

步骤 1 选择菜单 **日志报表 > 安全防护日志 > Web 访问日志**，进入 Web 访问日志页面，如图 6-6 所示。

图 6-6 Web 访问日志



默认情况下，Web 访问日志只显示最新的 1000 条符合查询条件的日志，如需查询所有日志，请单击【查询所有日志】按钮。

步骤 2 配置 Web 访问日志查询参数，参数说明如表 6-6 所示。

表 6-6 Web 访问日志参数说明

配置项	描述
日期	查询 Web 访问日志的时间段。 • <=：查询所设定时间之前的 Web 访问信息。 • >=：查询所设定时间至当前时间内的 Web 访问信息。 • 介于：查询所设定起止时间内的 Web 访问信息。
服务器/客户端 IP	Web 访问事件对应的服务器/客户端 IP 地址，IP 地址支持 IPv4 和 IPv6。
服务器/客户端端口	Web 访问事件对应的服务器/客户端端口。
方法	Web 访问事件的 HTTP 请求方法，如 GET、POST 等。
URI	Web 访问事件对应的 URL 路径字段。URI 同时支持精确查询和模糊查询： • =：表示精确查询； • >=：表示模糊查询； • !=：查询时不进行匹配的内容。
匹配次数	与该条安全信息相匹配的 Web 访问次数。
浏览器 Agent	Web 访问事件对应的浏览器信息。
域名	Web 访问事件对应的域名。
Referer	Web 访问事件对应的 referer 内容。
协议类型	Web 访问事件对应的协议类型。
客户端地理位置	Web 访问事件对应的客户端所在的地理位置信息。

步骤 3 单击【查询】按钮，即可得到符合条件的 Web 访问日志。

步骤 4 （可选）日志操作。

- 单击 Web 访问日志列表“操作”栏中的图标，查看该条 Web 访问日志对应的站点 ID、访问日期等日志详情。
- 单击 Web 访问日志列表“操作”栏中的图标，选择“会话标识追踪”或“浏览器标识追踪”，跳转到会话追踪日志页面查看该条 Web 访问日志对应的会话追踪日志。会话追踪日志的查看操作请参见 6.1.7 查看会话追踪日志。

----结束

6.1.7 查看会话追踪日志

步骤 1 选择菜单 **日志报表** > **安全防护日志** > **会话追踪日志**，进入会话追踪日志页面，如图 6-7 所示。

图 6-7 会话追踪日志

步骤 2 配置会话追踪日志查询参数，参数说明如表 6-7 所示。

表 6-7 会话追踪日志参数说明

配置项	描述
日期	查询会话追踪日志的时间段。 • **<=**：查询所设定时间之前的会话追踪信息。 • **>=**：查询所设定时间至当前时间内的会话追踪信息。 • **介于**：查询所设定起止时间内的会话追踪信息。
事件类型	会话追踪事件类型，如数据安全传输、SQL 注入攻击等。
URL	会话追踪事件对应的 URL 路径字段。URI 同时支持精确查询和模糊查询： • **=**：表示精确查询； • **>=**：表示模糊查询； • **!=**：查询时不进行匹配的内容。
协议类型	会话采用的协议，可选项有：HTTP 和 HTTPS。
用户名	会话追踪事件对应的用户名称。
浏览器 Agent	会话追踪事件对应的浏览器信息。
会话标识	会话追踪事件对应的会话标识，即由 WAF 下发的会话标识 WSI。
浏览器标识	会话追踪事件对应的浏览器标识，即由 WAF 下发的浏览器标识 WCI。

配置项	描述
服务器 IP/端口	会话追踪事件对应的服务器/客户端 IP 地址，IP 地址支持 IPv4 和 IPv6。
客户端地理位置	会话追踪事件对应的客户端所在地理位置信息。

步骤 3 单击【查询】按钮，即可得到符合条件的会话追踪日志。

----结束

6.2 查看流量控制日志

流量控制日志仅当 WAF 设备部署方式为反向代理时产生。

步骤 1 选择菜单 **日志报表** > **流量控制日志**，进入流量控制日志页面，如图 6-8 所示。

图 6-8 流量控制日志

步骤 2 配置流量控制日志查询参数，参数说明如表 6-8 所示。

表 6-8 流量控制日志参数说明

配置项	描述
实际上行速率	流量控制对象的实际上行速率，大于、等于或小于指定的阈值。
实际下行速率	流量控制对象的实际下行速率，大于、等于或小于指定的阈值。
限流对象阈值	进行流量限制的阈值，大于、等于或小于指定的阈值。
限流对象名称	流量控制对象的名称关键字。
事件类型	限流状态的类型，分为**开始限流**和**结束限流**。
日期	查询流量控制日志的时间段。 • **<=**：查询所设定时间之前的流量控制状态信息。 • **>=**：查询所设定时间至当前时间内的流量控制状态信息。 • **介于**：查询所设定起止时间内的流量控制状态信息。

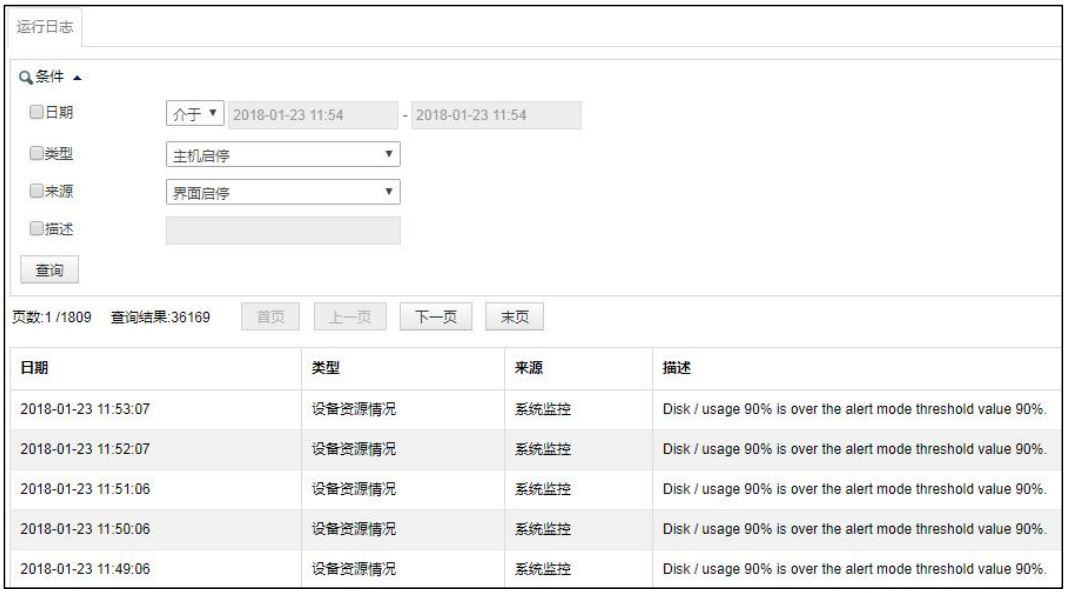
步骤 3 单击【查询】按钮，即可查看一定时间段内的流量控制日志信息。

----结束

6.3 查看系统运行日志

步骤 1 选择菜单 **日志报表** > **系统运行日志** > **运行日志**，进入系统运行日志页面，如图 6-9 所示。

图 6-9 系统运行日志



步骤 2 配置系统运行日志查询参数，参数说明如表 6-9 所示。

表 6-9 系统运行日志参数说明

配置项	描述
日期	查询系统运行日志的时间段，可选项有<=、>=和**介于**。 • **<=**：查询所设定时间之前的系统运行状态信息。 • **>=**：查询所设定时间至当前时间内的系统运行状态信息。 • **介于**：查询所设定起止时间内的系统运行状态信息。
类型	系统运行状态变化的类型，分为**主机启停**、**服务启停**、**数据库启停**、**引擎启停**、**WEB 服务启停**、**链路状态变化**、**紧急模式切换**、**ADS 联动事件**、**规则升级**和**设备资源情况**。
来源	系统运行状态变化的操作源，可选项有**界面启停**、**系统正常启停**、**引擎启停**和**系统监控**。
描述	对系统运行状态变化的详细描述。

步骤 3 单击【查询】按钮，即可查看一定时间段内不同类型的系统运行状态变化信息。

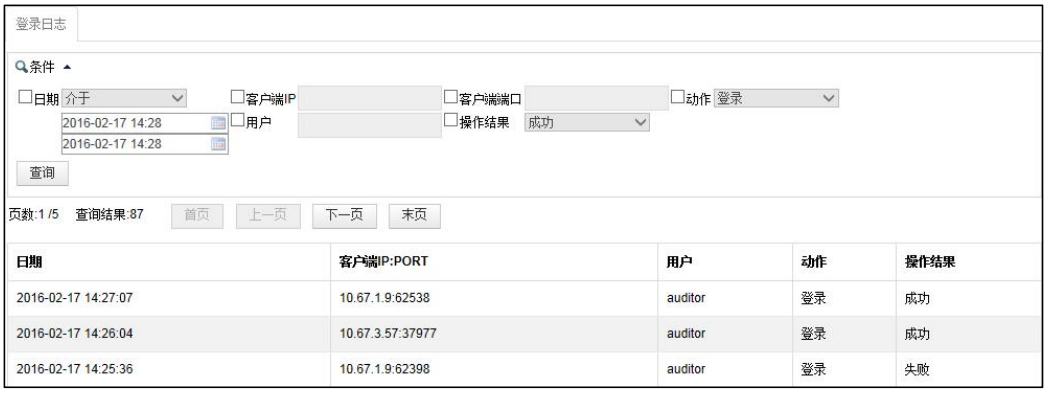
----结束

6.4 查看登录日志

审计用户成功登录后，可以查看审计员、管理员等各类用户的登录日志信息。

步骤 1 选择菜单 **审计日志** > **登录日志** > **登录日志**，进入查看登录日志页面，如图 6-10 所示。

图 6-10 登录日志信息



步骤 2 配置登录日志查询参数，参数说明如表 6-10 所示。

表 6-10 登录日志信息参数说明

配置项	描述
日期	查询登录日志的时间段。 • **<=**：查询所设定时间之前的登录日志信息。 • **>=**：查询所设定时间至当前时间内的登录日志信息。 • **介于**：查询所设定起止时间内的登录日志信息。
客户端 IP	登录 WAF Web 管理界面的客户端 IP 地址，IP 地址支持 IPv4 和 IPv6。
用户	登录 WAF Web 管理界面的用户。
客户端端口	登录 WAF Web 管理界面的客户端端口号。
操作结果	用户的登录/退出操作结果：**成功**或**失败**。
动作	用户对 WAF Web 管理界面的**登录**或**退出**操作。

步骤 3 单击【查询】按钮，即可得到符合条件的登录日志信息。

----结束

6.5 查看操作日志

审计用户成功登录后，可以查看审计员、管理员等各类用户对 WAF 系统的操作日志信息。

步骤 1 选择菜单 **审计日志** > **操作日志** > **操作日志**，进入查看操作日志页面，如图 6-11 所示。

图 6-11 操作日志信息

步骤 2 配置操作日志信息查询参数，参数说明如表 6-11 所示。

表 6-11 操作日志信息参数说明

配置项	描述
日期	查询操作日志的时间段。 • **<=**：查询所设定时间之前的操作日志信息。 • **>=**：查询所设定时间至当前时间内的操作日志信息。 • **介于**：查询所设定起止时间内的操作日志信息。
客户端 IP	通过 Web 管理界面对 WAF 系统进行操作的客户端 IP 地址，IP 地址支持 IPv4 和 IPv6。
用户	通过 Web 管理界面对 WAF 系统进行操作的用户。
操作类型	用户的操作类型，包括**系统启停**、**许可证更新**、**系统升级**、**系统配置**、**安全配置**、**用户管理**、**日志报表**和**测试工具**。
操作结果	用户的操作结果：**成功**或**失败**。

步骤 3 单击【查询】按钮，即可得到符合条件的操作日志信息。

----结束

6.6 导出日志

审计用户成功登录后，不仅可以查看审计员、管理员等各类用户的登录日志信息和对 WAF 系统的操作日志信息，还可以导出日志信息并进行下载及清除操作。

选择菜单 **审计日志** > **导出日志** > **导出日志**，进入导出日志页面，如图 6-12 所示。

图 6-12 导出日志

导出日志

定期导出日志是清理存储空间的一种方式，即将日志以文件的形式存储到其他存储介质，进行永久保存。

在图 6-12 所示页面中，根据需要单击不同日志类型对应“操作”栏中的导出按钮，将 WAF 服务器数据库中的日志信息打包成日志文件存放在 WAF 服务器目录中。

以登录日志为例：

- 单击【分时导出】按钮，选择导出日志的时间段，在弹出的对话框中单击【开始导出】按钮后，开始导出日志，导出的日志将显示在相应日志类型的“下载”栏中。
- 单击【全部导出】按钮，自动导出当前该类日志的所有信息，导出的日志将显示在相应日志类型的“下载”栏中。

下载日志

WAF 支持将导出的日志下载至本地。在图 6-12 所示页面中，根据需要单击导出的日志文件，可将打包的日志文件保存至本地。

清除日志文件

在图 6-12 所示页面，根据需要单击不同日志类型对应“操作”栏中的【清除文件】按钮，可清除由“导出”操作所生成的日志文件。

说明	【清除文件】操作仅清除服务器上由导出操作生成的日志文件，对数据库中的原始日志信息无影响。

6.7 日志管理配置

用户可根据需要通过直接导出、Syslog 以及 SNMP 多种方式将系统日志进行备份。

6.7.1 日志导出备份

选择菜单 **日志报表** > **日志管理配置** > **日志导出备份**，进入日志导出备份页面，如图 6-13 所示。用户可对不同类型的安全防护日志信息进行导出、下载及清空操作。

图 6-13 日志导出备份

导出日志

定期导出日志是清理存储空间的一种方式，即将日志以文件的形式存储到其他存储介质，进行永久保存。

在图 6-13 所示页面，根据需要单击不同日志类型对应的“操作”栏中的【导出】按钮，将 WAF 服务器数据库中的日志信息打包成日志文件存放在 WAF 服务器目录中。

以 Web 安全日志为例：

- 单击【分时导出】按钮，选择导出日志的时间段，在弹出的对话框中单击【开始导出】按钮后，开始导出日志，导出的日志将显示在相应日志类型的“下载”栏中。
- 单击【全部导出】按钮，自动导出当前该类日志的所有信息，导出的日志将显示在相应日志类型的“下载”栏中。

下载日志

WAF 支持将导出的日志下载至本地。在图 6-13 页面中，根据需要单击导出的日志文件，可将打包的日志文件保存至本地。

清除日志文件

在图 6-13 所示页面，根据需要单击不同日志类型对应的“操作”栏中的【清除文件】按钮，可清除由“导出”操作所生成的日志文件。

说明	【清除文件】操作仅清除服务器上由导出操作生成的日志文件，对数据库中的原始日志信息无影响。

清空数据库

在图 6-13 所示页面，根据需要单击不同日志类型对应的“操作”栏中的【清空数据库】按钮，可清空数据库中的原始日志信息。

注意	数据库中日志信息一经删除则无法恢复，请谨慎操作。

清空日志报表

单击图 6-13 页面下方的【清空日志报表】按钮，将清空如下内容：

- 数据库数据，包括引擎/接口流量、引擎连接数、安全防护日志信息；
- 由上述数据库数据生成的统计报表、处理数据文件。

注意	数据库数据及由此数据生成的统计报表、处理数据文件一经删除则无法恢复，请谨慎操作。

6.7.2 Syslog 配置

WAF 支持将日志信息保存至 Syslog 服务器。

选择菜单 **日志报表** > **日志管理配置** > **Syslog 配置**，进入 Syslog 配置页面，如图 6-14 所示。页面默认显示已配置的 Syslog 服务器 IP 地址及端口信息列表，用户可根据需要自行添加/删除 Syslog 服务器。

图 6-14 Syslog 配置

说明	Syslog 配置需与日志发送参数配置配合使用。有关日志发送参数配置的操作请参见 6.7.4 日志发送参数配置。

添加 Syslog 服务器

添加 Syslog 服务器的步骤如下：

步骤 1 单击图 6-14 中的【添加】按钮，添加 Syslog 服务器，如图 6-15 所示。

图 6-15 添加 Syslog 服务器

步骤 2 输入服务器地址和端口信息，单击【保存】按钮，保存配置。

----结束

删除 Syslog 服务器

单击图 6-14 中的图标，即可删除相应的 Syslog 服务器配置。

启用/停用 Syslog 服务器

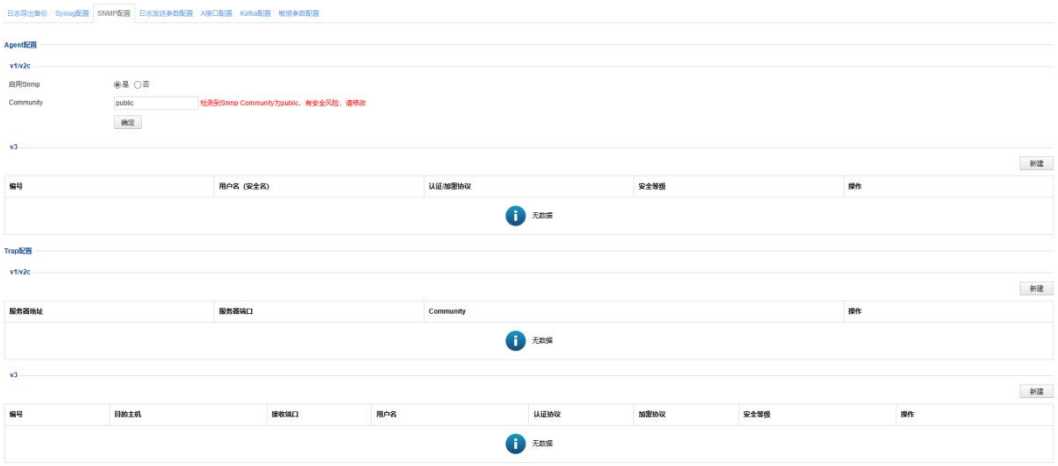
在图 6-14 所示页面选择“是”启用 Syslog 后，需要配置日志内容存储到 Syslog 服务器时的方式，可选方式有：**明文传输**和 **base64 编码**。单击【确定】按钮，使 Syslog 配置生效。

停用 Syslog 服务器时，只需选择“否”即可停用 Syslog 服务器。

6.7.3 SNMP 配置

WAF 支持将日志信息保存至 SNMP 服务器。选择菜单 **日志报表** > **日志管理配置** > **SNMP 配置**，进入 SNMP 配置页面，如图 6-16 所示。

图 6-16 SNMP 配置



说明	SNMP 配置需与日志发送参数配置配合使用。有关日志发送参数配置的操作请参见 6.7.4 日志发送参数配置。

6.7.3.2 配置 SNMP Agent

WAF 设备支持 v1/v2c、v3 版本的 SNMP 协议，下面分别对不同版本的 Agent 配置进行介绍。

配置 v1/v2c 版本 Agent

v1/v2c 版本的 SNMP Agent 配置步骤如下：

步骤 1 在图 6-16 中的 Agent 配置 v1/v2c 区域启用 Snmp 并配置参数 Community。

步骤 2 单击【确定】按钮，保存配置。

----结束

配置 v3 版本 Agent

配置 v3 版本的 Agent 需要确保 Snmp 处于启用状态。V3 版本的 SNMP Agent 配置步骤如下：

步骤 1 在图 6-16 中的 Agent 配置 v1/v2c 区域启用 Snmp。

步骤 2 单击图 6-16 中 Agent 配置 v3 区域中的【新建】按钮，弹出对话框，如图 6-17 所示。

图 6-17 新建 v3 版本 Agent

步骤 3 配置 v3 版本 SNMP Agent 参数，参数说明如表 6-12 所示。

表 6-12 v3 版本 SNMP Agent 参数

配置项	描述
用户名	SNMP v3 用户的名称。
认证协议	进行认证时使用的认证协议，可选项：**MD5** 和 **SHA**。
认证用 key	进行认证时使用的密钥。
加密协议	加密传送信息时使用的加密算法，可选项：**DES** 和 **AES**。
加密用 key	进行信息加密时使用的密钥。
安全等级	用户必须满足什么安全等级才能访问，可选项：**不认证**、**需认证**、**认证且加密**。

步骤 4 单击【保存】按钮，完成配置。

----结束

6.7.3.3 配置 SNMP Trap

配置所有版本的 SNMP Trap 时都需要确保 SNMP 处于启用状态。下面分别对 v1/v2c、v3 版本的 Agent 配置进行介绍。

配置 v1/v2c 版本 SNMP 服务器

v1/v2c 版本 SNMP 服务器的配置步骤如下：

步骤 1 单击图 6-16 中 Trap 配置 v1/v2c 区域中的【新建】按钮，弹出添加 v1/v2c 版本 SNMP 服务器对话框，如图 6-18 所示。

图 6-18 添加 v1/v2c 版本 SNMP 服务器

步骤 2 输入服务器地址、端口和 Community 信息，单击【保存】按钮，保存配置。

----结束

配置 v3 版本 SNMP 服务器

v3 版本 SNMP 服务器的配置步骤如下：

步骤 1 单击图 6-16 中 Trap 配置 v3 区域中的【新建】按钮，弹出添加 v3 版本 SNMP 服务器对话框，如图 6-19 所示。

图 6-19 添加 v3 版本 SNMP 服务器

步骤 2 配置 v3 版本的 SNMP Trap 参数，参数说明如表 6-13 所示。

表 6-13 v3 版本的 SNMP Trap 参数

配置项	描述
目的主机	接收 WAF 设备发出 SNMP Trap 报警消息的主机。 支持 IPv4 或 IPv6 地址，例：192.168.1.0 或 2001:abcd:123:1::。
接收端口	用于接收 SNMP Trap 报警消息的端口号。
用户名	SNMP v3 用户的名称。
认证协议	进行认证时使用的认证协议，可选项：**MD5** 和 **SHA**。
认证用 key	进行认证时使用的密钥。
加密协议	加密传送信息时使用的加密算法，可选项：**DES** 和 **AES**。
加密用 key	进行信息加密时使用的密钥。
安全等级	用户必须满足什么安全等级才能访问，可选项：**不认证**、**需认证**和**认证且加密**。
engineID	SNMP 引擎的 ID 号。 ID 号为 16 位的 16 进制数，填写时不用加“0x”开头。

步骤 3 单击【保存】按钮，完成配置。

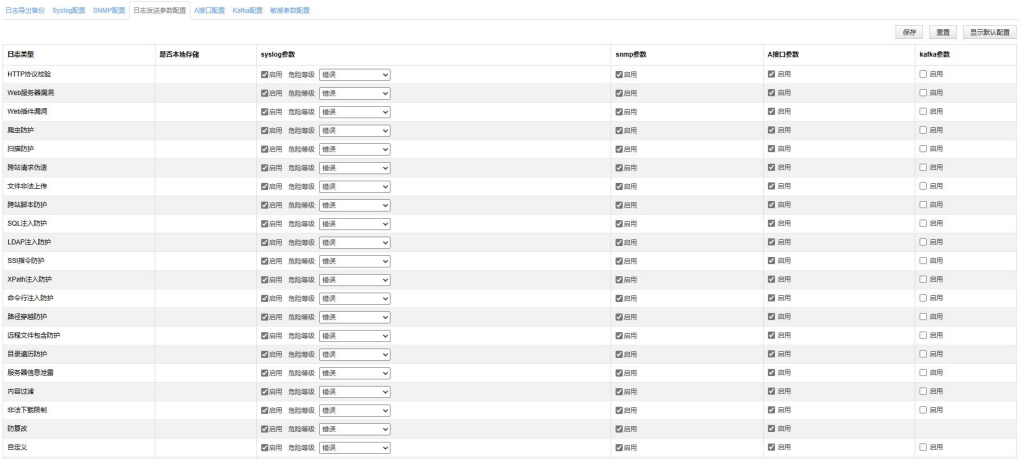
----结束

6.7.4 日志发送参数配置

WAF 支持用户对不同日志类型分别进行 Syslog 参数、SNMP 参数以及 A 接口参数配置。

步骤 1 选择菜单 **日志报表** > **日志管理配置** > **日志发送参数配置**，进入日志发送参数配置页面，如图 6-20 所示。

图 6-20 日志发送参数配置



步骤 2 配置日志发送参数，参数说明如表 6-14 所示。

表 6-14 日志发送参数说明

配置项	描述
日志类型	Web 安全事件对应的日志类型，包括 HTTP 协议校验、Web 服务器漏洞、Web 插件漏洞等。
是否本地存储	是否在 WAF 本地存储各种类型日志。 Web 访问日志，默认勾选本地存储，若不勾选，则 WAF 本地数据库不记录访问日志，使用 ESPC 上的【WAF 可管理安全服务】，依旧可以在管理端获取到访问日志。
syslog 参数	通过 Syslog 导出日志的配置参数。 启用：是否启用所选类型日志的 Syslog 服务。 危险等级：Web 安全事件的危险等级，从高到低分为**系统已不可用**、**必须马上采取行动**、**危急**、**错误**、**警告**、**普通但重要的情形**、**通知消息**和**调试信息**共 8 个等级。
snmp 参数	通过 SNMP 导出日志的配置参数。 启用：是否启用所选类型日志的 SNMP 服务。
A 接口参数	通过 A 接口将日志导出至企业安全中心的配置参数。 启用：是否启用所选类型日志的 A 接口服务。

步骤 3 单击【保存】按钮，使配置生效。

单击【重置】按钮，可将日志发送参数恢复为修改前的状态。

单击【显示默认设置】按钮，将日志发送参数显示为默认设置。

----结束

6.7.5 A 接口配置

当 WAF 与云或 ESPC 设备连接时，必须通过 A 接口上传数据，此时必须开启 A 接口。A 接口默认开启，当关闭 A 接口，需要重新开启时，操作如下：

步骤 1 选择菜单 **日志报表 > 日志管理配置 > A 接口配置**，进入 A 接口配置页面，如图 6-21 所示。

图 6-21 A 接口配置

步骤 2 选择“启用”。

步骤 3 单击【确定】按钮，保存配置。

----结束

6.7.6 Kafka 配置

WAF 支持将日志信息保存至 Kafka 服务器。Kafka 侧已完成相关配置，可以实时接收日志。

WAF 侧配置 Kafka 的步骤如下：

步骤 1 进入 **日志报表 > 日志管理配置 > Kafka 配置** 页面，完成 Kafka 的参数配置，单击【确定】按钮。页面默认显示已配置的 Kafka 集群列表，用户可根据需要自行添加/删除 Kafka 服务器。

Kafka 配置的参数说明如表 6-15 所示。

表 6-15 Kafka 配置的参数说明

配置项	描述
启用 Kafka	是否使用 Kafka 保存日志。可选项为：是、否。
日志内容	发送日志内容的方式。可选项为：明文传输、base64 编码。 当“启用 Kafka”选择“否”，日志内容仅支持 base64 编码，且不可更改。
设备位置	配置随日志发送的编码，如 sz 等。
IP	填写数据统计上报和特征库信息上报 URL 对应的 IP 地址。
端口	填写数据统计上报和特征库信息上报 URL 对应的端口号。

步骤 2 单击集群配置区域后的图标 ，集群列表新增一条记录。

步骤 3 单击新增记录后的【新增配置】按钮，弹出添加集群配置窗口，填写服务器地址、服务器端口和主题后，单击【保存】按钮。

新增集群展示在 Kafka 配置页面的集群列表中。一个集群支持配置多台服务器。

----结束

删除操作

在 Kafka 配置页面，可以执行以下删除操作：

- 单击集群后的图标 ，删除所选的集群。
- 单击【删除配置】按钮，删除所选的服务器。

6.7.7 敏感参数配置

启用敏感参数信息屏蔽功能并设置敏感参数后，当请求 URL 中包含已有的敏感参数时，则敏感参数相应的字段内容会被 WAF 记录到 Web 访问日志以及 Web 安全日志中，并且对字段内容做屏蔽处理。

例如：敏感参数配置中添加了“username”，若检测到一条请求 URL 为 http://10.67.1.205/py/xssResponse.php?username=123456，那么：

- 在 Web 访问日志记录中，URL 将被处理为 /py/sqlResponse.php?testid=1+&username=%5b**\x0A****%5d\x0A。
- 在 Web 安全日志记录中，URL 将被处理为/py/sqlResponse.php?testid=1 or 1=1&username=[******]。

注意	如果参数内容既是敏感信息，同时又包含攻击特征，则不予屏蔽。

配置敏感参数的步骤如下：

步骤 1 选择菜单 **日志报表** > **日志管理配置** > **敏感参数配置**，进入敏感参数配置页面，如图 6-22 所示。

图 6-22 **敏感参数配置**

步骤 2 启用“敏感信息屏蔽”，并在文本框中输入敏感参数。

可输入多个敏感信息参数，用分号分隔。

步骤 3 单击【确定】按钮，保存配置。

----结束

7 系统管理

系统管理主要包括以下内容：

功能	描述
网络配置	介绍如何进行工作组管理、路由配置、DNS 配置。
系统部署	介绍如何进行运行模式、HA、BYPASS、VRRP 配置以及 VRRP 配置信息管理。
系统工具	介绍系统工具的配置方法。
测试工具	介绍几种测试工具的作用和使用方法。
流量控制管理	介绍流量控制的相关操作。
系统参数配置	介绍系统维护员如何进行系统参数配置。
SSL 硬件加速	介绍如何开启/关闭 SSL 硬件加速卡。
系统运维	介绍如何进行 WAF 设备相关信息的一键收集以及系统恢复。
REST API	介绍如何管理数字签名。

7.1 网络配置

网络配置页面主要包含如下内容：

- 工作组管理
- 路由配置
- DNS 配置

7.1.1 工作组管理

不同部署模式的工作口管理界面有所不同，按照部署模式将设备的接口管理分为串联模式接口管理、旁路部署模式接口管理、反向代理部署模式接口管理和插件部署模式接口管理。关于系统部署模式的选择，请参见 7.2.1 配置运行模式。

说明	默认管理接口为 M 或 M、H1，工作口为 G1/1、G1/2 等依次类推（老平台仍为 eth0、eth1 等依次类推）。此处以 NX3-P1600B 为例进行介绍。

7.1.1.1 反向代理模式的工作组管理

反向代理模式下，工作组管理配置页面如图 7-1 所示。在该页面下，可以查看当前设备的可用接口，并可对管理接口和工作组接口进行管理。

图 7-1 反向代理模式 – 工作组管理

只有在反向代理模式下，接口的 IP 地址最多可以添加 253 个，并且可以批量管理当前配置的 IP 地址。在反向代理模式下，接口的编辑页面，如图 7-2 所示。反向代理模式下的工作组管理与串联模式类似，请参考串联模式的相关介绍。

图 7-2 反向代理模式 – 编辑接口

7.1.2 路由配置

WAF 支持缺省网关和静态路由配置。

静态路由是由管理员手工配置的一类路由。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。但是当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

在静态路由中有一类特殊的路由，那就是缺省路由。当设备在路由表中没有找到与数据包相匹配的路由时，通常将其丢弃，如果配置了缺省路由，则设备可以根据缺省路由的配置来转发报文。

本节主要介绍如何配置缺省网关和添加、删除静态路由。

7.1.2.1 配置缺省网关

配置缺省网关的操作如下：

步骤 1 选择菜单 **系统管理** > **网络配置** > **路由配置**，进入路由配置页面，如图 7-3 所示，配置缺省网关为 10.67.255.254”。

图 7-3 路由配置

步骤 2 在缺省网关参数的输入框中，输入网关地址，单击【确定】按钮，完成配置。

----结束

7.1.2.2 添加静态路由

添加静态路由的具体操作如下：

步骤 1 单击图 7-3 中静态路由列表右上方的【添加】按钮，弹出添加静态路由对话框，如图 7-4 所示。

图 7-4 添加静态路由

步骤 2 配置静态路由参数，参数详情如表 7-1 所示。

表 7-1 静态路由配置参数说明

配置项	描述
目的网络	目的网络的 IP 地址，IP 地址支持 IPv4 和 IPv6。
掩码	目的网络的 IP 地址的子网掩码。
网关	目的网络的 IP 地址的网关，即路由的下一跳。

步骤 3 单击【确定】按钮保存配置。

----结束

单击图 7-3 中静态路由列表里某条路由相应“操作”栏中的图标，弹出删除确认窗口，单击该窗口中的【确定】按钮，删除该静态路由。

7.1.3 DNS 配置

DNS 服务是互联网上非常重要和基础的服务之一，用来确定主机域名和 IP 地址之间的对应关系。WAF 作为 DNS 客户端，可以向指定的 DNS 服务器请求域名解析服务。WAF 设计了两种域名解析方法：

- 通过 DNS 服务器解析

  WAF 解析域名时需要获取域名对应的 IP 地址，此时 WAF 会向 DNS 服务器发送域名解析请求数据包。DNS 服务器通过查看表项获取对应的 IP 地址并发送给 WAF。

- 通过自定义域名解析

  WAF 解析自定义域名时，通过查看自定义域名表项来获取域名对应的 IP 地址，将待解析的域名和 IP 地址对应后，即可解析域名。自定义域名配置一般用于将域名解析为私网 IP 地址。

7.1.3.1 配置 DNS 服务器

配置 DNS 服务器的操作如下：

步骤 1 选择菜单 **系统管理** > **网络配置** > **DNS 配置**，进入 DNS 服务器配置页面，如图 7-5 所示。

图 7-5 DNS 服务器配置

步骤 2 在 DNS 服务器配置列表下方，输入 IPV4/IPV6 首选和备用 DNS 服务器。

步骤 3 单击【确定】按钮，完成配置。

----结束

7.1.3.2 管理自定义域名

管理自定义域名包括新建、编辑以及删除自定义域名。

新建自定义域名

新建自定义域名的具体步骤如下：

步骤 1 在图 7-5 所示自定义域名列表右上方，单击【添加】按钮，弹出配置自定义域名对话框，如图 7-6 所示。

图 7-6 自定义域名配置

步骤 2 配置自定义域名参数，包括 IP 地址和域名。

步骤 3 单击【确定】按钮，保存配置。

----结束

编辑自定义域名

步骤 1 在图 7-5 所示自定义域名列表中，单击某条域名相应“操作”栏中的图标  ，编辑该域名的参数。

步骤 2 编辑完成后，单击【确定】按钮，保存配置

----结束

删除自定义域名

在图 7-5 所示自定义域名列表中，单击某条域名相应“操作”栏中的图标  ，弹出删除确认窗口，单击该窗口中的【确定】按钮，删除该自定义域名。

7.2 系统部署

部署页面主要包含以下内容：

- 配置运行模式
- HA 配置
- BYPASS 配置（反向代理部署下无该配置页签）
- VRRP 配置（串联部署下无该配置页签）
- VRRP 配置信息管理（串联部署、旁路部署下均无该配置页签）

7.2.1 配置运行模式

选择菜单 **系统管理 > 系统部署 > 运行模式**，进入运行模式配置页面，如图 7-7 所示。

- WAF 的部署拓扑有四种：串联部署、旁路部署、反向代理部署和插件部署；
- 模式配置分为：转发模式、防护模式、调试模式和紧急模式（不同部署模式下支持的模式配置有所不同）；
  - 转发模式：进入该模式后，流量将不经过引擎处理直接转发，没有防护功能。反向代理部署模式下不支持该模式。
  - 防护模式：是 WAF 的工作模式，在防护模式下，WAF 具有防护功能。
  - 调试模式：与防护模式类似，WAF 也有防护功能，但是能从后台看到更多的调试信息，通常用于调试设备。
  - 紧急模式：当 WAF 处于紧急模式时，对新建的连接由引擎直接转发，对原有连接则仍然由引擎处理。

    紧急模式包括三种形式：不启用、永久启用、自动切换。如果选择“永久启用”，WAF 会一直处于紧急模式；如果选择“自动切换”，WAF 会根据 TCP 连接数、CPU 占用率、内存使用率自动进行切换。

    自动切换模式下，连接数、CPU、内存至少要开启一种，如果开启多种，当任何一种超过进入紧急模式阈值，则进入紧急模式；当全部低于退出紧急模式阈值同时超过弛豫时间，则退出紧急模式。

图 7-7 运行模式

配置紧急模式的详细信息如表 7-2 所示。

表 7-2 配置紧急模式参数信息

配置项		描述
驰豫时间（秒）		当 WAF 处于紧急模式时，若统计到 TCP 连接数、CPU 占用率、内存使用率低于上述定义的退出临界值，且持续时间超过了“驰豫时间”所定义的时间周期，则退出紧急模式。
连接数	开启连接数紧急模式	是否开启连接数紧急模式。
	进入紧急模式阈值	当 WAF 统计到连接数超过该临界值，则进入紧急模式。
	退出紧急模式阈值	当 WAF 统计到连接数低于该临界值，并且持续时间超过驰豫时间时，则退出紧急模式。

配置项		描述
CPU	开启 CPU 紧急模式	是否开启 CPU 紧急模式。
	进入紧急模式阈值	当 WAF 统计到 CPU 占用率超过该临界值，则进入紧急模式。
	退出紧急模式阈值	当 WAF 统计到 CPU 占用率低于该临界值，并且持续时间超过驰豫时间时，则退出紧急模式。
内存	开启内存紧急模式	是否开启内存紧急模式。
	进入紧急模式阈值	当 WAF 统计到内存使用率超过该临界值，则进入紧急模式。
	退出紧急模式阈值	当 WAF 统计到内存使用率低于该临界值，并且持续时间超过驰豫时间时，则退出紧急模式。

7.2.2 HA 配置

高可用性 HA（High Availability），是指通过尽量缩短因日常维护操作（计划）和突发的系统崩溃（非计划）所导致的停机时间，以提高系统和应用的可用性。HA 系统是目前企业防止核心计算机系统因故障停机的最有效手段。

HA 配置用于串联模式和反向代理模式下，设备的 HA 采用主从或主主工作方式（不同部署模式下支持的工作方式有所不同），可以实现如下功能：

- 链路状态的监测。
- 配置策略的同步。

HA 机制（双机热备）设置，需要两台 WAF 设备，其中一台设置为主模式，另外一台设置为从模式，两台设备之间通过心跳线通讯。

正常情况下，主模式的设备正常工作，从模式的设备不工作。当从模式的设备连续失去心跳的次数达到配置的上限后，立即启动工作口，开始工作，确保业务不间断。如图 7-8 所示，如果从模式的设备连续三次未能接收到主模式的设备心跳信号，就认为主模式的设备失去心跳。从模式的设备则会根据配置选项，决定是否启用工作口。

步骤 1 选择菜单 **系统管理 > 系统部署 > HA 配置**，进入 HA 配置页面，如图 7-8 所示。

图 7-8 HA 配置

步骤 2 配置 HA 参数，参数详细信息如表 7-3 所示。

表 7-3 配置 HA 的参数信息

配置项	描述
启用 HA	必选 是：立即启用 HA 功能； 否：不启用 HA 功能。
工作模式	有五种工作模式： 1、主设备：主-从模式的主设备，工作组的工作口正常运行，心跳口正常监测，当主模式 WAF 的工作口出现故障 down 掉时，网络流量会从主模式的 WAF 切换至从模式的 WAF。 2、从设备：主-从模式的从设备，工作组的工作口停止运行，从模式的 WAF 检测到主模式的 WAF 心跳丢失后，立即启动

配置项	描述
	从模式 WAF 的工作口。 3、端口同步：多路端口同步模式，支持所有已添加的工作组，此时 WAN 口和 LAN 口的状态具有联动性，同一个工作组内一个接口的工作状态会影响到对端接口的状态(例如:当 WAN 口状态为 DOWN 时，LAN 口状态也会 DOWN;而当系统检测到 WAN 口状态恢复至 UP 时,会自动将 LAN 口状态从 DOWN 切换到 UP）。 4、单机同步:双路备份模式,当主模式的工作组的工作口 down 掉，主模式工作组通过内部心跳信号通知从模式工作组，流量切换至从模式工作组。 5、主-主>：主-主模式，两台 WAF 都处于 Active 状态，同时工作。 启用 HA 后，将显示 WAF 的当前状态，如图 7-8 红框所示。 说明 不同部署模式下支持的工作模式有所不同。
工作组	选择启用 HA 防护的工作组。
心跳接口	WAF 用于发送心跳信号和接收对端心跳信号的接口，接口模式为 management。
对端 IP 地址	与本机心跳口相连的对端心跳接口的 IP 地址，IP 地址支持 IPv4 和 IPv6。 单击【配置同步】按钮，可进行配置同步： • 主-从模式配置同步：主设备可以将其配置同步到从设备，只能在主设备上进行同步操作； • 主-主模式配置同步：可以在两台设备上分别进行同步操作，在哪台设备上使用，即将该台设备的配置同步到对端设备； 配置同步后需等待一段时间，使对端设备同步到的配置应用生效。等待期间，请避免操作对端设备。
心跳协议端口	心跳信号采用 udp 传输协议，心跳协议端口为 udp 端口。
心跳时间间隔	心跳信号的频率。
失去心跳次数	定义 WAF 不能接收到对端主机心跳信号超过该次数，则认为对端主机失去了心跳。
配置同步端口	处于主模式的 WAF 可以同步配置到从模式的 WAF，同步配置采用 TCP 传输协议，同步端口就是 TCP 的端口。
同步间隔	同步配置的频率。
网关信息	如有需要，可以添加对端设备的网关信息。

步骤 3 单击【确定】按钮完成配置。

----结束

7.2.3 VRRP 配置

只有旁路部署模式、反向代理部署模式下才有 VRRP 配置，串联部署模式以及插件部署模式下无 VRRP 配置。

VRRP（Virtual Router Redundancy Protocol），即虚拟路由器冗余协议。VRRP 作为 RFC 的一种标准协议，它通过在客户的网络拓扑中部署两台（或多台）WAF，达到双机热备的功效。当主机 WAF 出现异常网络状况时（如工作组接口状态异常等），备机 WAF 能够迅速自动接管，保证网络的通信畅通。

反向代理部署模式下，配置 VRRP 的步骤如下：

步骤 1 选择菜单 **系统管理** > **系统部署** > **VRRP 配置**，进入 VRRP 配置页面，如图 7-9 所示。

图 7-9 VRRP 配置

步骤 2 单击【添加】按钮，添加 G1/1 接口，如图 7-10 所示。

注意	只能在工作口上配置 VRRP，管理口不能配置 VRRP。

图 7-10 添加接口

步骤 3 单击【确定】按钮，返回 VRRP 配置列表，如图 7-11 所示。

图 7-11 添加接口后的 VRRP 配置列表

步骤 4 单击 VRRP 实例列表操作栏中的图标，进入该接口的实例管理配置页面，如图 7-12 所示。

图 7-12 VRRP 实例管理页面

步骤 5 单击【添加】按钮，进入添加接口 VRRP 实例页面，如图 7-13 所示。

说明	配置 VRRP 时，在主机和备机 WAF 上，接口实例管理中的分组号、虚拟 IP 地址、发送间隔等参数必须保持一致。

图 7-13 添加接口 VRRP 实例

步骤 6 配置 VRRP 实例参数，参数详细信息如表 7-4 所示。

表 7-4 VRRP 实例参数信息

配置项	描述
分组号	分组号为虚拟设备标识，在同一个 VRRP 备份组内的设备必须有相同的分组号。取值范围为 1-255 的整数。 说明 主机和备机 WAF 必须配置相同的分组号。
优先级	数值越大，优先级越高，则越有可能成为 Master 设备。当优先级相同时，首要 IP 越大，则越有可能成为 Master 设备。取值范围为 1-254 的整数。
虚拟 IP 地址	主机和备机 WAF 上必须配置相同的虚拟 IP，一个 VRRP 实例中最多可配置 16 个虚拟 IP，IP 地址支持 IPv4 和 IPv6。
是否启用	必选 是：立即启用 VRRP 功能； 否：不启用 VRRP 功能；

配置项	描述
是否允许抢占	是指主机和备机 WAF 的工作模式： 1、非抢占方式：如果备份组中的设备工作在非抢占方式下，则只要 Master 设备没有出现故障，Backup 设备即使随后被配置了更高的优先级也不会成为 Master 设备。 2、抢占方式：如果备份组中的设备工作在抢占方式下，它一旦发现自己的优先级比当前的 Master 设备的优先级高,就会对外发送 VRRP 通告报文。导致备份组内设备重新选举 Master 路由器,并最终取代原有的 Master 设备。相应地,原来的 Master 设备将会变成 Backup 设备。
初始状态	当启动该实例时设备的初始状态。 1、Master：处于工作状态，承担安全防护的 WAF 设备。 2、Backup：备份设备，不处于工作状态，当 Master 设备出现故障时，能够代替 Master 设备工作的设备。
发送间隔	取值范围为 1-255 的整数。为保证主备 WAF 能合理有效地进行 VRRP 通告，应将两者 VRRP 实例配置中的发送间隔值设为一致。
首要 IP 地址	VRRP 通告报文总是用首要 IP 地址作为该报文 IP 包头的源 IP，默认为启用该实例的接口第一个 IP 地址,IP 地址支持 IPv4 和 IPv6。
监控接口	启用 VRRP 实例时所监控的接口，可多选。定义默认监控接口为添加当前 VRRP 实例的接口。
路由信息	根据实际拓扑环境配置链路通畅时所需路由。
描述	对该条 VRRP 配置的说明信息。

步骤 7 单击【保存】按钮，保存配置。

----结束

7.2.4 VRRP 配置信息管理

只有反向代理模式下才能使用 VRRP 配置信息管理功能。

VRRP 配置信息管理页面可以将在 WAF 上配置的 VRRP 信息文件导出到本地，也可以将已导出的 VRRP 配置文件导入 WAF。

导入 VRRP 配置文件

导入 VRRP 配置文件的操作如下：

步骤 1 选择菜单 **系统管理** > **系统部署** > **VRRP 配置信息管理**，进入 VRRP 配置信息管理页面，如图 7-14 所示。

图 7-14 VRRP 配置信息管理

步骤 2 单击【浏览】按钮，从本地选择待导入的 VRRP 配置文件。

步骤 3 单击【导入配置信息】按钮，在弹出的对话框中单击【确定】按钮，即可在 WAF 上导入该文件。

成功导入后的文件信息会自动显示在导入结果信息列表中。

说明	导入 VRRP 配置信息会导致 WAF 失去已有防护策略配置，请在系统工具的备份还原中创建当前 WAF 配置的还原点。 导入 VRRP 配置时，只导入 master 上代理 IP 为虚拟 IP 的站点解决方案。

----结束

导出 VRRP 配置文件

在图 7-14 所示页面，单击【导出配置信息】按钮，将 WAF 上当前的 VRRP 配置信息导出为 VRRP 配置文件。导出后的文件信息会自动显示在导出结果信息列表中。

查看导出的 VRRP 配置文件

导出 VRRP 配置文件后，可在 WAF 上查看 VRRP 配置文件的详细信息。

在图 7-14 所示页面的导出结果信息列表的“操作”栏，单击图标，查看该文件中备份的信息，如图 7-15 所示。

图 7-15 查看导出的 VRRP 配置文件详情

7.3 系统工具

系统工具页面主要包含如下内容：

- 系统信息
- 系统升级
- 规则升级
- 配置同步
- 许可证
- 时间语言
- 系统控制
- 端口设置
- Google Analytics 设置

7.3.1 系统信息

选择菜单 **系统管理** > **系统工具** > **系统信息**，进入系统信息页面，若 WAF 设备未搭载 SSL 加速卡，则系统基本信息如图 7-17 所示。该页面显示系统的硬件设备型号、序列号、硬件 HASH、固件版本、系统版本、系统规则库和规则库依赖信息。其中，每台 WAF 设备拥有唯一的硬件 HASH 值。

图 7-16 系统基本信息 – 无 SSL 加速卡

若 WAF 设备搭载 SSL 加速卡，则还会在图 7-17 所示的信息基础上展示“SSL 硬件加速”一项，如图 7-17 所示。

图 7-17 系统基本信息图 – 有 SSL 加速卡

7.3.2 规则升级

对于导入了销售证书的系统，在证书有效期内均可对规则进行升级，通过增加内置规则库的文件，提高系统的防护效果。

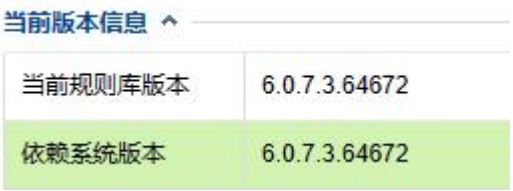
选择菜单 **系统管理** > **系统工具** > **规则升级**，进入规则升级页面，如图 7-18 所示。

图 7-18 规则升级

7.3.2.1 查看当前版本信息

在规则升级页面的“当前版本信息”区域，显示的当前版本信息包括：当前规则库版本和依赖系统版本信息，如图 7-19 所示。

图 7-19 当前版本信息



7.3.2.2 规则库升级

WAF 规则库升级包均为全量升级包，规则包升级方式分为定时升级和手动升级。

- 定时升级

  定时升级方式下，管理员需配置升级参数，系统在指定时间检查升级服务器，有最新的规则升级包时，自动下载升级包。下载升级包后，升级包安装方式又可设置为自动安装和手动安装。

- 手动升级

  手动升级方式下，管理员需要获取规则升级包后手动进行安装。

定时升级

规则升级页面的“定时升级”区域如图 7-20 所示。

图 7-20 定时升级

定时升级规则包的步骤如下：

步骤 1 配置定时升级参数，参数说明如表 7-5 所示。

表 7-5 定时升级规则包参数

配置项	描述
升级站点	WAF 获取规则升级包文件的升级服务器地址。 说明 必须保证 WAF 与升级站点之间的网络互通，否则 WAF 不能进行定时升级、检查更新等操作。
升级周期	WAF 下载规则升级包文件的周期。单位：天。
更新时间	WAF 检查升级服务器中是否有新的升级包的时间。 更新时间的格式如 12:38。
安装方式	按照设定周期下载升级服务器中的新规则升级包后的安装方式。 • 关闭自动更新：禁用定时升级功能。关闭自动更新时，系统将弹出提示信息“取消自动升级，将使您的产品无法得到最新的产品支持”。 • 下载后手动安装：下载新规则升级包后，不自动安装，而是通过推送消息通知管理员进行安装。 • 自动安装：下载新规则升级包后，系统会自动安装，并且在安装完成后推送消息通知管理员。 说明 • 仅对管理员帐号推送信息。 • 当产生推送信息时，若管理员帐号处于登录状态，推送信息将展示在任意 web 界面。 • 当产生推送信息时，若管理员帐号未登录，则在管理员登录系统后，进行推送信息展示。

步骤 2 单击【确定】按钮，完成配置。

----结束

手动升级

规则升级页面的“手动升级”区域如图 7-21 所示。

图 7-21 手动升级

手动升级规则包的步骤如下：

步骤 1 单击【浏览...】，选择后缀名为 **bin** 的规则升级文件。

步骤 2 单击【提交】按钮，在弹出的对话框中单击【确认】按钮，对规则进行升级。

升级过程中，系统会有如下提示：“系统正在升级，请稍候.....”。

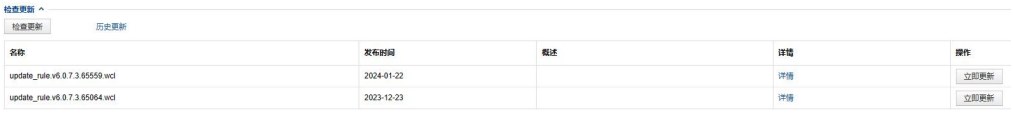
升级成功后将在历史更新链接中看到相应的升级记录。如果升级失败，可通过备份还原功能，还原到上个版本。

----结束

7.3.2.3 检查更新

在规则升级页面的“检查更新”区域，用户可检查更新以及查看历史更新记录，如图 7-22 所示。

图 7-22 检查更新

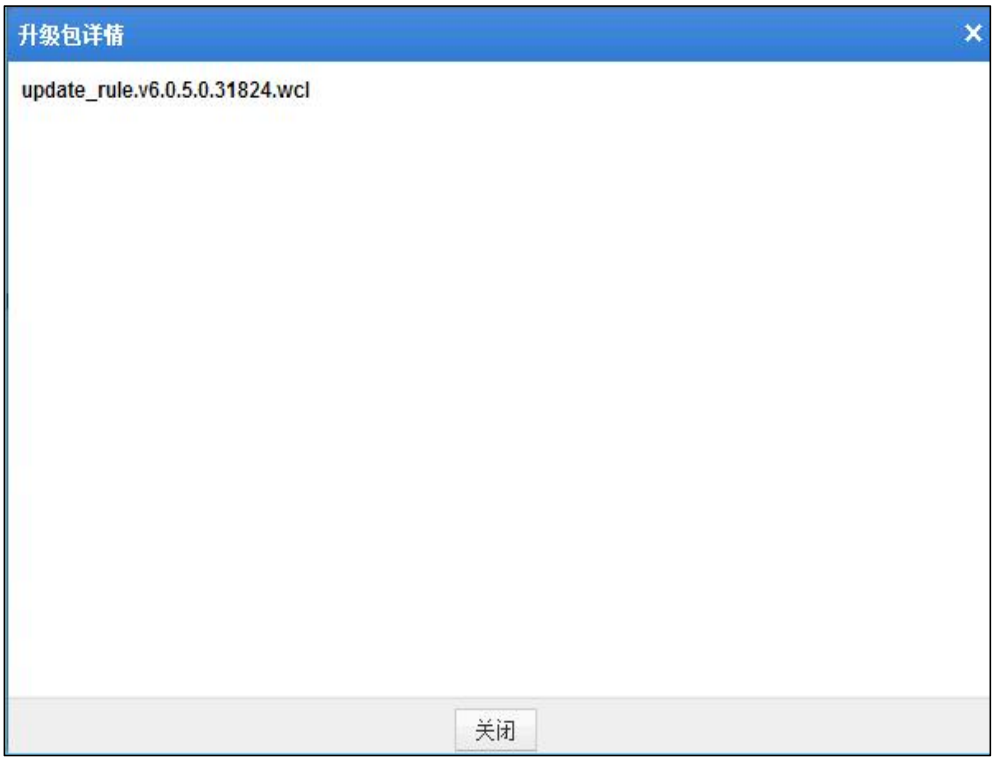


检查更新

单击【检查更新】按钮，WAF 将在升级服务器中检查是否有可用的新的规则升级包，并将新的规则升级包下载到 WAF 并显示在规则包列表中。若【检查更新】按钮置灰，则表示当前规则升级包已是最新版本。

- 单击规则包列表详情栏中的“详情”链接，查看规则升级包的详细信息，如图 7-23 所示。

图 7-23 规则升级包详情



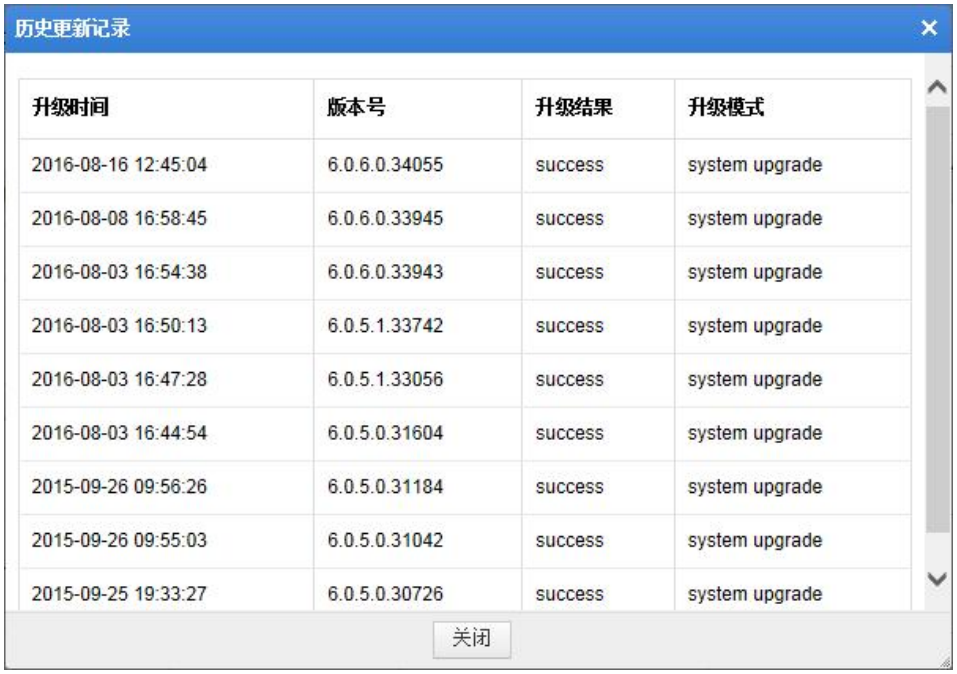
- 单击规则包列表操作栏中的【立即更新】按钮，立即安装规则升级包。

  规则升级包为全量升级包，选择某规则升级包升级更新完成后，升级包列表中该升级包以下的升级包都将显示为已经安装。

查看历史更新记录

单击“历史更新”链接文字，弹出历史更新记录对话框，如图 7-24 所示。

图 7-24 历史更新



历史记录包括规则升级包的安装时间、版本号、升级结果以及升级模式。

7.3.2.4 管理规则升级包

当 WAF 从升级服务器下载并安装规则升级包后，将自动备份规则库信息并记录在规则升级包列表中，用户可以在规则升级页面的“自动备份规则库信息”区域进行查看和管理，如图 7-25 所示。

图 7-25 自动备份规则库信息

查看规则升级包信息

如图 7-22 所示，WAF 把下载到本地的规则升级包按照版本号降序依次排列在规则升级包列表中。升级包列表的最大容量为 20 个，当超过容量限制后，WAF 将自动删除版本号最小的规则升级包，然后下载新的规则升级包。

列表中还显示每一个规则升级包的名称、发布时间、概述、详情、操作等信息。操作栏显示为已经安装的升级包，后台自动删除升级包文件。

还原规则升级包

用户可以将 WAF 的规则升级包还原到指定版本。

例如：对版本 A 的规则升级包进行了安装备份后，又安装了版本 B 的规则升级包，此时若对版本 A 规则升级包执行还原操作，则在满足依赖系统版本的情况下，可将当前的版本 B 规则升级包还原至版本 A。

单击图 7-25 规则升级包列表操作栏中“还原”链接，将 WAF 系统的规则库还原到指定版本。

7.3.3 配置同步

系统提供配置同步功能，当 WAF 出现异常情况，如：配置信息（例如安全管理和系统管理下用户的策略配置和系统配置等）损坏后，用户可以通过以下两种方式进行配置文件恢复，实现设备配置的还原。

- 离线同步：利用创建的还原点备份还原设备的配置。
- 在线同步：利用网络将选定的同步范围中的文件同步到另一设备。

7.3.3.1 离线同步配置

离线同步配置的操作如下：

步骤 1 选择菜单 **系统管理** > **系统工具** > **配置同步**，进入配置同步管理页面，如图 7-26 所示。

图 7-26 离线同步

步骤 2 创建还原点。

a. 选择同步范围，可选项如表 7-6 所示。

表 7-6 同步范围

配置项	描述
整机同步	备份内容包含：防护资产、防护策略、网络接口特性三大部分，包括对规则库的备份。
资产&策略同步	备份内容包含： • **安全管理**中：站点防护、自学习策略、自定义规则、策略管理、模板管理、代理信息配置、XSD/WSDL 文件管理、规则库。 • **系统监控**中：服务器存活状态检测。
策略同步	备份内容包含**安全管理**中：规则库管理、模板管理、策略管理中的所有策略类型。

b. 选择“离线同步”方式。

c. 单击【创建还原点】按钮，自动生成一个后缀名为 wafc 的文件。

步骤 3 还原配置。

离线同步还原配置有以下两种方式：

- 在图 7-26 所示历史还原点列表中，选择还原点后，单击相应操作栏中的图标，弹出确认还原对话框，单击【确定】按钮根据该还原文件还原系统。
- 若已下载还原点文件进行本地备份，也可通过单击图 7-26 中的【选择文件】按钮，提交事先下载到本地的还原点文件，实现配置的还原。

说明	• 若同步范围为整机同步：（1）需要重启设备来使整机同步范围内的网络接口配置信息立即生效；（2）网络配置（设备 ip）需要重启 Apache 服务生效，用户可以同步时选择“是”重启 Apache 服务，也可以选择“否”，待同步完成后手动重启设备使之生效。 • 其他同步范围的还原点备份文件无需关注。

----结束

在图 7-26 所示历史还原点列表中，还可进行如下操作：

- 单击操作栏中的图标，将还原文件下载到本地进行备份。
- 单击操作栏中的图标，删除相应还原文件。
- 单击操作栏中的图标，查看该还原文件的详细内容，如图 7-27 所示。

图 7-27 **还原文件详情**

7.3.3.2 在线同步

在线同步配置的操作如下：

步骤 1 选择菜单 **系统管理** > **系统工具** > **配置同步**，开启被同步设备的 rsync-606 服务，单击【确定】后，获取服务密码。然后选择同步范围，选择同步方式为“在线同步”，如图 7-28 所示。

图 7-28 在线同步

步骤 2 选择同步范围，可选项如表 7-6 所示。

步骤 3 选择同步方式为在线同步，并配置另一设备的 IP 地址和服务密码。

步骤 4 单击【同步】按钮，将选择的同步内容通过网络同步到配置的 IP 地址对应的设备中。

在线同步将被记录在在线同步列表中，单击列表右上方的【清除记录】按钮，清除在线同步所有历史记录。

----结束

在图 7-28 所示的历史在线同步记录列表中，单击操作栏中的图标，查看在线同步详情，如图 7-29 所示。

图 7-29 在线同步详情

7.3.4 许可证

初次使用本系统时，必须导入正确的许可证。

WAF 的证书分为以下两类：

- 试用证书

  试用证书过期后，系统无法升级，页面的【提交】按钮呈灰色不可用状态。此时引擎运行停止，系统自动进入包转发状态，无法继续使用本系统的防护功能。

说明	此时，如果导入了新的许可证，需要先检查设备当前的状态，如果已处于包转发状态，则手动切换至防护模式即可。

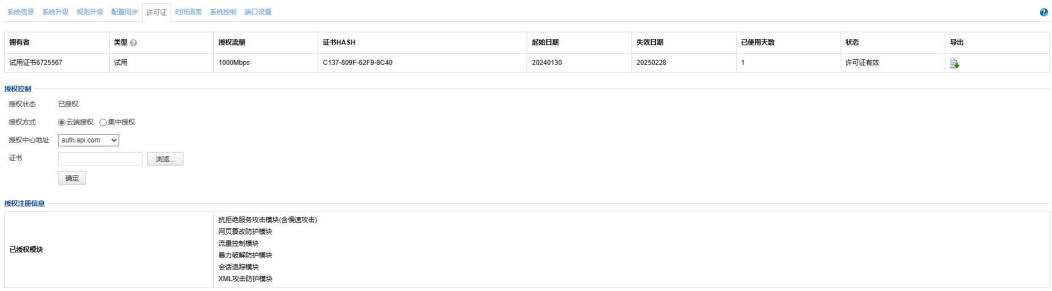
- 销售证书

  销售证书过期后，系统可正常防护，界面仍支持导入原有过期证书，且允许升级至证书有效期内的最新版本系统升级包。

7.3.4.1 查看许可证

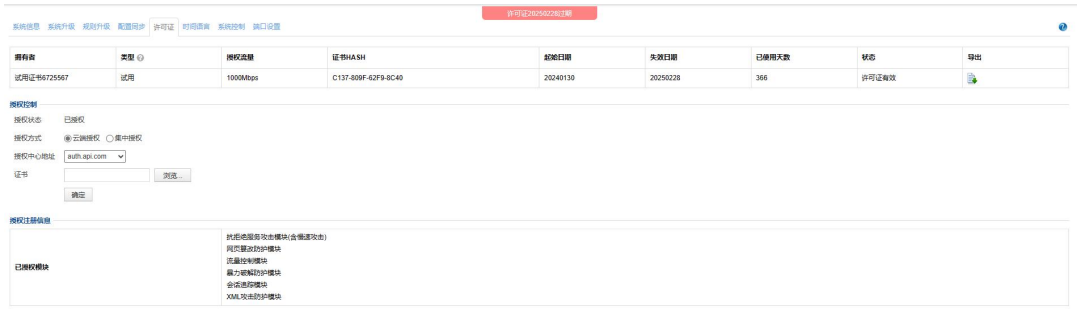
选择菜单 **系统管理** > **系统工具** > **许可证**，进入许可证管理页面，如图 7-30 所示。

图 7-30 许可证信息



用户导入许可证后，即可在此查看许可证信息，包括许可证信息和授权注册信息。当证书授权剩余时间小于等于一个月时，显示证书即将过期的提示信息，如图 7-31 所示。

图 7-31 证书过期提示



用户导入许可证后，即可在此查看许可证信息，包括许可证信息和授权注册信息。

7.3.4.2 导入许可证

导入证书的操作步骤如下所示：

在图 7-30 所示的许可证信息页面，单击【浏览...】选取证书文件（*.lic），然后单击【提交】按钮，等待授权完成。

----结束

7.3.5 时间语言

选择菜单 **系统管理** > **系统工具** > **时间语言**，进入系统时间语言配置页面，如图 7-32 所示。管理员可以进行系统时间设定、时间服务器设定和系统语言设定等。

图 7-32 配置时间语言

7.3.6 系统控制

选择菜单 **系统管理** > **系统工具** > **系统控制**，进入系统控制配置界面，如图 7-33 所示。

图 7-33 系统控制

通过单击相应的按钮可以进行以下系统控制的操作：

- 单击【重启引擎】——重新启动引擎，所有配置文件将被重新加载生效。当试用许可证过期后，引擎运行停止，重启引擎的【应用】按钮呈灰色不可用状态。
- 单击【重启设备】——重新启动 WAF 硬件系统。

  单击【关闭设备】——在关闭 WAF 硬件电源开关前，请先执行关闭设备的操作，确保设备正常关闭。

7.3.7 端口设置

选择菜单 **系统管理** > **系统工具** > **端口设置**，进入端口设置页面，如图 7-34 所示。

图 7-34 端口设置

WAF 默认的端口为 443，当 443 端口被占用后，访问 WAF 时，需要更改端口号。更改端口后，需要在 WAF 的访问地址后加上端口号重新访问。

7.4 测试工具

本节介绍调试设备时的常用工具，以便查看当前网络的连接状态和网卡状态等信息，例如：发生异常情况时，可通过 ping 或 traceroute 等工具进行相应的诊断和查看。

本节的测试工具主要分为系统调试的常用工具和安全扫描工具两类：

- Ping 工具、抓包工具、Trace Route 工具、邻居表、系统支持工具和调试日志追踪都是调试 WAF 设备和维护系统时的常用调试工具。
- 扫描工具用来检测系统的安全状况。

7.4.1 Ping 工具

Ping 工具用于检测主机存活或当前网络的连接情况。选择菜单 **系统管理** > **测试工具** > **Ping**，进入 Ping 页面，如图 7-35 所示。

图 7-35 Ping 工具

在文本框中输入目标主机的 IP 地址，然后单击【Ping】按钮，显示 ping 命令的诊断结果，如图 7-36 所示。

图 7-36 Ping 工具诊断结果

7.4.2 邻居表

WAF 提供邻居表，用于查看二层转发的 IPMAC 地址列表，以便排查网络问题。选择菜单 **系统管理** > **测试工具** > **邻居表**，进入 IPMAC 地址列表页面，如图 7-37 所示。

图 7-37 邻居表

7.4.3 Traceroute 工具

Traceroute 即路由追踪，用于检测网络路由线路。选择菜单 **系统管理** > **测试工具** > **Traceroute**，进入 Traceroute 页面，如图 7-38 所示。

图 7-38 Traceroute 工具

在文本框中输入目标主机的 IP 地址，单击【Traceroute】按钮，显示 Traceroute 命令的诊断结果，如图 7-39 所示。

图 7-39 Traceroute 工具诊断结果

7.4.4 抓包工具

管理员可以通过抓包工具获取经过 WAF 接口的数据包，帮助管理员分析、调试网络部署中遇到的问题。

配置抓包的具体操作如下：

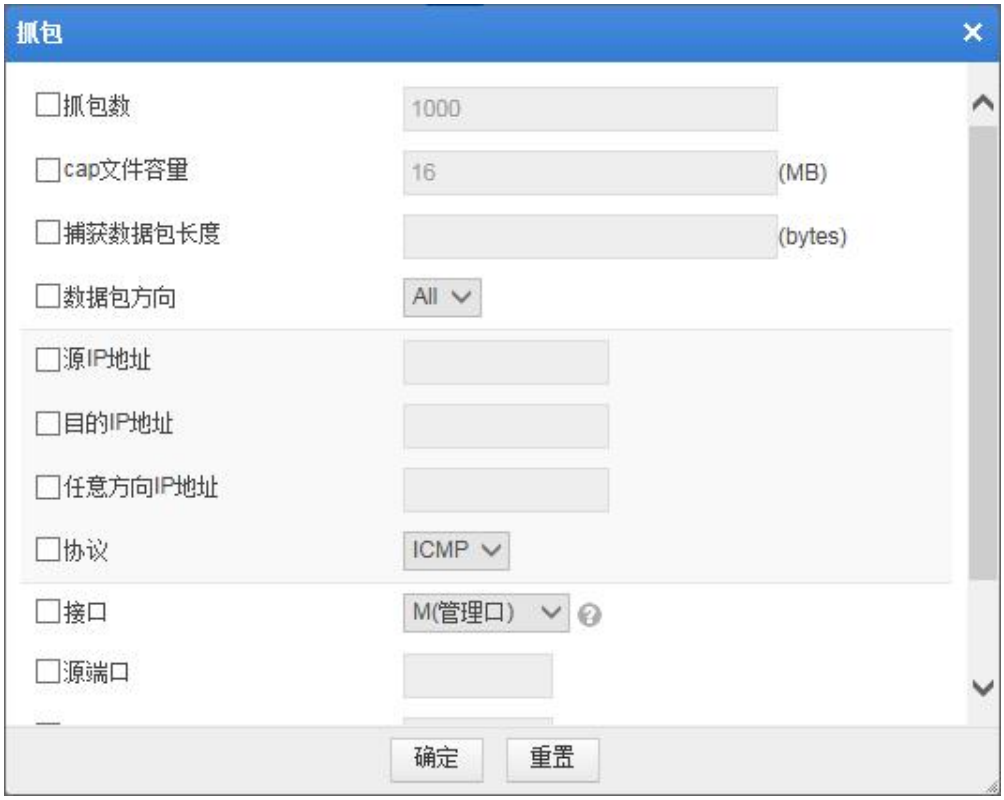
步骤 1 选择菜单 **系统管理** > **测试工具** > **抓包**，进入抓包列表页面，如图 7-40 所示。

图 7-40 抓包工具

步骤 2 单击【抓包】按钮，弹出抓包配置对话框，如图 7-41 所示。

勾选抓包参数左侧的复选框后，才能对参数进行配置。

图 7-41 抓包配置



步骤 3 配置抓包任务的主要参数，参数含义如表 7-7 所示。

表 7-7 配置抓包任务的参数说明

配置项	描述
抓包数	需要抓包的数量。
cap 文件容量	抓取数据包的文件大小的最大值。
捕获数据包长度	需要抓包的字节量，0 表示不限字节数。
数据包方向	需要抓取的数据包的方向，可以选择 **ALL**、**Rx**、**Tx**。其中 ALL 表示同时抓取发送和接收的数据包，Rx 表示抓取接收的数据包，Tx 表示抓取发送的数据包。
源 IP 地址	本次抓包任务开始的源 IP 地址，不填写表示不对源 IP 进行限制。
目的 IP 地址	本次抓包任务结束的目的 IP 地址，不填写表示不对目标 IP 进行限制。
任意方向 IP 地址	本次抓包任务开始的任意源或目的 IP 地址，不填写表示不对 IP 进行限制。
协议	抓包的协议类型，可以选择 **NON**、**ARP**、**TCP**、**UDP** 或 **ICMP**。不勾选，表示对所有协议不进行限制。
接口	选择一个接口号，表示本次任务是对该接口进行抓包。
源端口	本次抓包任务开始的源端口，不填写表示不对源端口进行限制。
目的端口	本次抓包任务结束的目的端口，不填写表示不对目的端口进行限制。
任意方向端口	本次抓包任务开始的任意源或目的端口，不填写表示不对端口进行限制。

步骤 4 单击【确定】按钮，立即开始抓包，如图 7-42 所示。如果单击【重置】按钮后，抓包配置参数将恢复为系统默认值，重新配置。

图 7-42 抓包过程

抓包过程中，单击图 7-42 所示页面右上角的【停止抓包】按钮，可中断抓包。

步骤 5 成功抓包后，数据包即会自动显示在如图 7-43 列表中。

此时，单击文件名栏中对应的文件名蓝色链接，或者单击操作栏中的图标，可将已抓取的数据包下载到本地，以便进一步分析设备发送或接收的数据包是否符合预期，或者分析 WAF 规则告警的详细信息。

图 7-43 抓包结果

在抓包列表中，单击操作栏图标，即可删除对应的抓包文件。

----结束

7.4.5 系统支持工具

系统支持工具主要用于调试人员进一步查看系统的接口状态、进程状态、系统路由、磁盘空间等，并可下载调试日志。选择菜单 **系统管理** > **测试工具** > **系统支持工具**进入系统支持工具页面，如单击图 7-44 所示的按钮，即可进行相应操作。

图 7-44 系统支持工具

7.4.6 扫描工具

WAF 内置扫描工具，用于扫描被保护服务器的网站漏洞。

配置扫描的具体操作如下：

步骤 1 选择菜单 **系统管理** > **测试工具** > **扫描工具**，进入扫描任务列表页面，如图 7-45 所示。

图 7-45 扫描配置列表

步骤 2 单击【新建】按钮，添加新的扫描任务，如图 7-46 所示。

图 7-46 扫描工具配置界面图

步骤 3 配置扫描工具参数，参数详细信息如表 7-8 所示。

表 7-8 配置扫描参数信息

配置项	描述
名称	扫描任务的名称。
扫描方式	即扫描类型，有以下两种： • SQL 注入和 XSS 漏洞扫描； • 挂马扫描。
入口 URL	开始扫描的第一个 URL，如 http://192.168.1.100/index.html。
扫描深度	扫描任务要扫描的网页链接层数，建议深度为 5。
扫描广度	域名的关键字。表示包含该关键字的 URL 网页均要被扫描；如果扫描入口 URL 为 IP 地址形式，则此处填入 IP 地址即可。
扫描定时类型	该扫描为定期扫描，周期分为：**每天**、**每月**、**每周**。

配置项	描述
星期/日期	如果配置扫描周期为每周和每月时，需要配置该项，即配置每周的星期几或每月的哪天进行扫描。
定时扫描时间	每天开始定时扫描的具体时间。
策略是否应用	是否应用该扫描策略。 • **启用**：表示扫描策略立即生效，会在设定的时间开始扫描。 • **停用**：表示扫描策略暂不生效，只有被启用后，才能生效。

步骤 4 单击【确定】按钮，WAF 会在配置的扫描时间进行扫描。

扫描结束后，扫描结果自动显示在如图 7-47 所示的列表中。

图 7-47 扫描结果列表

----结束

7.4.7 调试日志追踪

调试日志追踪是指，WAF 对指定客户端源 IP 的 HTTP 请求处理过程的调试级别日志进行追踪，用于排查各类引擎问题。

调试日志追踪的适用范围：追踪对象支持 IPV4/IPV6，支持 HTTP X-forward-for 头中代理 IP 的追踪。

配置调试日志追踪的具体操作如下：

步骤 1 选择菜单 **系统管理** > **测试工具** > **调试日志追踪**，进入调试日志追踪页面，如图 7-48 所示。

图 7-48 调试日志追踪

步骤 2 开启/关闭日志追踪功能。

单击【开启】/【关闭】按钮，开启/关闭日志追踪。

步骤 3 调试日志追踪全局配置。

单击蓝色链接文字“全局配置”展开调试日志追踪全局参数，全局参数说明如表 7-9 所示。

表 7-9 调试日志追踪全局参数

配置项	描述
日志级别	调试日志级别，可选级别有：**debug**、**info**、**warn**、**error**。 默认级别为 **warn**，请不要随意修改该日志级别。
追踪次数	某客户端 IP 访问服务器的一次完整 TCP 过程，从连接建立到连接关闭，识别成一次追踪。当追踪次数达到配置数时，停止追踪。
追踪时长	某客户端 IP 加入追踪列表后的追踪时长。从 IP 加入到追踪列表开始计算，累计追踪时长到达配置的时长时，停止追踪。

说明	追踪次数和追踪时长都可以终止追踪过程。无论哪一个阈值被达到，都会停止追踪。

步骤 4 管理追踪 IP 列表。

通过管理追踪 IP 列表，可追踪客户端 IP 的 HTTP 请求的调试日志。

a. 新建追踪 IP。

单击追踪 IP 列表区域的【新建】按钮，弹出新建 IP 对话框，如图 7-49 所示。

图 7-49 新建 IP

b. 输入 IP 地址，单击【确定】按钮，保存配置。

添加的 IP 地址将显示在追踪 IP 地址列表中，“追踪状态”栏中显示，表示相应 IP 未追踪或已完成追踪，如图 7-50 所示。

图 7-50 追踪列表

c. 单击“操作”栏中的图标，为相应 IP 下发追踪任务或为已完成追踪的 IP 重新下发追踪任务。

“追踪状态”栏中显示，表示当前该 IP 处于追踪中的状态。

d. （可选）单击“操作”栏中的图标，删除相应的追踪 IP 地址。

步骤 5 管理追踪日志。

追踪完成后生成的日志展示在追踪日志区域，如图 7-51 所示。

图 7-51 追踪日志

a. 下载追踪日志。

单击“操作”栏中的图标，下载相应 IP 的追踪日志到本地进行查看。

b. 单击“操作”栏中的图标，清除相应 IP 的追踪日志。

说明	当前追踪日志的阅读对象是研发人员，因此目前仅提供追踪日志的下载和清空界面接口。请用户将下载后的调试日志发送给研发人员辅助排查问题。

----结束

7.5 流量控制管理

当 WAF 以串联部署模式、旁路部署模式、反向代理部署模式部署时，可以对指定域名的流量进行限速，以缓解或减少当前网络的流量冲突。

启用/停用流量控制功能

步骤 1 选择菜单 **系统管理** > **流量控制管理**，进入流量控制对象管理页面，如图 7-52 所示。

图 7-52 流量控制管理

步骤 2 勾选“启用流量控制”，在弹出的对话框中单击【确定】按钮，使流量控制配置生效。

如需停用流量控制功能，取消勾选，在弹出的对话框中单击【确定】，即可停用流量控制。

说明	当执行以下操作后，流量控制对象中对应域名的流量控制功能即失效，系统会自动删除流量控制对象列表中相应的信息，同时该流量控制对象对应域名的流量控制日志也会被删除。如果流量控制对象下包含的所有域名都被删除后，该流量控制对象及对应的流量控制日志也都会被删除。 具体操作如下： 1、 包含流量控制对象中指定域名的站点或站点组被删除。 2、 编辑已有站点中被代理服务器的域名。

----结束

新建流量控制对象

新建流量控制对象前，必须先在站点防护界面中添加站点和站点的域名，相关介绍请参见 4.3.2.1 新建站点中的新建站点（反向代理模式）。同一域名只能被一个流控对象所包含，当可用域名用完时，则无法再创建新的流量控制对象。

新建流量控制对象的操作如下所示：

步骤 1 单击流量控制管理页面中的【新建】按钮，弹出新建流量控制对象对话框，如图 7-53 所示。

图 7-53 新建流量控制对象

步骤 2 配置流量控制对象参数，参数说明如表 7-10 所示。

表 7-10 流量控制对象参数说明

配置项	描述
对象名称	流量控制对象的名称，不能与已有名称重复。
限流值	流量限制的阈值，必须为数字。
描述	对流量控制对象的描述信息。
包含域名	选择流量控制对象包含的域名，至少需勾选一个或多个，勾选 all 表示选择全部域名；其中，域名列表由系统自动获取用户在反向代理模式下配置的站点的域名。

步骤 3 单击【保存】按钮，保存配置。

----结束

编辑流量控制

流量控制对象配置完成后，管理员可以重新编辑其参数，具体操作如下所示：

步骤 1 单击流量控制对象列表“操作”栏中的图标，编辑相应流量控制对象的参数，包括对象名称均可编辑。

步骤 2 单击【保存】按钮，保存配置并返回到流量控制对象列表界面。

----结束

删除流量控制对象

删除单个流量控制对象的具体操作如下所示：

步骤 1 单击流量控制对象列表“操作”栏中的图标，弹出删除确认窗口。

步骤 2 单击【确定】按钮，删除该流量控制对象。

----结束

删除多个流量控制对象的具体操作如下所示：

在流量控制对象列表中勾选一个或多个流量控制对象，单击流量控制对象列表右上方的【批量删除】按钮，弹出删除确认窗口，单击该窗口中的【确定】按钮，删除被选中的流量控制对象。

启用流量控制对象

新建的流量控制对象默认一直启用，当手动禁用某个流量控制对象后，可以重新启用。

- 启用单个流量控制对象

  单击流量控制对象列表“操作”栏中的图标，对应流量控制对象的状态变为，表示该流量控制对象已启用。

- 启用多个流量控制对象

  在流量控制对象列表中勾选一个或多个流量控制对象，单击流量控制对象列表右上方的【批量启动】按钮，弹出启动确认窗口，单击该窗口中的【确定】按钮，启用被选中的流量控制对象。

停用流量控制对象

- 停用单个流量控制对象

  单击流量控制对象列表“操作”栏中的图标，对应流量控制对象状态变为，表示该流量控制对象已停用。

- 启用多个流量控制对象

  流量控制对象列表中勾选一个或多个流量控制对象，单击流量控制对象列表右上方的【批量停用】按钮，弹出停用确认窗口，单击该窗口中的【确定】按钮，停用被选中的流量控制对象。

是否关闭新连接

在图 7-52 所示页面勾选“限流后关闭新连接”，在弹出的对话框中单击【确定】按钮，使配置生效。当一个流量控制对象被限流，且 WAF 保持的连接数达到设定值后，客户端新请求的连接会被 WAF 断开。此时，对于新连接的客户端，无法访问流量控制对象中域名映射的网站。

取消勾选，在弹出的对话框中单击【确定】按钮，即可停用限流后关闭新连接。此时，即使 WAF 进行限流，客户端新发来的连接也不会被 WAF 断开，只会被保存在 WAF 内延迟发送，但会消耗 WAF 的部分资源。

7.6 系统参数配置

系统参数包括引擎参数、内核参数、apache 参数和其他参数。

7.6.1 系统参数

系统维护用户成功登录后，可以对引擎参数进行配置管理。系统维护用户的帐号信息请参见**错误!未找到引用源。错误!未找到引用源。**。

步骤 1 选择菜单 **系统管理** > **系统参数配置** > **引擎参数**，进入引擎参数配置页面，如图 7-54 所示。

图 7-54 引擎参数配置

步骤 2 配置引擎参数（参数配置注意事项请参见 Web 页面），如需了解详细的参数说明，请联系技术支持人员。

步骤 3 单击【确定】按钮，将引擎参数配置下发给引擎。

引擎重启后，这些配置会被还原。

步骤 4 （可选）单击【持久化保存】按钮，将引擎参数配置保存到引擎的配置文件中，并下发给引擎。

引擎重启后，配置的引擎参数继续生效。

----结束

7.6.2 内核参数

内核核心参数默认关闭，在 NAT 环境下不能开启，其它环境下当需要测试 tcp 协议栈时，可开启该选项。

步骤 1 选择菜单 **系统管理** > **系统参数配置** > **内核参数**，进入内核参数配置页面，如图 7-55 所示。

图 7-55 内核参数

步骤 2 选择“开启”TCP 时间戳。

- 单击【确定】按钮，一次性开启 TCP 时间戳，当 WAF 引擎重启后，恢复默认的关闭状态。
- 单击【持久化保存】按钮，永久保持 TCP 时间戳开启状态。

----结束

7.6.3 Apache 参数

系统维护用户成功登录后，可以通过 Apache 参数对 Apache 模式进行配置。默认使用“低”强度加密算法证书来支持 IE 8 等浏览器，如需要使用“高”强度加密算法证书可切换到“高”。

步骤 1 选择菜单 **系统管理** > **系统参数配置** > **Apache 参数**，进入 Apache 参数配置页面，如图 7-56 所示。

图 7-56 Apache 参数

步骤 2 配置 Apache 模式为“高”。

- 单击【确定】按钮，一次性配置 Apache 模式为“高”，当 WAF 引擎重启后，恢复为“低”模式。
- 单击【持久化保存】按钮，永久保持 Apache 模式为“高”。

----结束

7.6.4 其他参数

系统维护用户成功登录后，可以通过其他参数对是否开启国密模式进行配置。系统维护用户的帐号信息请参见**错误!未找到引用源。错误!未找到引用源。**。

国密模式默认关闭。开启国密模式后，用户在新建站点时可以新建国密站点。

注意	国密模式和 SSL 硬件加速只能启用一个。若开启国密模式之前已经开启了 SSL 硬件加速，需要关闭 SSL 硬件加速之后再开启国密模式。

步骤 1 选择菜单 **系统管理** > **系统参数配置** > **其他参数**，进入国密模式管理页面，如图 7-57 所示。

图 7-57 其他参数

步骤 2 选择启用/关闭国密模式。

步骤 3 单击【确定】按钮，保存配置。

----结束

7.7 SSL 硬件加速

系统维护用户成功登录后，可以开启/关闭 SSL 硬件加速卡。系统维护用户的帐号信息请参见**错误!未找到引用源。错误!未找到引用源。**。

注意	SSL 硬件加速和国密模式只能启用一个。若开启 SSL 硬件加速之前已经开启了国密模式，需要关闭国密模式之后再开启 SSL 硬件加速。

步骤 1 选择菜单 **系统管理** > **SSL 硬件加速**，进入 SSL 硬件加速管理页面，如图 7-58 所示。

图 7-58 SSL 硬件加速

步骤 2 选择开启或关闭，开启/关闭 SSL 硬件加速卡。

步骤 3 单击【确定】按钮，保存配置。

----结束

7.8 系统运维

系统维护用户成功登录后，可以对系统进行一键收集和系统恢复操作。系统维护用户的帐号信息请参见**错误!未找到引用源。错误!未找到引用源。**。

步骤 1 选择菜单 **系统管理** > **系统运维**，进入系统运维页面，如图 7-59 所示。

图 7-59 系统运维

步骤 2 一键收集。

当设备故障时，“一键收集”可收集设备相关信息，便于分析设备异常原因、定位设备故障。

单击【一键收集】按钮，搜集设备相关信息。

- 单击一键收集文件相应操作栏中的图标，下载文件到本地进行查看。
- 单击一键收集文件相应操作栏中的图标，删除文件。

步骤 3 系统恢复。

当系统数据库、进程、引擎等发生异常时，使用以下“系统恢复”功能可紧急修复。

- 数据库：重建数据库。
- 进程：重启 WEB 服务、重启引擎服务、重启日志服务。
- 引擎：生成引擎内存转储。

注意	• 重建数据库会清空设备上所有日志。 • 生成引擎内存转储是指生成引擎的内存转储文件，可通过一键收集功能来获取此文件。

----结束

7.9 REST API

系统维护用户成功登录后，可以对系统 REST API 进行配置管理。系统维护用户的帐号信息请参见**错误!未找到引用源。错误!未找到引用源。**。

步骤 1 选择菜单 **系统管理 > REST API > 数字签名参数**，进入数字签名参数配置页面，如图 7-60 所示。

图 7-60 数字签名参数配置

步骤 2 配置 API 请求超时时间。

步骤 3 单击【确定】按钮，保存配置。

----结束

A 正则表达式语法

A.1 单个字符

符号	含义
.	任意单个字符（默认不包括换行，当开启 s 选项时可包括换行）
[任意字符]	匹配[]中指定的任意单个字符，如： [xyz]可匹配 axb 中的 x，cya 中的 y 或 ucz 中的 z； 可用-指定一个范围，如： [a-z]可匹配任意小写字母或[0-9]可匹配 0～9 中间任意一个数字
[^任意字符]	匹配除[]中的其他任意单个字符
\d	单个数字，等同于[0-9]
\D	非数字字符，等同于[^0-9]
\w	英文大小写字符、数字和下划线_，等同于[a-zA-Z0-9_]
\W	非英文大小写字符、数字和下划线_的其他任意字符，等同于[^a-zA-Z0-9_]
\s	空白字符，等同于[\t\n\f\r]
\S	非空白字符，等同于[^\t\n\f\r]

A.2 转义字符

符号	含义
^	整行或整个文本(开启多行模式时)的开头，如： ^t,只匹配 test 中第一个 t，不会匹配最后一个 t

符号	含义
$	整行或整个文本(开启多行模式时)的结尾，如：t$，只匹配 test 中最后一个 t，不会匹配第一个 t
\b	单词边界，如 a：、b 、\nc 或 a\n
\B	非单词边界
\A	整段文本的开头，等同于(?s)^
\Z	整段文本的结尾，等同于(?s)$
\a	Ascii 的 bell 符
\f	换页符
\t	水平制表符
\n	换行
\r	回车
\v	垂直制表符
*	*号
\\	\转义
\123	8 进制码表示字符，如\011 为水平制表符
\x7f	16 进制码表示字符，如\x0a 为换行

A.3 量词

符号	含义
x{n,m}	模式串 x 重复至少 n 次，最多 m 次，倾向于查找能够匹配的最大长度
x{n,}	模式串 x 重复至少 n 次，最多不限，倾向于查找能够匹配的最大长度
x{n}	模式串 x 精确重复 n 次
x*	模式串 x 重复 0~任意次，等同行于 x{0,} ，倾向于查找能够匹配的最大长度
x+	模式串 x 重复 1~任意次，等同于 x{1,} ，倾向于查找能够匹配的最大长度
x?	模式串 x 重复 0~1 次，等同于 x{0,1}
?	非贪婪模式，当将问号加在其他量词后面则表示倾向于查找能够匹配的最小次数，如 x{2,4}会匹配 xxxx，但是 x{2,4}?只会匹配 xx

A.4 分组

符号	含义
x|y	匹配模式串 x 或模式串 y，如 ab|cd 可匹配 tab 中

符号	含义
	的 ab 或 pcd 中的 cd
（x）	将模式串 x 作为一个分组用来分割模式串中的各部分，如匹配 abc 或 abd 可写 ab(c|d) 但如果写成 abc|d 只能匹配出 abc 或 d。
(?flags)	对之后的模式串启用什么选项，可用项如下： i：大小写不敏感（默认为关闭） m：多行模式（默认为关闭） s：可以匹配换行（默认为关闭） U：所有量词采用非贪婪模式（默认为关闭） 使用举例： (?i)表示大小写不敏感；(?-i)表示大小写敏感；模式串(?i)a(?-i)a 中第一个 a 表示大小写不敏感，第二个 a 表示大小写敏感

A.5 样例

- 匹配任意 IPv4 地址：
  (\d{1,3}\.){3}\d{1,3}
- 匹配所有 nsfocus.com 域名下的所有主机：
  ([\w-]+\.)+nsfocus\.com
- 匹配根目录中 log 子目录下的所有 txt 文件：
  ^/log/[^*\?:”<>|]+\.txt$
- 匹配所有包含.svn 的 url-path：
  ^.*/\.svn/.*$
- 匹配 jpg 和 jpeg 文件：
  ^.*/ [^*\?:”<>|]+\.(jpeg|jpg)$