RELIABLE NETWORK
SAFE WORLD
TOPSEC

天融信 WEB 应用安全防护系统
管理手册

北京市海淀区上地东路 1 号华控大厦 100085

电话：+8610-82776666

传真：+8610-82776677

服务热线：+86-4007770777

http://www.topsec.com.cn

版权声明

商标声明

信息反馈

http://www.topsec.com.cn

目录

1 前言

本管理手册主要介绍天融信 Web 应用安全防护系统（本文档简称为 TopWAF）的配置、使用和管理。通过阅读本文档，管理员可以了解 TopWAF 的基本设计思想，并根据实际应用环境配置 TopWAF。

本章内容主要包括：

- 文档目的
- 读者对象
- 约定
- 技术服务体系
- 文档意见反馈

1.1 文档目的

本文档主要介绍如何配置 TopWAF。通过阅读本文档，管理员能够正确地配置 TopWAF，并综合运用安全设备提供的多种安全技术有效地保护用户网络，控制网络的非法访问和抵御网络攻击，实现高效可靠的安全通信。并综合运用 TopWAF 提供的防护功能抵御针对 Web 站点的攻击。

1.2 读者对象

本管理手册适用于具有基本网络知识的系统管理员和网络管理员阅读，通过阅读本文档，他们可以独自完成以下一些工作：

- 对 TopWAF 进行基本管理。
- 配置防护对象、邮件策略、告警策略、报表策略及 Web 防护策略。
- 查看流量日志、攻击日志、调试日志和防篡改日志等日志信息。

- 管理与配置 TopWAF 的附加功能模块，如备份系统、高可用性、告警等。

1.3 约定

本文档遵循以下约定。

1）命令行格式采用以下约定：

格式	说明
粗体	命令行关键字（命令中保持不变，必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	方括号表示可选项。
< >	尖括号表示手工输入的参数。
{ }	大括号表示命令或参数组合。
|	竖线表示隔开多个相互独立的关键字或参数。
-	短线表示数字形式的参数范围，如 1-20。
,	逗号分割参数表示参数个数不确定的参数格式。比如向用户组添加若干个用户，每个用户间用“，”分隔。

2）图形界面操作的描述采用以下约定：

格式	说明
【XX】	表示按钮。如：点击【XX】按钮。
『』	表示带链接的文字。如：点击『添加』。
“”	表示页面内容引用。如：激活“XX”页签，弹出“XX”窗口，在下拉框中选择“XX”参数。
>	分隔多个菜单项，且此时菜单项采用“菜单命令”格式。 如：点击（选择） **高级管理** > **特殊对象** > **用户**。
<>	带尖括号表示键盘按钮名。如：按 <Ctrl> + <Alt> 即可。

3）为了叙述方便，本文档采用了大量网络拓扑图，图中的图标用于指明天融信和通用的网络设备、外设和其他设备，以下图标注释说明了这些图标代表的设备：

4）文档中出现的说明、注意、示例等标志，是关于管理员在安装和配置 TopWAF 过程中需要特别注意的部分，请管理员在明确可能的操作结果后，再进行相关配置。这些标志的意义如下：

格式	说明
	“说明”图标，对操作内容的描述进行必要的补充和说明。
	“注意”图标，提醒操作中应注意的事项，不当的操作可能会导致数据丢失或设备损坏。
	“示例”图标，对相关描述进行举例说明。

1.4 技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

http://www.topsec.com.cn

天融信全国安全服务热线

400-777-0777

1.5 文档意见反馈

如果您在使用过程中发现文档的任何问题，可通过服务热线或在线客服的方式进行反馈。感谢您的反馈，让我们做得更好！

2 TopWAF 简介

天融信公司自主研发的 Web 应用防火墙系统（本文档简称 TopWAF），继承了天融信公司“完全你的安全”的信息安全理念，通过多种检测方法，提供针对用户 Web 服务器的完整安全解决方案。保障用户业务的连续性和信息资产的安全性。

TopWAF 产品支持在线串接、旁路检测、负载均衡、反向代理部署。能够提供 OWASP Top10 的全面防御，同时可以主动对业务系统建立正向模型，用于防御未知的威胁和 0day 攻击。TopWAF 产品融合了天融信积累多年的 DDoS 防御功能，可以有效的缓解针对 Web 服务器的 Syn flood、CC、慢速攻击等各种拒绝服务攻击。不同于传统的网络安全设备（如 IDS、IPS、防火墙等），TopWAF 工作在 OSI 模型的应用层，检测 HTTP（S）流量。

TopWAF 产品提供了详细的 Web 流量日志和攻击事件日志，以及基于攻击事件日志实现的各种统计报表，并以可视化方式动态展示，实现实时的威胁监控，是一种可信的防御 Web 威胁的安全产品，适用于政府、企业、高校以及运营商等各种用户。

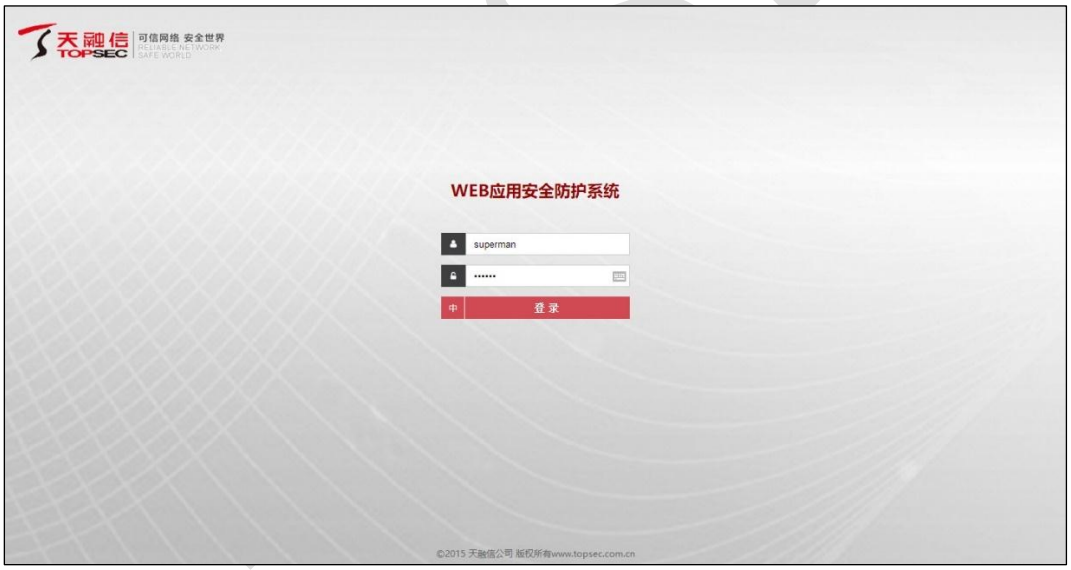
3 Web 管理

管理员在登录系统前应首先安装部署 TopWAF，安装成功后开启电源，才能通过管理主机登录并管理系统。具体的安装和简单配置过程请参见《TopWAF 安装手册》。

本章主要介绍登录界面及管理界面常用图标说明。

3.1 登录界面

管理员在管理主机的浏览器上输入 TopWAF 的管理 URL，例如：https://192.168.1.254，弹出如下的登录页面。

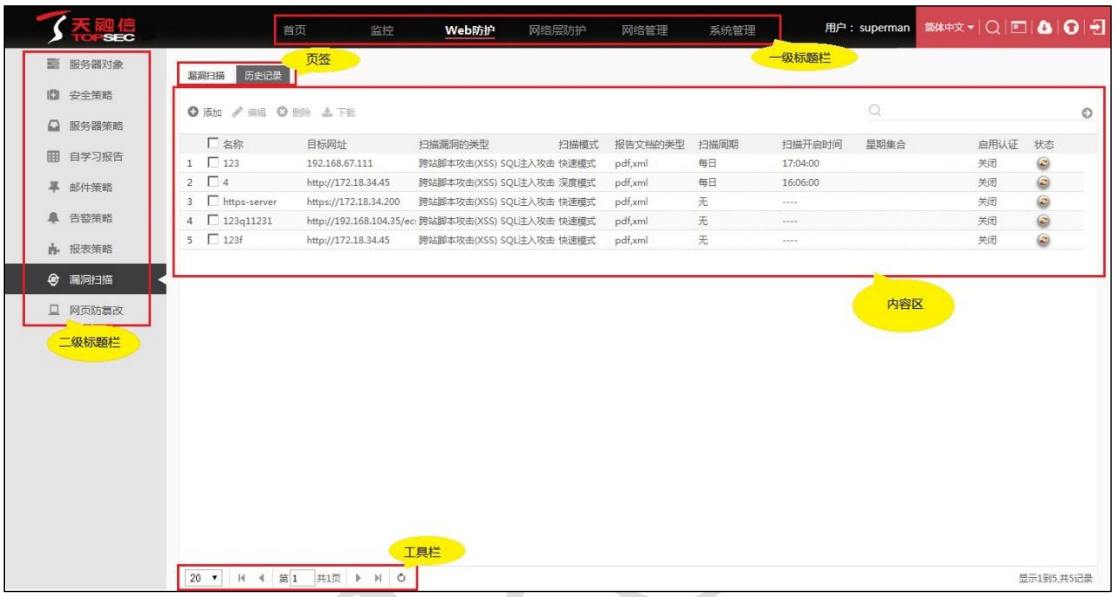


输入用户名/密码（默认用户名/密码为：superman/talent）后，点击【登录】按钮，即可进入管理页面。

- ✧ 在输入 URL 时要注意以“https://”作为协议类型，例如 https://192.168.1.254。
- ✧ TopWAF 对于用户名和密码大小写敏感。
- ✧ 建议使用最新版本的 Firefox 浏览器或者 chrome 浏览器。

3.2 管理界面

Web 管理界面由一级标题栏、二级标题栏、页签、内容区和工具条组成。管理界面如下图所示。



对上图的说明如下：

图标	说明
20	每页显示信息条数，如“20”表示每页最多可显示 20 条信息。
	显示第一页。
	显示上一页。
	显示下一页。
	显示最后一页。
	刷新当前页面数据。
	搜索 TopWAF 的功能模块，可以快速链接到每个模块的设置页。
简体中文	设置 TopWAF 的系统语言。可选项：简体中文，English。
	打开终端登录页面，可以通过 Web 终端配置 TopWAF。
	保存当前配置。
	更换界面外观皮肤。
	退出登录。

3.3 图标说明

管理页面中有很多图标帮助用户进行配置操作，下表将对页面中出现频率较高的图标进行说明。

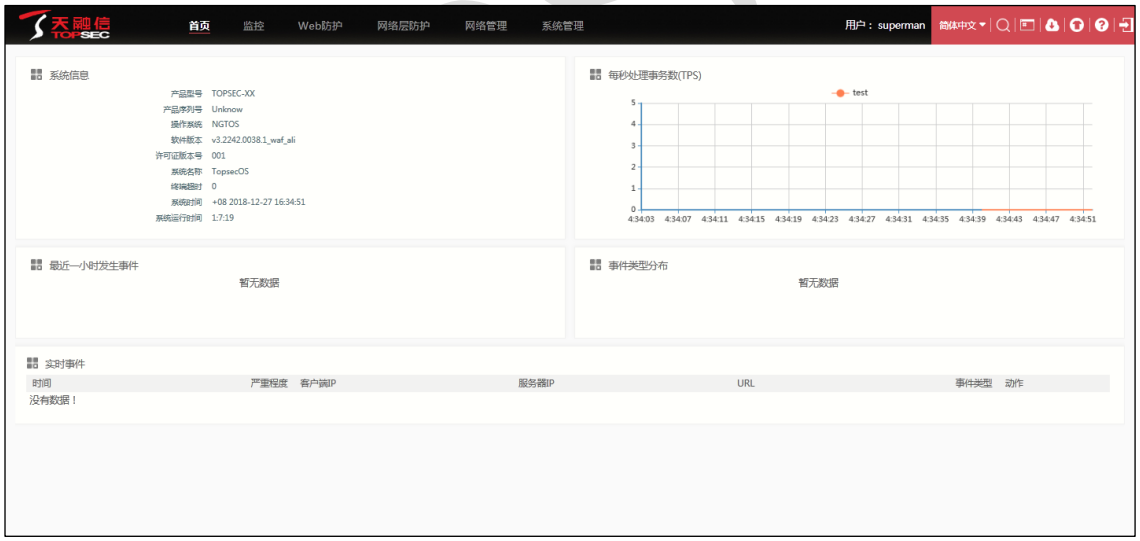
图标	名称	说明
查看	查看	选中需要查看的条目，点击该图标即可查看该条目的详细信息。
	添加	点击该图标，添加新条目。
	编辑	选中需要修改的条目，点击该图标即可对该条目重新进行编辑。
	删除	选中需要删除的条目，点击该图标即可将该条目删除。
	搜索	在该图标处输入查询关键字，点击“”图标可查询带有关键字信息的条目。
	清空	点击该图标即可以清空该条目的统计或者配置信息。
	属性	选中需要修改属性的条目，点击该图标，即可修改该条目的属性。
	另存为	点击该图标，备份配置信息。
	导入	点击该图标，在弹出的窗口中，配置导入信息，即可完成导入。
	导出	选中需要导出的条目，点击该图标，在弹出的窗口中，选择条目的保存地址，即可完成导出。
	克隆	选中需要复制的条目，点击该图标即可复制该条目。
	开启	功能已开启，点击该按钮将关闭此功能。
	关闭	功能已关闭，点击该按钮将开启此功能。

4 首页和监控

TopWAF 能够精准的监测网络中的攻击事件，用户可以根据事件统计分析网络中的潜在风险，并根据监控结果修改 Web 服务器的配置。首页和监控页面以丰富清晰的界面对 TopWAF 的各种实时和历史信息进行生动展现，为管理员提供可靠的网络监管平台，管理员可轻松快捷掌握网络中是否存在安全威胁，结合 TopWAF 的日志报表功能可快速追踪攻击来源、发现网站漏洞等，保障 Web 服务器安全。

4.1 首页

选择 **首页**，进入首页界面，如下图所示。



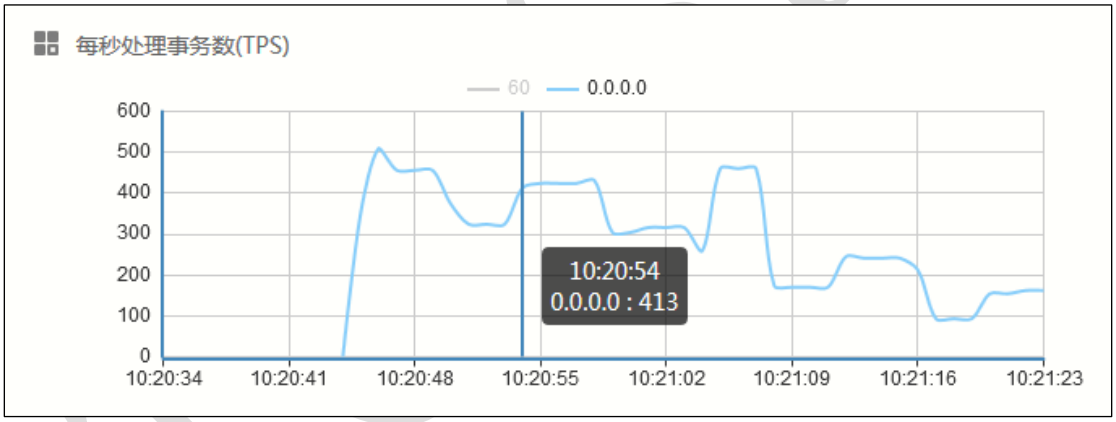
首页共包括系统信息、每秒处理事务数（TPS）、最近一小时发生事件、事件类型分布、实时事件共 5 个模块窗口。

- 系统信息

系统信息面板显示 TopWAF 的型号、序列号、操作系统、软件版本、许可证版本号、系统名称、终端超时时间、系统时间、系统运行时间，如下图所示。

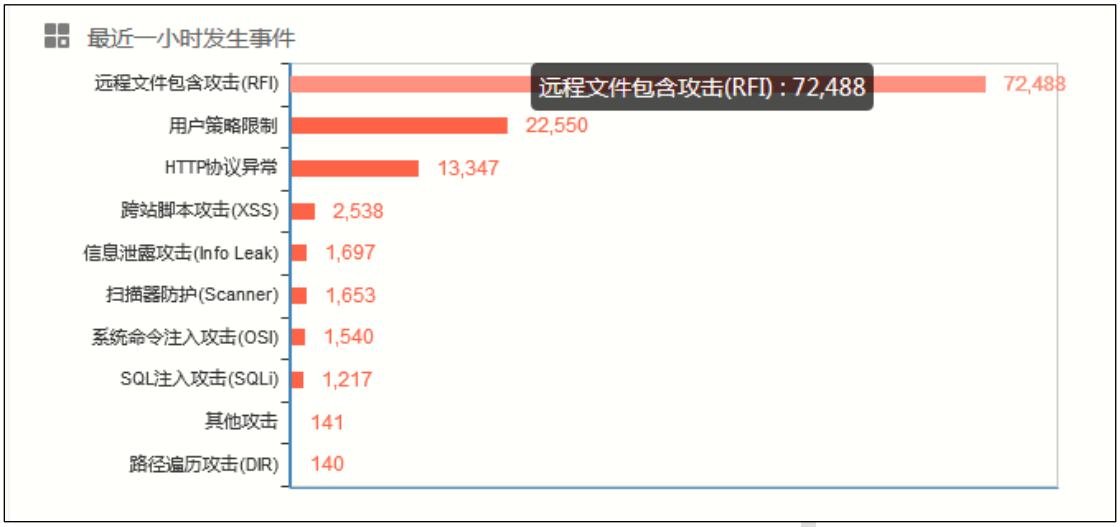
- 每秒处理事务数（TPS）

每秒处理事务数（TPS）面板以曲线图的形式实时显示 TopWAF 所有服务器策略每秒处理事务的数量，不同的服务策略使用不同颜色的曲线表示，关于服务器策略的配置具体请参见 5.3 服务器策略。将鼠标移动至图形的任意部分，会显示相应时刻各个服务器策略的每秒处理事务数（TPS）。点击界面上的服务器策略名称，可以设置是否在统计图中显示该策略的统计信息。隐藏该策略的统计信息后，该策略的图标及说明将变为灰色，如下图所示。



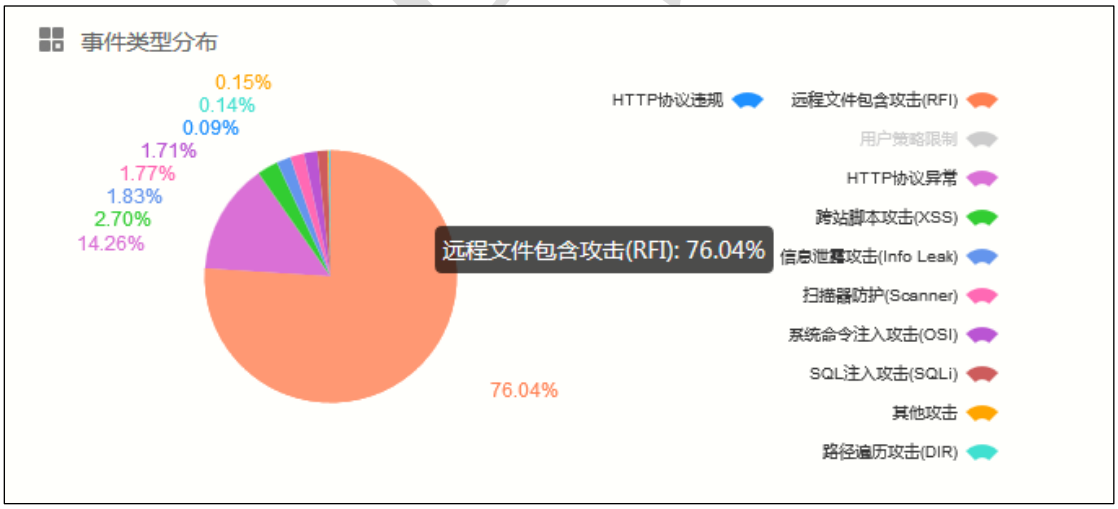
- 最近一小时发生事件

最近一小时发生事件面板以柱状图的形式显示最近的一个小时内服务器受到的攻击事件的统计信息。界面中按照受到攻击事件的数量由高到低进行排序。将鼠标移动至任意柱形，会显示在最近一小时内相应事件的发生数量，如下图所示。关于更详细的攻击事件统计信息可选择 **监控** > **威胁统计**，进行查看。管理员在了解最近一小时发生事件后，可以选择 **监控** > **日志查看** > **安全日志**，查看具体的攻击信息并制定或者修改相应的防护策略。



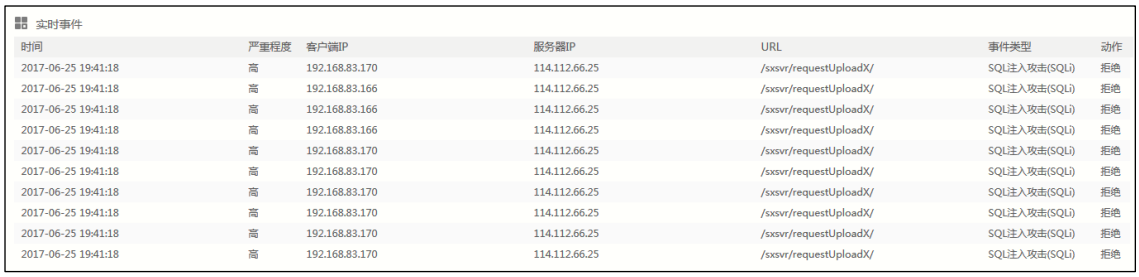
- 事件类型分布

事件类型分布面板以饼状图的形式显示服务器受到的攻击事件所占百分比。图中不同颜色代表不同类型的安全事件。将鼠标移动至饼图的任意部分，会显示相应的安全事件及其所占百分比。点击界面右侧上的事件名称，可以设置是否在统计图中显示该类型的事件。隐藏该类型的事件后，该类型的图标及说明将变为灰色，如下图所示。关于更详细的攻击事件统计信息可选择 **监控** > **威胁统计**，进行查看。



- 实时事件

实时事件面板以表格形式显示 TopWAF 检测到的最近 10 个攻击事件，包括攻击的时间、严重程度、客户端 IP、服务器 IP、URL、事件类型及动作。可以选择 **监控** > **日志查看** > **安全日志**，激活“攻击日志”页签，查看更为详细的攻击日志信息，具体请参见 4.2.1 日志查看。



实时事件

时间	严重程度	客户端IP	服务器IP	URL	事件类型	动作
2017-06-25 19:41:18	高	192.168.83.170	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.166	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.166	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.166	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.170	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.170	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.170	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.170	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.170	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝
2017-06-25 19:41:18	高	192.168.83.170	114.112.66.25	/sxsvr/requestUploadX/	SQL注入攻击(SQLi)	拒绝

4.2 监控

4.2.1 日志查看

日志查看主要用于查看具体的日志，管理员通过查看日志信息，可以获知当前访问网络应用、网络安全事件以及流经设备的流量特征，识别出潜在的安全威胁，从而制定更加合理的 Web 防护策略。

- ✧ 点击某条日志前的“ ”或双击日志可查看详细信息。
- ✧ 在服务器策略中开启“流量日志”开关后即可产生流量日志，关于流量日志功能的开启具体请参见 5.3 服务器策略。
- ✧ 在系统日志配置中勾选“调试日志”、“系统运行”后即可产生调试日志和系统运行日志，关于系统日志功能的配置具体请参见 8.5.1 日志配置。
- ✧ 一个 DDoS 攻击在发起时产生一条日志，在结束时再产生一条日志。

可以查看的日志种类包括以下几种：

- 流量日志：流量日志用来记录客户端向服务器发起请求过程中的详细信息，比如请求方法、参数、URL、上行流量、下行流量等。
- 攻击日志：攻击日志用来记录 TopWAF 检测到攻击的详细信息。通过查看攻击日志，管理员可以掌握服务器的状态并发现潜在的攻击行为，从而保护 Web 站点的安全。
- 防篡改日志：用来记录网站上的文件被恶意篡改的详细情况，通过查看防篡改日志，管理员可以快速定位被攻击的网站文件。关于网页防篡改的配置具体请参见 5.8 漏洞扫描

漏洞扫描用来检测被保护站点存在的安全漏洞，以及安全漏洞的风险等级。管理员可以依据漏洞扫描形成的扫描报告，修复站点的安全漏洞，增强站点的安全性。管理员还可以把扫描

报告导入 TopWAF 自动生成对应的防护规则，具体请参见 5.2.14.2 漏洞扫描报告生成防护策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **漏洞扫描**，激活“漏洞扫描”页签。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。

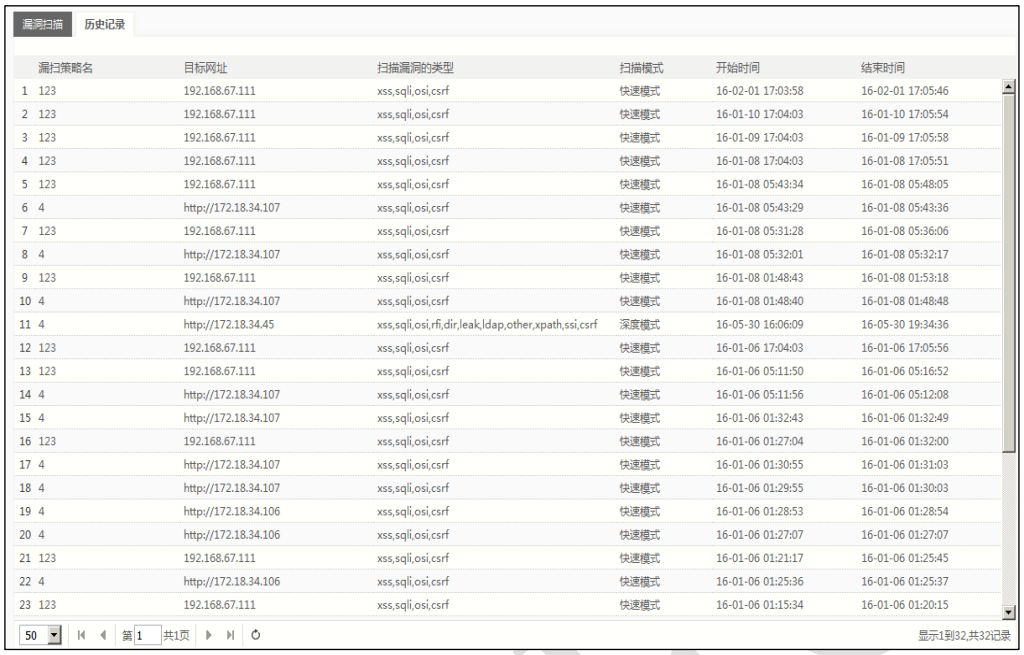
在配置漏洞扫描时，各项参数的具体说明如下表所示。

参数	说明
名称	设置漏洞扫描名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
目标网址	设置漏洞扫描的 URL 地址。
扫描漏洞的类型	设置漏洞扫描的类型。

参数	说明
	全选：选择所有的攻击类型。 反选：选择除已勾选的攻击类型外的攻击类型。 关于攻击类型的配置具体请参见 5.2.6 防护策略。
扫描的模式	选择漏洞扫描方式。 快速模式：快速扫描只扫描规则库中较为常见的漏洞，扫描耗时短。 深度模式：深度扫描对服务器进行全面扫描，扫描规则库中支持的漏洞扫描类型，扫描耗时长。
报告的文档类型	设置输出的报告文档类型，可选项：html、pdf、txt 和 xml。
扫描周期	设置漏洞扫描策略生效时间。 无：不进行周期性扫描，需要用户配置完成后，在漏洞扫描任务所在行，点击状态操作按钮，启动漏洞扫描。 每日：通过设置“定时扫描开启时间”参数，指定每日的指定时间扫描漏洞。 每周：通过设置“星期集合”和“定时扫描开启时间”参数，设置在指定的星期及时间扫描漏洞。 每月：通过设置“日期集合”和“定时扫描开启时间”参数，设置在指定的日期及时间扫描漏洞。
启用认证	设置是否开启邮件认证功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
用户名	启动“启用认证”后才能设置该参数值。用于发送报警信息的电子邮件用户名，必须是 SMTP 服务器的合法帐户。
密码	启动“启用认证”后才能设置该参数值。 设置发件人帐户对应的密码。
邮件策略名	选择通过邮件发送告警信息的漏洞扫描，关于漏洞扫描的配置具体请参见 5.5 邮件策略。
邮件标题	设置告警邮件的标题，默认值：TopWAF 漏洞扫描报告。
邮件内容	设置告警邮件的内容，默认值：TopWAF 漏洞扫描结果。由漏洞扫描进程发送。

步骤3 参数配置完成后，点击【确定】按钮完成漏洞扫描策略的添加。对于已经成功添加的策略，管理员可以进行编辑、下载和删除操作。

步骤4 在本页面激活“历史记录”页签，可查看漏洞扫描的历史记录，如下图所示。



	漏扫策略名	目标网址	扫描漏洞的类型	扫描模式	开始时间	结束时间
1	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-02-01 17:03:58	16-02-01 17:05:46
2	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-10 17:04:03	16-01-10 17:05:54
3	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-09 17:04:03	16-01-09 17:05:58
4	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-08 17:04:03	16-01-08 17:05:51
5	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-08 05:43:34	16-01-08 05:48:05
6	4	http://172.18.34.107	xss,sqli,osi,csrf	快速模式	16-01-08 05:43:29	16-01-08 05:43:36
7	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-08 05:31:28	16-01-08 05:36:06
8	4	http://172.18.34.107	xss,sqli,osi,csrf	快速模式	16-01-08 05:32:01	16-01-08 05:32:17
9	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-08 01:48:43	16-01-08 01:53:18
10	4	http://172.18.34.107	xss,sqli,osi,csrf	快速模式	16-01-08 01:48:40	16-01-08 01:48:48
11	4	http://172.18.34.45	xss,sqli,osi,rfi,dir,leak,ldap,other,xpath,ssi,csrf	深度模式	16-05-30 16:06:09	16-05-30 19:34:36
12	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-06 17:04:03	16-01-06 17:05:56
13	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-06 05:11:50	16-01-06 05:16:52
14	4	http://172.18.34.107	xss,sqli,osi,csrf	快速模式	16-01-06 05:11:56	16-01-06 05:12:08
15	4	http://172.18.34.107	xss,sqli,osi,csrf	快速模式	16-01-06 01:32:43	16-01-06 01:32:49
16	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-06 01:27:04	16-01-06 01:32:00
17	4	http://172.18.34.107	xss,sqli,osi,csrf	快速模式	16-01-06 01:30:55	16-01-06 01:31:03
18	4	http://172.18.34.107	xss,sqli,osi,csrf	快速模式	16-01-06 01:29:55	16-01-06 01:30:03
19	4	http://172.18.34.106	xss,sqli,osi,csrf	快速模式	16-01-06 01:28:53	16-01-06 01:28:54
20	4	http://172.18.34.106	xss,sqli,osi,csrf	快速模式	16-01-06 01:27:07	16-01-06 01:27:07
21	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-06 01:21:17	16-01-06 01:25:45
22	4	http://172.18.34.106	xss,sqli,osi,csrf	快速模式	16-01-06 01:25:36	16-01-06 01:25:37
23	123	192.168.67.111	xss,sqli,osi,csrf	快速模式	16-01-06 01:15:34	16-01-06 01:20:15

CLI 方式

waf vulnerability-scan-policy add name <*mstring*> **url** <*mstring*> [**scantype** <*mstring*>] [**mode** <fast|deep>] [**formats** <*mstring*>] [**schedule** <none|daily|weekly|monthly>] [**attime** <*time*>] [**weekdays** < *mstring*>] [**mondays** < *mstring*>] [**auth** <on|off>] [**auth-username** < *mstring*>] [**auth-passwd** < *mstring*>] [**mail-policy** < *mstring*>] [**subject** <*mstring*>] [**body** <*mstring*>] [**auth-domain** <*mstring*>]

命令描述：

添加漏洞扫描策略。

可使用 **waf vulnerability-scan-policy delete** 命令删除漏洞扫描策略。

可使用 **waf vulnerability-scan-policy modify** 命令修改漏洞扫描策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置漏洞扫描策略名称。 字符串类型，支持数字、字母、中文和特殊字符“_-*.”，不以“\\”结尾且不包含“<script>”字符串。
url <*mstring*>	必选项，设置扫描的网站地址。 字符串类型，支持 IP 地址和 URL 域名形式，不以“\\”

参数	说明
	结尾且不包含“<script>”字符串。
scantype <*mstring*>	可选项，设置扫描漏洞的类型。 字符串类型，可选项：xss、csrf、sqli、osi、rfi、dir、leak、ldap、xpath、ssi、other、。支持多个输入形式，多个输入间用逗号分隔，例如“xss,csrf”。可使用可使用 **waf enumeration scantypes** <cr>命令查看 TopWAF 支持的告警策略支持的事件类型。
mode <fast|deep>	可选项，设置扫描模式。快速扫描|深度扫描，默认值：快速扫描。
formats <*mstring*>	可选项，设置报表文件的格式。 字符串类型，可选项：html、pdf、txt 和 xml。
schedule <none|daily|weekly|monthly>	可选项，设置定期扫描计划。无|每日发送|每周发送|每月发送，默认为无，表示不进行定扫描。
attime <*time*>	可选项，设置 **schedule** 为每日发送、每周发送或每月发送时，设置该参数，设置每日定时发送时间。 时间类型，格式为:“hour:minute:second”，如 08:12:30。
weekdays <*mstring*>	可选项，设置 **schedule** 为每周发送时，设置该参数，设置每周定时发送时间。 字符串类型，表示星期，可选项：mon、tue、wed、thu、fri、sat、sun，分别表示星期一、星期二、星期三、星期四、星期五、星期六、星期日。支持多输入形式，多个输入用逗号分隔，如“mon,tue”，表示星期一和星期二。
mondays < *mstring*>	可选项，设置 schedule 为每月发送时，设置该参数，设置每月定时发送时间。 字符串类型，取值范围：1-31，支持多输入形式，多个输入用逗号分隔，如“1,22”，表示每月的 1 日和 22 日。
auth <on|off>	可选项，设置是否开启邮件认证开关。 开启|关闭，默认值：关闭。
auth-username<*mstring*>	可选项，设置“auth”为 on 后，可设置发件人帐户对应的用户名。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-63。
auth-passwd <*mstring*>	可选项，设置“auth”为 on 后，可设置发件人帐户对应的用户密码。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-127。
mail-policy <*mstring*>	可选项，设置引用的邮件策略名称。 字符串类型，不以“\\”结尾且不包含“<script>”字

参数	说明
	符串。
subject <*mstring*>]	可选项，设置邮件的标题。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。长度范围：1-127；单位：字符；默认值：“TopWAF攻击告警报告”。
body <*mstring*>	可选项，设置邮件内容。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-2047。
auth-domain <*mstring*>	必须项，设置认证 domain。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-255。

命令示例：

添加一条名称为“v-report”的漏洞扫描策略，指定漏洞扫描指定的服务器地址为 192.168.3.3，每周的周日和周一的 23:12:12 定时扫描。

TopsecOS# **waf vulnerability-scan-policy add name** *v-report* **url** 192.168.3.3 **schedule** weekly **weekdays** *mon,sun* **attime** *23:12:12*

waf vulnerability-scan-policy show [**name** <*mstring*>]

命令描述：

查看漏洞扫描策略配置信息。

命令示例：

查看 v-policy 漏洞扫描策略的配置信息。

TopsecOS# **waf vulnerability-scan-policy show name** *v-policy*

profile Name: v-policy

Url: 2.3.3.3

Leaktype: xss,csrf,sqli,osi

Authenticate: off

Mode: fast

```
Schedule:          weekly
Formats:           pdf,xml
Attime:            23:12:12
Weekdays:          mon,sun
Monthdays:
Subject:           TopWAF 漏洞扫描报告
Body:              TopWAF 漏洞扫描结果。由漏洞扫描进程发送。
Username:
Password:
Auth domain:
Mailpolicy:
```

waf enumeration scantypes <cr>

命令描述：

查看漏洞扫描支持的漏扫类型。

命令示例：

```
TopsecOS# waf enumeration scantypes
type:xss          Description:  跨站脚本攻击
type:sqli         Description:  SQL 注入攻击
type:osi          Description:  操作系统命令注入攻击
type:rfi          Description:  远程文件包含攻击
type:dir          Description:  路径遍历攻击
type:leak         Description:  信息泄露攻击
type:ldap         Description:  LDAP 注入攻击
type:other        Description:  其他攻击
type:xpath        Description:  XPath 注入攻击
type:ssi          Description:  SSI 注入攻击
type:csrf         Description:  跨站请求伪造攻击
```

waf vulnerability-scan-policy clean <cr>

命令描述：

清除漏洞扫描策略配置信息。

waf vulnerability-scan-policy start name <*mstring*>

命令描述：

启动漏洞扫描策略。

waf vulnerability-scan-policy stop name <*mstring*>

命令描述：

停止漏洞扫描策略。

waf vulnerability-scan-policy history <cr>

命令描述：

查看漏洞扫描历史记录。

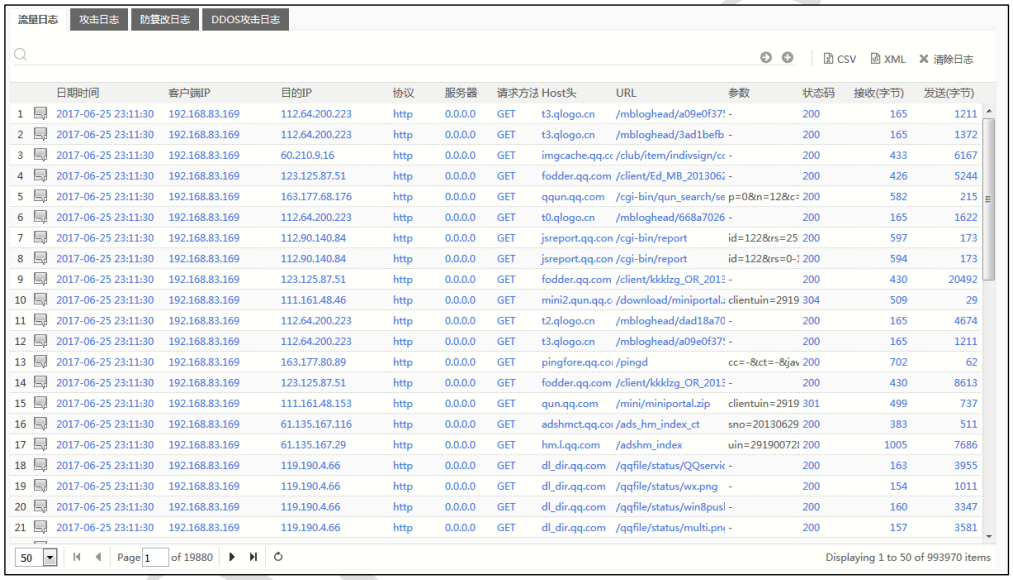
- 。
- DDoS 攻击日志：DDoS 攻击日志用来记录 TopWAF 系统抓取的通往防护对象的攻击数据包的攻击类型、攻击状态、攻击流量及相应的系统防御措施等信息。通过查看攻击日志，管理员可以查看某个时间段内防护对象受到 DDoS 攻击的具体情况，以及系统针对各种 DDoS 攻击的检测和防御情况的记录，了解曾经发生和正在发生的攻击事件，并做出策略调整或主动防御。
- 管理日志：管理日志记录了 TopWAF 运行期间配置管理的日志信息。
- 管理员登录日志：管理员登录日志记录了管理员登录 TopWAF 进行管理的日志信息。
- 系统运行日志：系统运行日志记录了 TopWAF 有关系统运行状况的日志。管理员可通过查看系统运行日志，跟踪 TopWAF 的工作状态。
- 本地服务日志：本地服务日志记录了 TopWAF 提供的管理服务的日志信息。

- 调试日志：调试日志用来记录 TopWAF 的处理请求报文和响应报文时产生的调试信息，仅供开发人员使用。

TopWAF 将各个功能的日志分开显示，操作方式类似，下面以安全日志中的流量日志为例介绍如何查看、查询和删除日志。

WEBUI 方式

步骤1 选择 **监控** > **日志查看** > **安全日志**，激活“流量日志”页签，如下图所示。



在查看流量日志时，各项参数的具体说明如下表所示。

参数	说明
日期时间	表示客户端访问 Web 服务器的具体时间。
客户端 IP	表示访问 Web 服务器的客户端 IP 地址。
目的 IP	表示被访问的 Web 服务器 IP 地址。
协议	表示协议类型，包括：http、https。
服务器	表示服务器策略名称。
请求方法	表示 HTTP 请求方法。 GET：请求服务器向客户端发送资源； POST：客户端向服务器发送请求数据； HEAD：类似于 GET，但仅发送资源响应中的 HTTP 首部； OPTIONS：客户端可以发现服务器或其某个特定资源所支持的功能。
Host 头	表示客户端访问的服务器的主机头。
URL	表示客户端访问的服务器的具体页面。
参数	表示请求参数。

参数	说明
状态码	HTTP 状态码，为客户端提供一种理解事务处理结果的便捷方式。 200：OK，文档正确返回。 302：Redirect（重定向），到其他地方去获取资源。 404：Not Found（没找到），无法找到这个资源。 100-199：信息性状态码，200-299：成功状态码，300-399：重定向状态码，400-499：客户端错误状态码，500-599：服务器错误状态码。
接收/发送	表示服务器接收到的客户端的报文个数|服务器发送给客户端的报文个数

步骤2 添加查询条件。

1）点击“⊕”，弹出查询条件窗口。

2）设置查询条件，然后点击【添加】按钮，查询条件可显示在查询条件文本框中，可继续设置多个查询条件，每设置完一个查询条件点击【添加】按钮，设置完成全部的查询条件后，点击【完成】，完成查询条件设置。

3）点击“⊙”，与设置查询条件匹配的日志信息将显示在日志列表中。

✧ 可以通过点击日志信息的某个字段添加查询条件。支持多个查询条件，多个查询条件直接“与”的关系，通过多次点击不同的字段实现。例如，点击请求方法下的“POST”，在搜索框中将会显示“(method eq POST)”，再次点击“响应码”下的“403”，此时搜索框显示“(method eq POST) and (status eq 403)”，点击“⊙”，与设置查询条件匹配的日志信息将显示在日志列表中。

步骤3 以 CSV 格式文件导出日志信息。

点击『CSV』，弹出选择导出日志条数的界面，选择要导出的日志条数，如下图所示。

点击【确定】按钮，弹出保存 CSV 格式文件的窗口进行文件的打开或保存操作，并弹出“日志导出成功，请等待文件下载完毕”的提示信息。

步骤4 以 XML 格式文件导出日志信息。

点击『XML』，弹出选择导出日志条数的界面，选择要导出的日志条数，如下图所示。

点击【确定】按钮，弹出保存 XML 格式文件的窗口进行文件的打开或保存操作，并弹出“日志导出成功，请等待文件下载完毕”的提示信息。

步骤5 按照条件清除日志。

1）点击『清除日志』，弹出“清除日志”窗口，如下图所示。

2）设备支持按照比例清除和按照时间段清除日志信息。

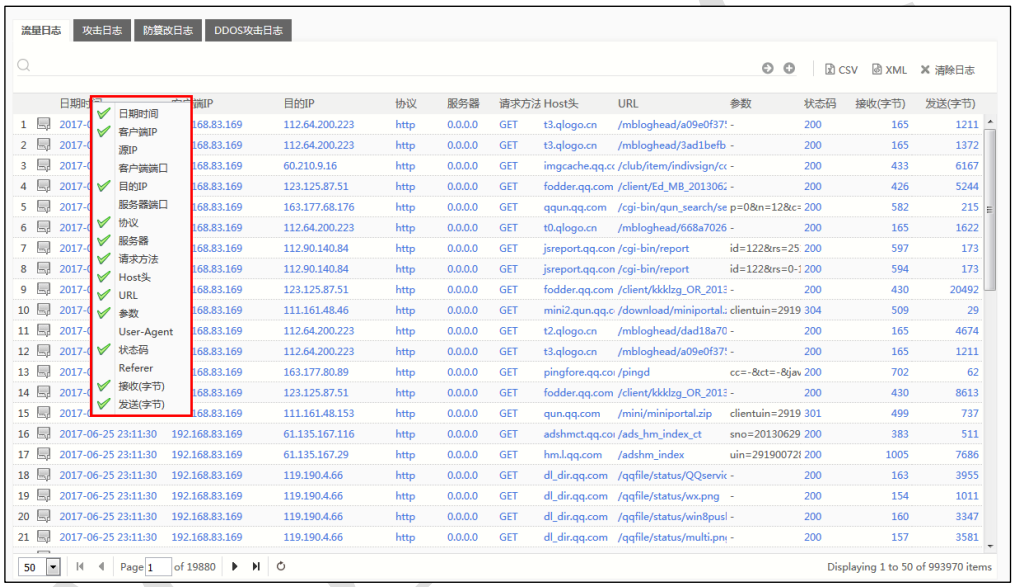
- 按比例删除：设置清除的日志所占设备总日志数量的比例，可选项 30%、50%、80%和全部；默认值：全部。假设 N=现有设备中日志的总数量*所设比例的清除比例，将清除设备中 N 条时间较早的日志信息。
- 按时间删除：设置清除日志的时间，将清除设备中早于该时间的日志信息。

3）配置完成后，点击【确定】按钮，完成清除日志。

步骤6 筛选日志显示列、排序日志信息。

1）筛选日志显示列

滑动鼠标至标题行，右击标题行，可以在弹出的菜单中勾选相应的列选项，筛选可显示的日志列信息，如下图所示。



2）按列排序日志信息

滑动鼠标至标题行，点击标题行指定列，可按照该列升序显示日志信息，此时该列图标将显示“▲”，再次点击该列标题，图标将变为“▼”，表示将按照降序显示日志信息。

CLI 方式

log message show from <*num*> **to** <*num*> [**keyword** <*string*>] [**level** <*num*>] [**type** <anti-tamper|audit|debug|mgmt|mgmtlogin|pf|system|traffic|ddos>] [**date_range** <*string*>]

命令描述：

查看日志的内容。

参数说明：

参数	说明
from <*num*>	必选项，设置读取日志的起始位置。实数类型，取值范围：1-2048。
to <*num*>	必选项，设置读取日志的结束位置。实数类型，取值范围：1-2048。
keyword <*string*>	可选项，设置检索日志的关键词。字符串类型。
level <*num*>	可选项，设置当前日志的级别。实数类型，取值范围：0-7。 0：紧急 1：告警 2：严重 3：错误 4：警示 5：通知 6：信息 7：调试
type <anti-tamper|audit|debug|mgmt|mgmtlogin|pf|system|traffic|ddos>	可选项，设置当前日志的类型。 防篡改日志|WAF 攻击日志|调试日志|管理日志|管理员登录日志|pf 日志|系统日志|流量日志|DDoS 攻击日志
date_range <*string*>	可选项，设置查看当前日志的时间范围。 字符串类型，格式为 YYYYMMDD-YYYYMMDD。其中，Y 表示年，M 表示月，D 表示日。

命令示例：

TopsecOS# **log message show from** *1* **keyword** *name* **to** *2048* **type** system **date_range** *20131011-20141010*

log message clean <cr>

命令描述：

清除日志信息。

log stat show<cr>

命令描述：

显示日志计数。

命令示例：

TopsecOS# **log stat show**

log statistic:

dp_sended:176736428

dp_droped:0

dp_failed:0

mp_sended:38615

mp_droped:0

mp_failed:0

log stat reset <cr>

命令描述：

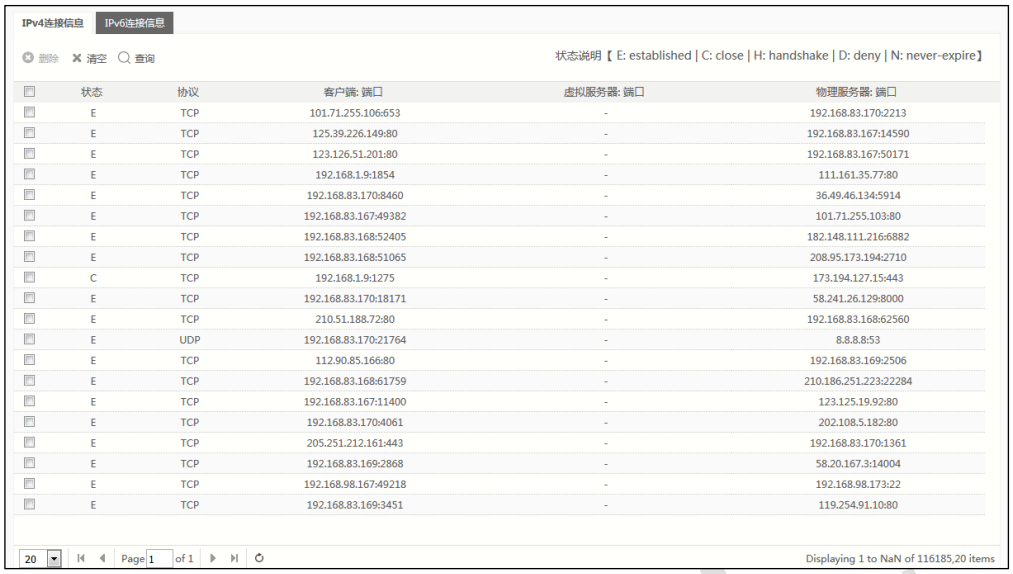
重置日志计数功能。

4.2.2 连接信息

TopWAF 会记录客户端与服务器建立的 IPv4/IPv6 连接的基本信息，包括状态、协议、客户端地址及其端口、虚拟服务器/物理服务器的 IP 地址及其端口。TopWAF 将 IPv4 和 IPv6 连接信息分开显示，操作方式类似，下面以 IPv4 连接信息为例介绍如何查看 TopWAF 的连接信息。

WEBUI 方式

选择 **监控** > **连接信息**，激活“IPv4 连接信息”页签，如下图所示。



在查看 IPv4 连接信息时，各项参数的具体说明如下表所示。

参数	说明
状态	显示连接的状态。 E：表示 established，已连接建立连接。 C：表示 close，已关闭连接。 H：表示 handshake，正在协商连接。 D：表示 deny，已拒绝连接请求。 N:：表示 never-expire，连接永不超时。
协议	显示连接所使用的通信协议。
客户端：端口	显示连接的客户端地址及端口号。
虚拟服务器：端口	显示连接的虚拟服务器地址及端口号。
物理服务器：端口	显示连接的物理服务器地址及端口号。

按条件查找连接信息。

1）点击『查询』，在弹出的“搜索”窗口中设置查询参数，然后符合所有查询参数的连接信息将被筛选出来。

在查询 IPv4 连接信息时，各项参数的具体说明如下表所示。

参数	说明
协议	设置需要查询的连接所使用的通信协议。
客户端 IP	设置需要查询的连接的客户端地址。
客户端端口	设置需要查询的连接的客户端端口号。
物理服务器 IP	设置需要查询的连接的物理服务器 IP 地址。
物理服务器端口	设置需要查询的连接的物理服务器端口号。

- ✧ 当输入多个查询参数时，同时满足所有的查询条件的连接信息才会显示在列表中。
- ✧ 如果不设置某个查询参数表示该参数不做限制。

2）点击【确定】按钮，完成查询。

选择一条或多条连接信息，点击『删除』，连接信息将被删除；点击『清空』，所有连接信息将被清空。

CLI 方式

network session search [**family** <ipv4|ipv6>] [**saddr** <*string*>] [**sport** <*num*>] [**daddr** <*string*>] [**dport** <*num*>] [**protocol** <*string*>] [**from** <*num*>] [**num** <*num*>] [**flags** <on|off>] **[app_name** <*string*>] [**vsys_name** <*string*>] [**user_name** <*string*>]

命令描述：

根据输入条件显示连接信息。

参数说明：

参数	说明
app_name <*string*>	可选项，设置应用协议名称。字符串类型。
daddr <*string*>	可选项，设置目的 IP 地址。字符串类型。
dport <*num*>	可选项，设置目的端口。实数类型。取值范围：1-65535。
family <ipv4|ipv6>	可选项，设置协议类型。默认值：ipv4。 IPv4 协议|IPv6 协议
flags <on|off>	可选项，设置是否显示内部标志。默认不显示。 显示|不显示
from <*num*>	可选项，设置从第几个连接开始显示连接信息，默认从第一个连接开始显示。实数类型。
num <*num*>	可选项，设置需要显示的连接数目。实数类型。最大值：256；默认值：20。
protocol <*string*>	可选项，设置协议类型，可选项：TCP、UDP、ICMP、ICMPv6。字符串类型。
saddr <*string*>	可选项，设置源 IP 地址。字符串类型。
sport <*num*>	可选项，设置源端口。实数类型。取值范围：1-65535。
vsys_name <*string*>	可选项，设置虚系统名称。字符串类型。
user_name <*string*>	可选项，设置用户名称。字符串类型。

network session clean

命令描述：

删除所有连接信息。

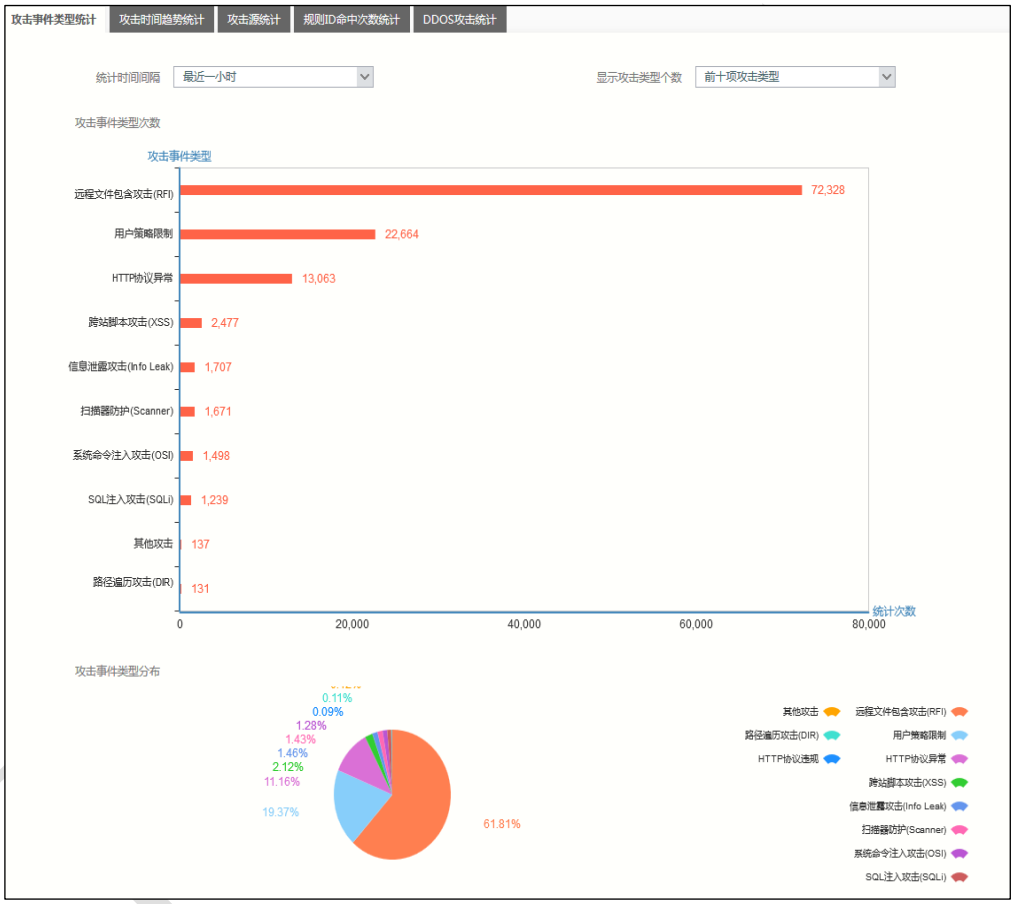
4.2.3 威胁统计

TopWAF 提供威胁统计功能，能够分析攻击类型、攻击次数、攻击流量趋势等信息，并以图表的形式展示。

步骤1 选择 **监控** > **威胁统计**

步骤2 查看攻击事件类型统计信息。

激活“攻击事件类型统计”页签，如下图所示。

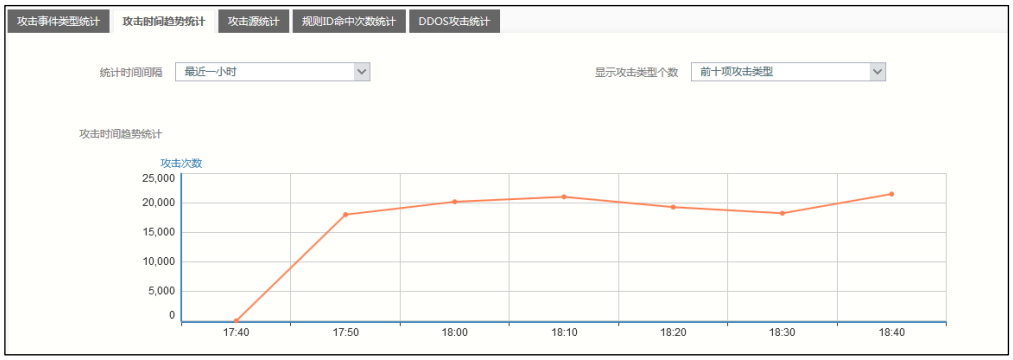


界面上方以柱状图显示各个攻击事件类型的次数统计信息，界面下方以饼状图显示各个攻击事件类型占总的攻击事件的百分比。

点击界面左上角的下拉列表选择统计时间间隔；点击界面右上角的下拉列表选择攻击类型的显示个数。

步骤3 查看攻击时间趋势统计信息。

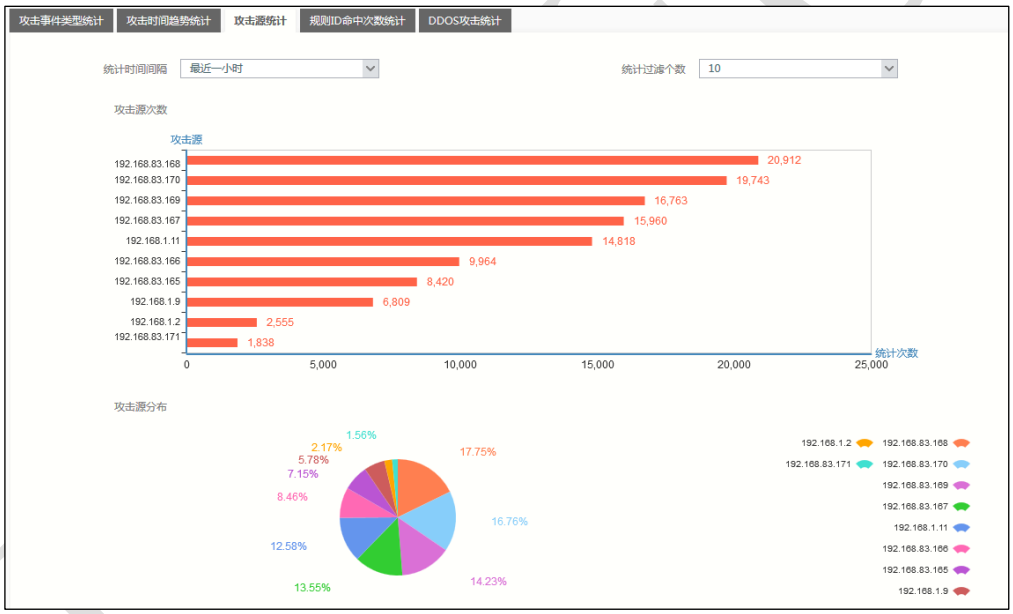
激活“攻击时间趋势统计”页签，如下图所示。



界面以曲线图显示攻击事件数量随着时间变化的趋势。点击界面左上角的下拉列表选择统计时间间隔；点击界面右上角的下拉列表选择攻击类型的显示个数。

步骤4 查看攻击源统计信息。

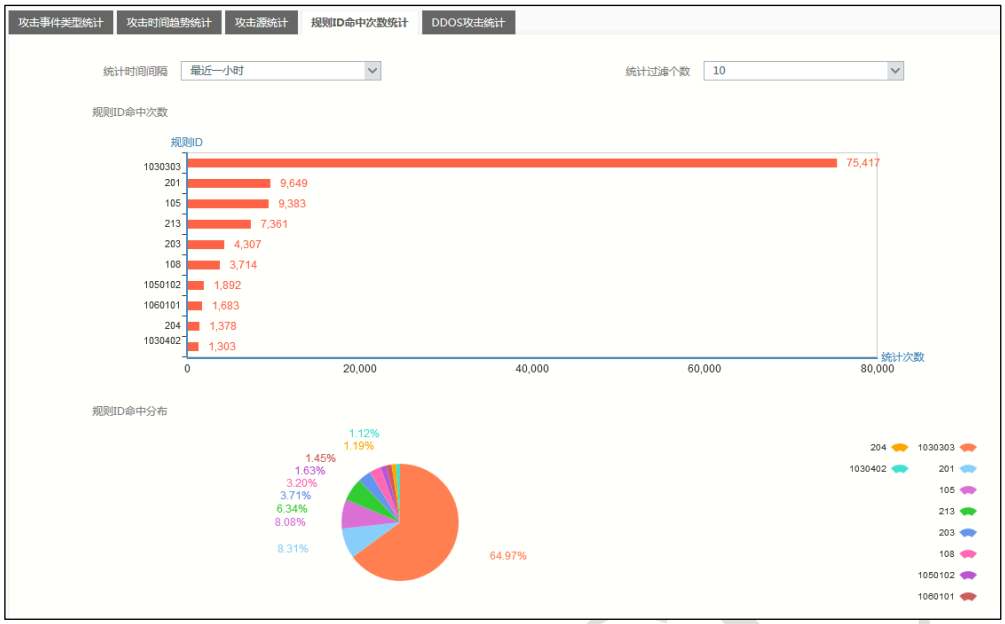
激活“攻击源统计”页签，如下图所示。



界面上方以柱状图显示各个攻击源的攻击次数统计信息，界面下方以饼状图显示各个攻击源的攻击次数占总数的百分比。点击界面左上角的下拉列表选择统计时间间隔；点击界面右上角的下拉列表选择攻击源的显示个数。

步骤5 查看规则 ID 命中统计信息。

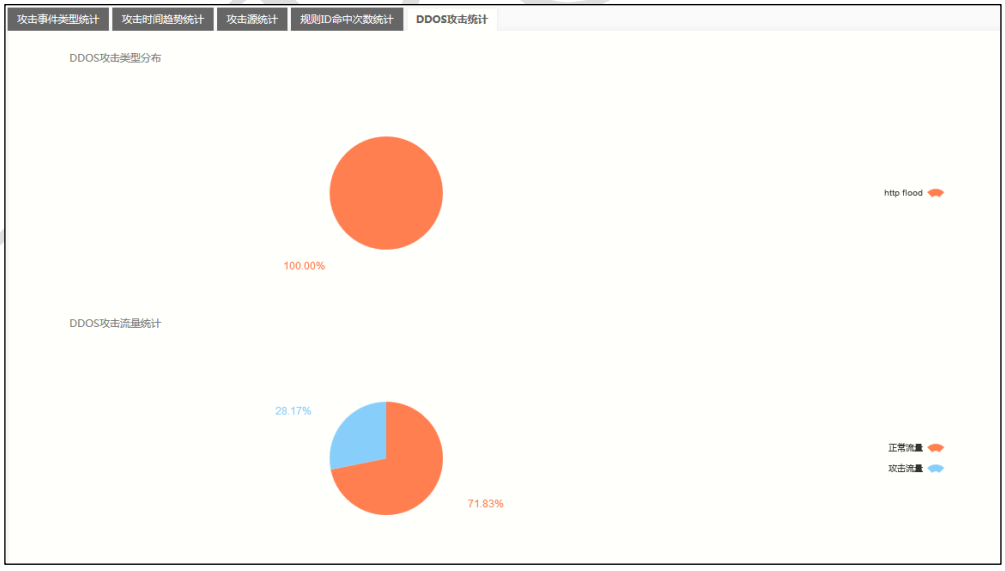
激活“规则 ID 命中次数统计”页签，如下图所示。



界面上方以柱状图显示各个规则 ID 命中攻击事件数量的统计信息，界面下方以饼状图显示各个规则 ID 命中的的攻击事件占总数的百分比。点击界面左上角的下拉列表选择统计时间间隔；点击界面右上角的下拉列表选择规则 ID 的显示个数。

步骤6 查看 DDoS 攻击统计信息。

激活“DDoS 攻击统计”页签，如下图所示。

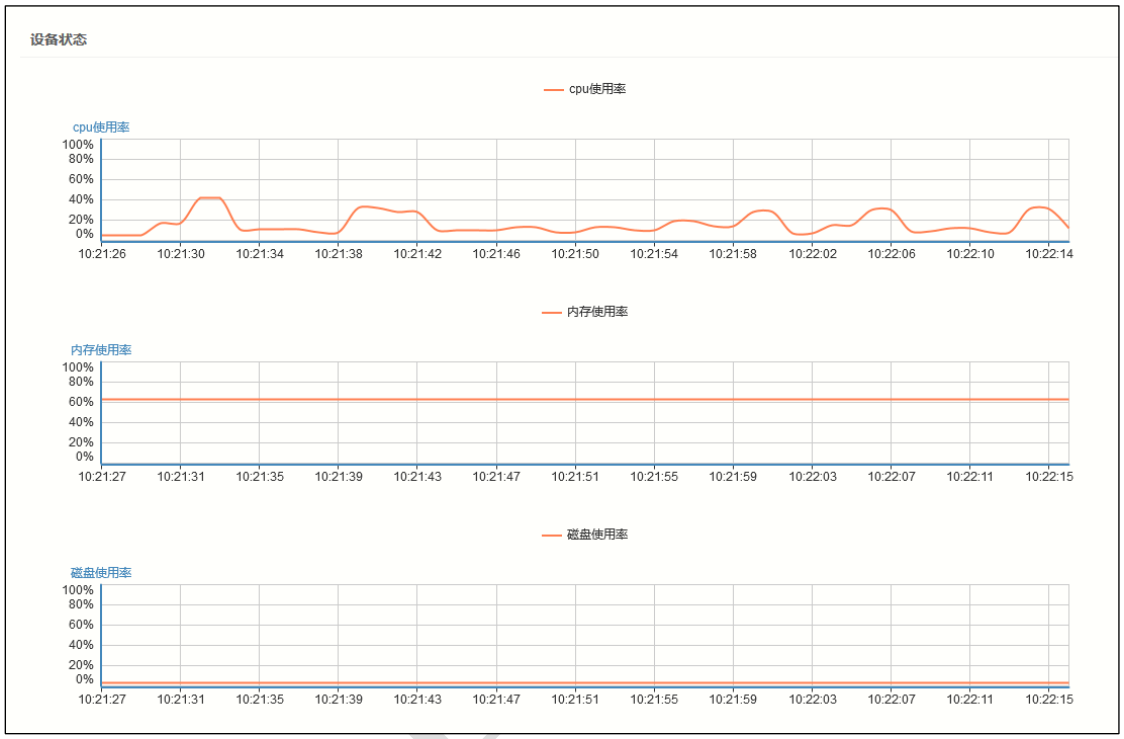


界面上方以饼状图的形式显示攻击类型分布，界面下方以饼状图的形式显示攻击流量与正常流量的百分比。

4.2.4 设备状态

管理员通过查看设备状态信息，可以了解硬件资源（磁盘、内存、CPU）的使用率。

选择 **监控** > **设备状态**，如下图所示。

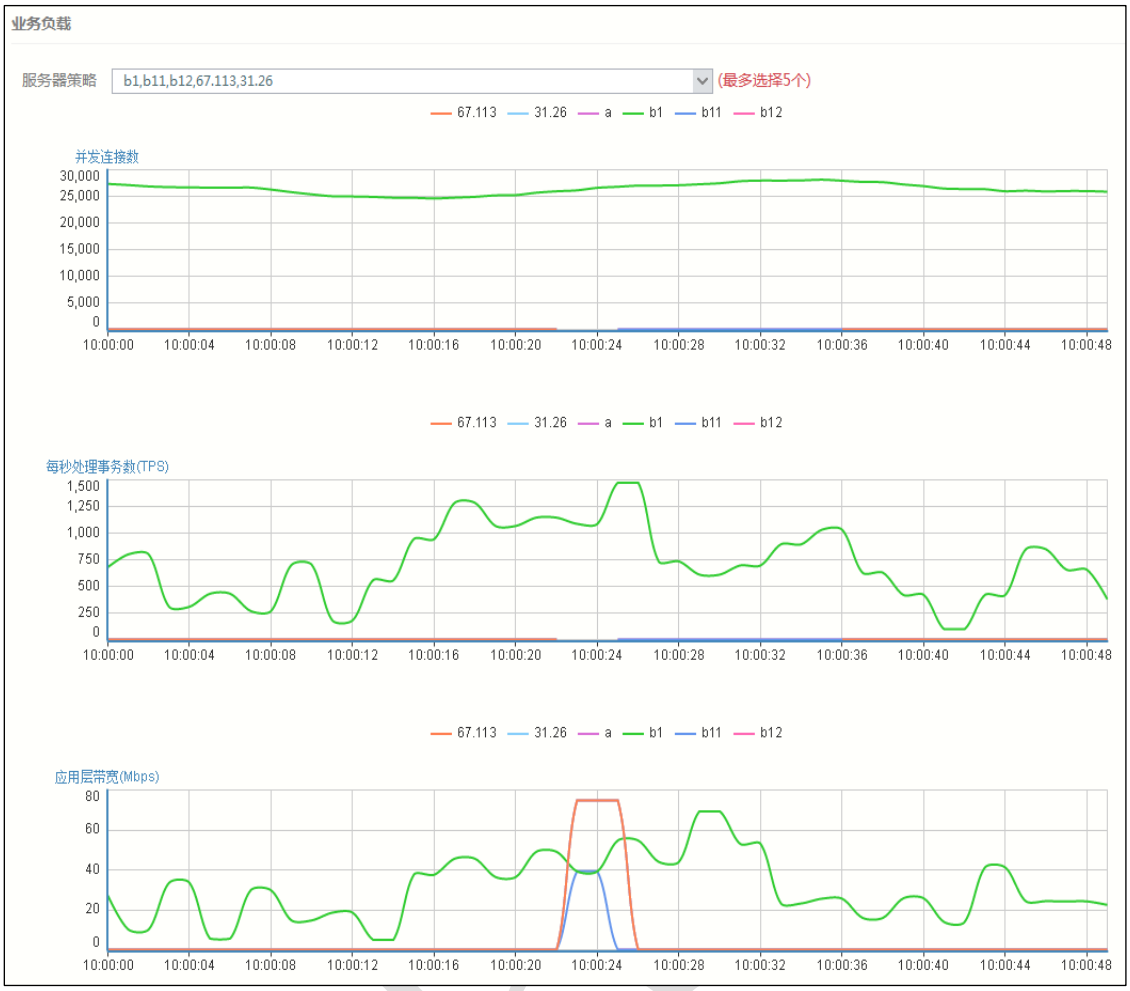


4.2.5 业务负载

业务负载显示被保护站点的并发连接数、每秒处理事务数（TPS）和应用层带宽（bps/Kbps/Mbps），以曲线图显示。关于服务器策略的配置具体请参见 5.3 服务器策略。

WEBUI 方式

选择 **监控** > **业务负载**，如下图所示。



TopWAF 业务负载显示 TopWAF 每一条服务器策略的并发连接数、每秒处理事务数（TPS）和应用层带宽（bps/Kbps/Mbps），以折线图显示。关于服务器策略的配置具体请参见 5.3 服务器策略。

通过服务器策略下拉列表可选择界面中显示的服务器策略的业务负载曲线，最多可以选择 5 个服务器策略。

CLI 方式

waf statistics show [**server-policy** <*mstring*>]

命令描述：

查看安全策略信息。

参数说明：

参数	说明
server-policy <*mstring*>	可选项，设置服务器策略名称。 字符串类型。不以\\'结尾、或不包含"<script>"的字符串。

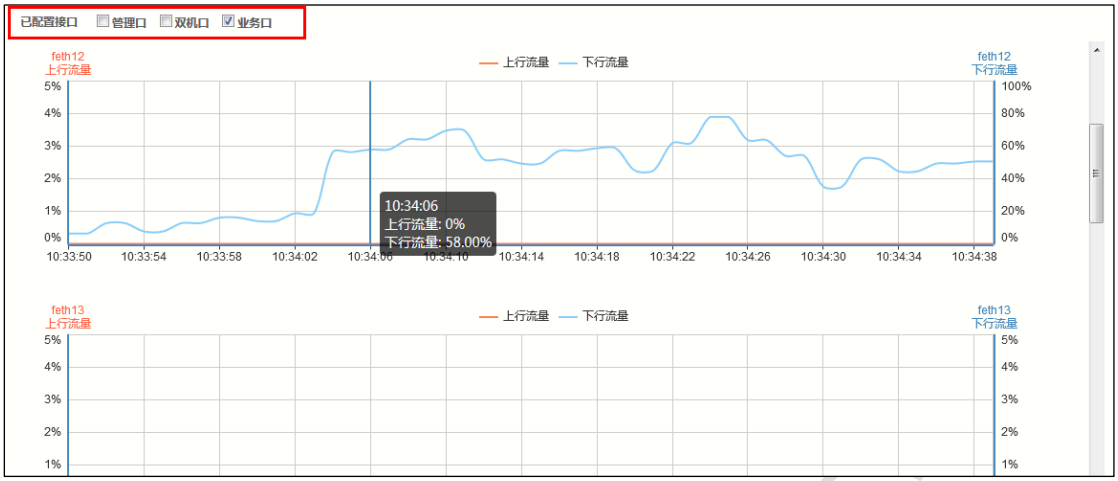
命令示例：

```
TopsecOS# waf statistics show
server-policy:      60
connections:        0
requests:           0
bandwidth:          0.00(bps)
server-policy:      0.0.0.0
connections:        25093
requests:           557
bandwidth:          28.10(Mbps)
```

4.2.6 接口流量

接口流量显示每个链路正常连接的接口的上行流量和下行流量的实时曲线图。管理员可以选择相应类型的接口，当接口正常工作时，下方将会显示相应接口流量信息。

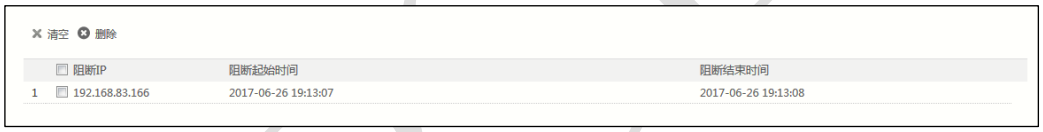
选择 **监控** > **接口流量**，此时将鼠标移动至曲线图区域，将显示具体的上传流量及下载流量信息，如下图所示。



4.2.7 动态阻断

动态阻断界面显示系统在运行策略的过程中被阻断的 IP 信息、阻断起始时间和阻断结束时间。

步骤1 选择 **监控** > **动态阻断**，如下图所示。



步骤2 选择一条或多条动态阻断信息，点击『删除』，阻断信息将被删除；点击『清空』，所有阻断信息将被清空。

5 Web 防护

黑客可利用安全漏洞攻击 Web 服务器，执行篡改网站页面、盗取账户密码等非法操作，危害网站安全。通过合理部署 TopWAF，可有效抵御黑客攻击，其中，“WEB 防护”是 TopWAF 的核心功能，根据其服务器策略对通过 TopWAF 的 HTTP（S）请求、响应进行检测，允许符合策略的合法请求通过 TopWAF 访问 Web 服务器，拦截非法请求，保护 Web 服务器免受来自黑客的攻击同时，保障正常用户的访问。

TopWAF 需部署在服务器前端，如下图所示。TopWAF 部署在最靠近 Web 服务器一侧，所有访问 Web 服务器的 HTTP（S）请求都要流经 TopWAF。

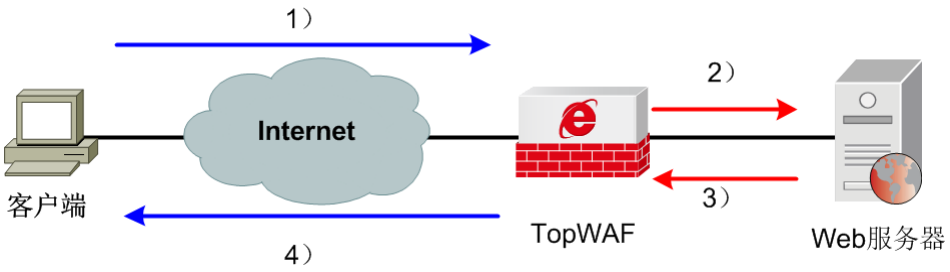


图 5-1 客户端通过 TopWAF 与服务器交互过程示意图

客户端访问由 TopWAF 防护的 Web 服务器的工作过程如下所示。

1）客户端发起 HTTP（S）请求。

2）TopWAF 接收客户端的 HTTP/HTTPS 请求，然后解析这些请求，然后将请求与服务器安全防护策略相匹配。如果这个请求未被任何的防护策略阻断，则将该请求转发给 Web 服务器；否则，拒绝该请求。

3）Web 服务器返回 HTTP（S）响应。

4）TopWAF 收到 Web 服务器的响应之后，进行解析，然后与安全策略相匹配。如果服务器响应未触发任何安全策略，则将服务器响应转发给客户端；否则，丢弃该响应。

“WEB 防护”主要包含以下几个部分：

- 服务器对象：用于在配置安全策略和服务器策略时进行引用。
- 安全策略：介绍如何配置从各安全角度防护服务器的安全策略，安全策略在服务器策略中被引用后才能生效。
- 服务器策略：服务器策略直接对 WEB 网站生效。
- 自学习报告：管理自学习报告，自学习报告结果可应用到 URL 例外的参数列表中。
- 邮件策略：指定邮件服务器、发件人地址和收件人地址。告警策略和报表策略通过引用邮件策略，根据邮件策略发送告警信息或报表。
- 告警策略：指定产生告警的攻击类型、发送告警时间计划表和告警方式。当服务器策略引用了告警策略，TopWAF 根据告警策略自动发送告警邮件或告警短信。
- 报表策略：统计一段时间间隔内的数据信息，形成报表，并制定报表发送计划。
- 漏洞扫描：介绍如何配置漏洞扫描策略，并查看漏洞扫描历史记录。
- 网页防篡改：介绍如何配置网页防篡改功能，并查看网站签名和清理缓存信息。

5.1 服务器对象

服务器对象，定义了安全策略和服务器策略某些公共参数，用于在配置安全策略和服务器策略时进行引用。合理地构建对象能够大大简化管理员对 TopWAF 的管理工作，当某个对象发生变化时，管理员只需要修改对象本身即可，而无需逐一地修改所有引用该对象的策略。

在 TopWAF 中，管理员可以定义的对象的类型包括：

- IP 黑白名单：IP 黑白名单是 IPv4 地址或 IPv6 地址的集合，用于服务器策略识别一个客户端 IP 是来自信任网络还是来自黑名单网络。
- 虚拟主机组：定义主机名，管理员可对指定的虚拟主机进行安全防护。
- 服务器组：定义服务器组所包含的服务器对象及其权重。
- 健康检查：定义健康检查对象，用于检查服务器是否可用。
- 爬虫：定义爬虫对象，用于限制恶意爬虫访问 Web 网站。
- 数据类型：定义数据类型，用于限制用户提交的参数、识别服务器响应中的敏感数据。
- 错误页面：定义错误页面对象，当用户请求访问服务器出现错误时，根据 HTTP 的不同状态码返回不同的错误页面。
- 证书：导入证书文件，用于实现对客户端与服务器的加密信息进行安全防护。

- 用户登录页面：定义用户登录页面的认证方式，用于防范暴力登录。

5.1.1 IP 黑白名单

IP 黑白名单是 IPv4 地址或 IPv6 地址的集合，可以将 IP/网段定义为 white/black 类型，用于服务器策略识别一个客户端 IP 是来自信任网络还是来自黑名单网络，对于信任网络，可以设置不进行防护规则处理直接转发请求，对于黑名单类型网络，会被 TopWAF 阻断请求。

WEBUI 方式

步骤1 选择 **Web 防护 > 服务器对象 > IP 黑白名单**。

步骤2 点击『添加』，弹出“添加 IP 黑白名单”窗口，如下图所示。

步骤3 点击窗口中的『添加』，在 IP 黑白名单中添加 IP 地址，并配置相关参数。

在添加 IP 黑白名单时，各项参数的具体说明如下表所示。

参数	说明
名称	设置 IP 黑白名单名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
IP 地址	设置 IP 地址，支持 IPv4 地址和 IPv6 地址。TopWAF 每个 IP 黑白名单最多支持添加 128 个 IP 地址。
掩码（IPv4）/前缀（IPv6）	设置 IPv4 地址的掩码或者 IPv6 地址的前缀。 1）IPv4 地址：输入 IPv4 地址的子网掩码。如果设置为 32 表示添加的

参数	说明
	地址为 IPv4 主机地址，如果设置为 1-31，表示添加地址为 IPv4 子网地址。 2）IPv6 地址：输入 IPv6 地址的前缀。如果设置为 128 表示添加的地址为 IPv6 主机地址，如果设置为 1-127，表示添加地址为 IPv6 子网地址。
类型	设置该 IP 地址的类型。 白名单：该地址为可信地址，可不对来自该地址的请求报文进行安全策略过滤。 黑名单：该地址为黑名单地址，对该来自地址的请求报文直接丢弃。

步骤4 参数配置完成后，点击【确定】按钮，完成 IP 黑白名单的添加。

CLI 方式

waf ip-group add name <*mstring*> [**address** <*string*>]

命令描述：

添加 IP 黑白名单。

可使用 **waf ip-group delete name** <*mstring*>命令删除 IP 黑白名单。

可使用 **waf ip-group modify name** <*mstring*> [**address** <*string*>]命令修改 IP 黑白名单。

参数说明：

参数	说明
name <*mstring*>	必选项，设置 IP 黑白名单名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
address <*string*>	设置地址，字符串类型，格式为：“IPv4 地址/掩码,可信度”或者“IPv6 地址/前缀,可信度”。其中掩码和前缀为可选项，默认值：掩码为 32，前缀为 128。可信度的取值为 white 和 black，分别表示可信地址和不可信地址，默认为 black。 支持多个输入形式，多个输入直接用“|”分隔，如“192.168.101.2,white|192.168.99.3/24,black”。 注意：不包含“&\"\\'%<>”和空格。

命令示例：

添加名称为 *ip-group* 的 IP 黑白名单，包括信任地址 *192.168.3.2*。

TopsecOS# **waf ip-group add name** *ip-group* **address** *192.168.3.2,white*

waf ip-group add-address name <*mstring*> **address** <*string*>

命令描述：

添加 IP 地址到 IP 黑白名单中。

可使用 **waf ip-group delete-address name** <*mstring*> **address** <*string*>命令删除 IP 黑白名单中的指定 IP 地址。

可使用 **waf ip-group modify name** <*mstring*> **address** <*string*>命令修改 IP 黑白名单中的 IP 地址。

参数说明：

参数	说明
name <*mstring*>	必选项，设置 IP 地址。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
address <*string*>	必选项，设置 IP 地址。字符串类型，表示 IP 地址，格式为：“IPv4 地址/掩码,可信度”或者“IPv6 地址/前缀,可信度”。其中掩码和前缀为可选项，默认值：掩码为 32，前缀为 128。可信度为可选项，取值为 white 和 black，分别表示可信地址和不可信地址，默认为 black。 支持多个输入形式，多个输入直接用“|”分隔，如“192.168.101.2, white |192.168.99.3/24,black”。 注意：不包含“ &\"\\'%<>”和空格。

使用说明：

必须先由 **waf ip-group add name** <*mstring*> **address** <*string*>命令创建 IP 黑白名单，否则添加失败。

可使用 **waf ip-group show** [**name** <*mstring*>]命令查看已创建的 IP 黑白名单信息。

命令示例：

TopsecOS# **waf ip-group add name** *ip-group* **address** *192.168.3.2, white*

TopsecOS# **waf ip-group add-address name** *ip-group* **address** *192.168.1.3*

waf ip-group show [**name** <*mstring*>]

命令描述：

查看 IP 黑白名单配置信息。

参数说明：

参数	说明
name <*mstring*>	可选项，设置 IP 黑白名单名称。字符串类型，表示 IP 黑白名单名称，支持数字、字母、中文和特殊字符“_-*.”。注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

TopsecOS# **waf ip-group show**

Name: ip-group

Addresses:

192.168.3.2/32, type=white

192.168.1.3/32, type=black

waf ip-group clean <cr>

命令描述：

清除所有的 IP 黑白名单配置信息。

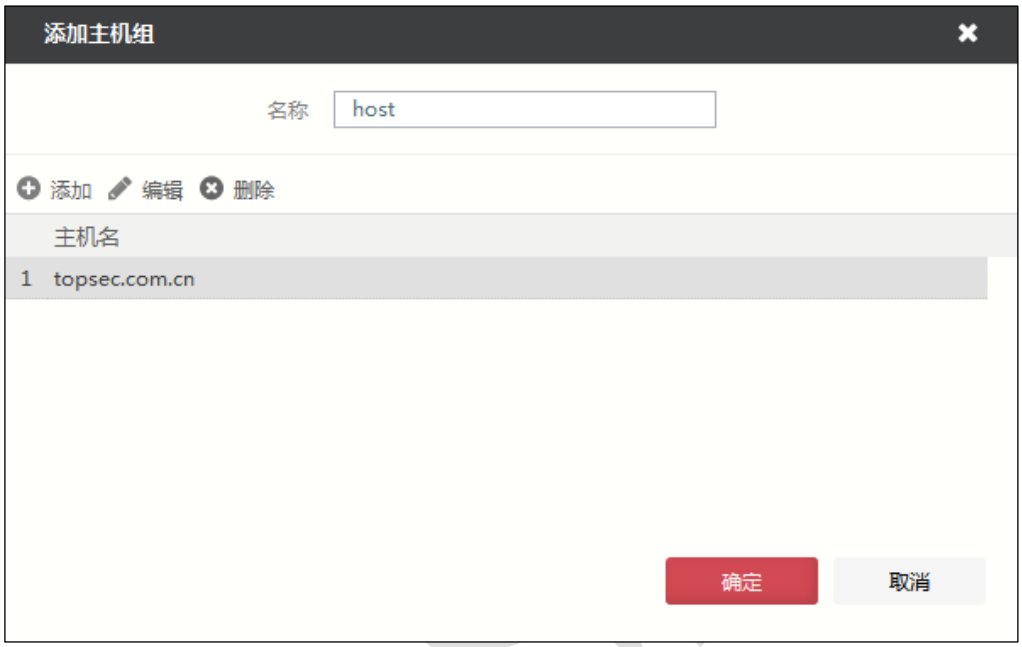
5.1.2 虚拟主机组

虚拟主机组包含一个或多个 IP 地址、完全合格域名(FQDN)，用来指定想保护的真实 WEB 主机或虚拟主机。引擎根据匹配用户请求中的 Host 字段，确定是否对请求进行安全检测。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **虚拟主机组**。

步骤2 点击『添加』，弹出“添加主机组”窗口，如下图所示。



步骤3 点击窗口中的『添加』，在主机组中添加主机名，并配置相关参数。

在添加主机组时，各项参数的具体说明如下表所示。

参数	说明
名称	设置虚拟主机组名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
主机名	设置虚拟主机组中的主机名，支持 IPv4 地址、IPv6 地址和 URL 域名形式。TopWAF 每个虚拟主机组最多支持添加 128 个主机名。

步骤4 参数配置完成后，点击【确定】按钮，完成虚拟主机组的添加。

CLI 方式

waf vhost-group add name <*mstring*> [**hosts** <*string*>]

命令描述：

添加虚拟主机组。

可使用 **waf vhost-group delete name** <*mstring*>命令删除虚拟主机组。

可使用 **waf vhost-group modify name** <*mstring*> [**hosts** <*string*>]命令修改主机组。

参数说明：

参数	说明
name <*mstring*>	必选项，设置虚拟主机组名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
hosts <*string*>	可选项，设置主机名称。字符串类型，支持 IPv4 地址、IPv6 地址和 URL 域名形式。支持多个输入形式，多个输入直接用逗号分隔，如“topsec.com.cn,192.168.3.3”。 注意：不包含“&\"\\'%<>”和空格。

命令示例：

添加主机组，并将主机名 *host1* 添加到主机组中。

TopsecOS# **waf vhost-group add name** *vhost-group* **hosts** *host1*

waf vhost-group add-host name <*mstring*> **hosts** <*string*>

命令描述：

添加主机名到虚拟主机组中。

可使用 **waf vhost-group delete-host name** <*mstring*>命令删除虚拟主机组中指定的主机。

可使用 **waf vhost-group modify name** <*mstring*> **hosts** <*string*>命令修改虚拟主机组中的主机名和地址。

参数说明：

参数	说明
name <*mstring*>	必选项，设置主机组名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
hosts <*string*>	必选项，设置主机名称。字符串类型，支持 IPv4 地址、IPv6 地址和 URL 域名形式。支持多个输入形式，多个输入直

参数	说明
	接用逗号分隔，如“topsec.com.cn,192.168.3.3”。 注意：不包含“&\"\\'%<>”和空格。

使用说明：

必须先由 **waf vhost-group add name** <*mstring*> **hosts** <*string*>命令创建虚拟主机组，否则添加失败。

命令示例：

TopsecOS# **waf vhost-group add name** *vhost-group* **hosts** *host1*

TopsecOS# **waf vhost-group add-host name** *vhost-group* **hosts** *192.168.1.3*

waf vhost-group show [**name** <*mstring*>]

命令描述：

查看虚拟主机组配置信息。

参数说明：

参数	说明
name <*mstring*>	可选项，设置主机组名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

TopsecOS# **waf vhost-group show**

Name: vhost-group

Hosts: host1

192.168.1.3

waf vhost-group clean <cr>

命令描述：

清除所有的虚拟主机组配置信息。

5.1.3 服务器组

5.1.3.1 服务器组

服务器组是一个集合，成员是 TopWAF 保护的服务器。

在 Web 保护、离线检测模式下，在同一个服务器组中的服务器应用相同的安全策略，提高了策略管理的方便性。

在负载均衡、反向代理模式下，服务器组中的多个服务器对象还可以按照不同方式组合进行负载分担，适用于多个服务器对外提供相同的服务，对外使用同一个公网 IP 地址，共同分担用户访问流量的场景。当某些服务器发生故障时，TopWAF 可以忽略故障服务器把流量分发给服务器组中的其他服务器。

配置服务器组对象后，需要被服务器策略引用才能生效，关于服务器策略的具体配置请参见5.3 服务器策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **服务器组**。

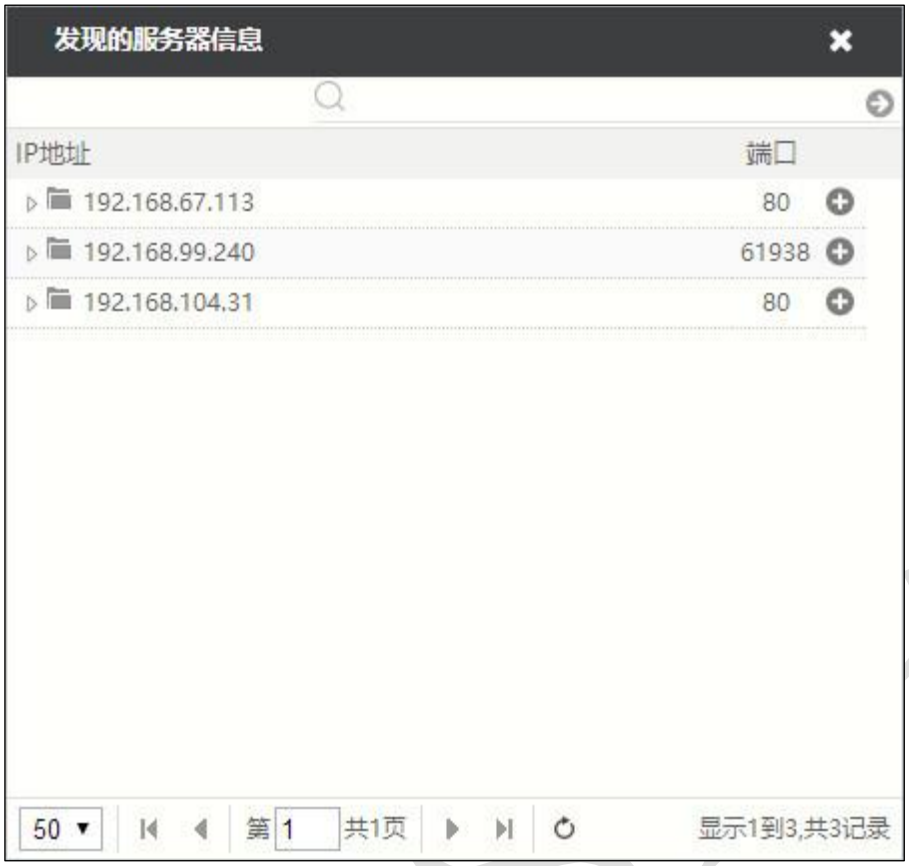
步骤2 点击『添加』，弹出“添加服务器组”窗口，如下图所示。

步骤3 点击窗口中的『添加』，在服务器组中添加 IP 地址，并配置相关参数。

在添加服务器组时，各项参数的具体说明如下表所示。

参数	说明
名称	设置服务器组名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
健康检查	设置是否开启健康检查功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
健康检查策略	选择健康检查策略，关于健康检查策略功能具体请参见 5.1.4 健康检查。
IP 地址	设置 IP 地址，支持 IPv4 地址和 IPv6 地址。TopWAF 每个服务器组最多支持添加 128 个服务器地址。
端口	设置服务器对外提供服务的端口号，数值类型，取值范围：1-65535。
权重	设置服务器地址的权重值，数值越大，当根据权重选择负载均衡方式时，该服务器承担的流量就越大。通常情况下根据服务器的性能或处理能力来定义权重，取值范围：1-10；默认值：5。

步骤4 （可选）点击窗口中的『IP 浏览』或『域名浏览』，可以查看发现服务器功能探测到的网络中的服务器。



点击 IP 地址对应的“⊕”按钮，添加指定的服务器到服务器组中。此时添加的服务器权重默认值为 5，可选中服务器，点击『编辑』，修改服务器参数。

步骤5 参数配置完成后，点击【确定】按钮，完成服务器组的添加。

CLI 方式

waf server-group add name <*mstring*> **servers** <*string*> [**health-enable** <on|off>] [**health-check** <*string*>]

命令描述：

添加服务器组。

可使用 **waf server-group delete name** <*mstring*>命令删除服务器组。

可使用 **waf server-group modify name** <*mstring*> [**servers** <*string*>] [**health-enable** <on|off>] [**health-check** <*string2*>]命令修改服务器组。

参数说明：

参数	说明
name <*mstring*>	必选项，设置服务器组名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
servers <*string*>	必选项，设置服务器组中的服务器。字符串类型，格式为：“IP 地址:端口号,权重”，端口号取值范围 1-65535；权重为可选项，取值范围：1-10；默认值：5。 支持多个输入形式，多个输入之间用竖线分隔，如“192.168.101.2:80|192.168.99.3:8080,3”。 注意：不包含“&\"\\'%<>”和空格。
health-enable <on|off>	可选项，设置是否启用健康检查策略。开启|关闭，默认值：关闭。
health-check <*string*>	可选项，设置引用的健康检查策略名称。字符串类型，表示引用的健康检查策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不包含“&\"\\'%<>”和空格。

命令示例：

添加名称为 *server-group* 服务器组，并添加地址为 12.3.3.3、端口号为 443、权重为 5 和地址为 12.3.3.13、端口为 80、权重为 8 的服务器。

TopsecOS# **waf server group add name** *server-group* **servers** 12.3.3.3:443|12.3.3.13:80,8

waf server-group add-server name <*mstring*> **servers** <*string*>

命令描述：

添加服务器到服务器组中。

可使用 **waf server-group delete-server name** <*mstring*>命令删除服务器组中指定的服务器。

可使用 **waf server-group modify-server name** <*mstring*> **servers** <*string*>命令修改服务器组中的服务器。

参数说明：

参数	说明
name <*mstring*>	必选项，设置服务器名称。字符串类型，表示服务器组名

参数	说明
	称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
servers <*string*>	必选项，设置服务器组中的服务器。字符串类型，格式为：“IP 地址:端口号,权重”，端口号取值范围 1-65535；权重为可选项，取值范围：1-10；默认值：5。 支持多个输入形式，多个输入之间用竖线分隔，如“192.168.101.2:80|192.168.99.3:8080,3”。 注意：不包含“&\"\\'%<>”和空格。

使用说明：

必须先由 **waf server-group add name** <*mstring*> **servers** <*string*>命令创建服务器组，否则添加失败。

可使用 **waf server-group show** [**name** <*mstring*>]命令查看已创建的服务器组配置信息。

命令示例：

添加地址为 192.168.1.3、端口为 80 的服务器到服务组 *server-group* 中。

TopsecOS# **waf server-group add-server name** *server-group* **servers** *192.168.1.3:80*

waf server-group show [**name** <*mstring*>]

命令描述：

查看服务器组配置信息。

参数说明：

参数	说明
name <*mstring*>	可选项，设置服务器组名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

TopsecOS# **waf server-group show**

Name: server-group

Health Enabled: off

Health Check:

Servers: 12.3.3.3:443, weigth = 5, status: unknown

12.3.3.13:80, weigth = 8, status: unknown

192.168.1.3:80, weigth = 5, status: unknown

waf server-group clean <cr>

命令描述：

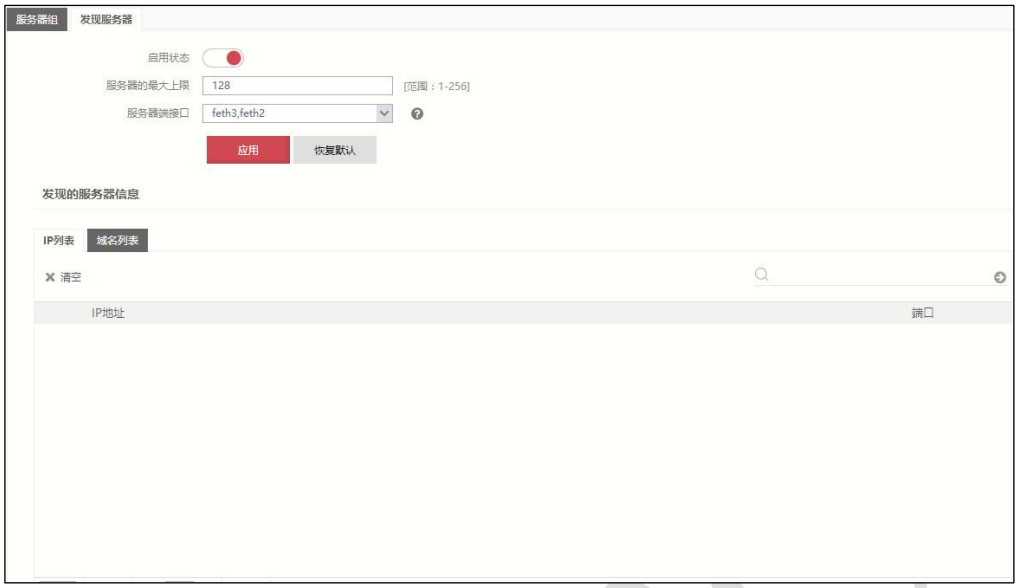
清除所有的服务器组配置信息。

5.1.3.2 发现服务器

在一些用户的网络环境中可能存在几十台甚至几百台的 HTTP 服务器，而网络管理员有可能不知道全部的服务器的地址，此时利用 TopWAF 的发现服务器功能，可以帮助管理员发现用户网络环境中存在的 HTTP 服务器，从而便于配置服务器组。关于服务器组的配置具体请参见 5.1.3.1 服务器组。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **服务器组**，激活“发现服务器”页签，如下图所示。



在配置发现服务器时，各项参数的具体说明如下表所示。

参数	说明
启用状态	设置是否启用访问控制功能。默认为“ ”，表示已关闭，点击该按钮将显示“ ”，表示已开启。
服务器的最大上限	设置发现服务器的数量的上限值。数值类型，取值范围：1-256；默认值：128。
服务器端接口	设置探测使用的 TopWAF 服务器侧的物理接口，可以添加多个物理接口。

步骤2 点击【应用】按钮，完成发现服务器配置。

CLI 方式

waf discover-servers set max <*num*> **enable** <off|on> **server-side-interface** <*mstring*>

命令描述：

配置发现服务器功能。

参数说明：

参数	说明
max <*num*>	设置发现服务器的数量的上限值。数值类型，取值范围：1-256。
enable <off|on>	发现服务器的开关，关闭|开启

参数	说明
server-side-interface <*mstring*>	设置 TopWAF 连接服务器侧的物理接口。字符串类型，表示接口名称，该接口需工作在路由模式下。

命令示例：

配置发现服务器功能，发现服务器数量的上限为 100，TopWAF 连接服务器侧的物理接口为任意接口，并开启发现服务器功能。

TopsecOS# **waf discover-servers set max** *100* **enable** on **server-side-interface** feth0

waf discover-servers clean <cr>

命令描述：

清除发现服务器功能配置信息。

waf discover-servers reset <cr>

命令描述：

恢复发现服务器功能配置为默认值。

缺省情况下，配置发现服务器功能，服务器侧接口为空，发现服务器数量的上限为 128，关闭发现服务器功能。

waf discover-servers show [config]

命令描述：

查看发现服务器功能。

参数说明：

参数	说明
config	可选项，查看发现服务器功能的配置信息。如果不选择该参数，则查看服务器发现功能探测到的服务器信息。

命令示例：

查看发现服务器功能的配置信息。

TopsecOS# **waf discover-servers show config**

waf discover-servers set server-side-interface 'feth0' max 128 enable off

查看发现服务器功能的探测结果。

TopsecOS# **waf discover-servers show**

changyan.sohu.com 123.125.116.218 80

err.taobao.com 125.39.199.50 80

cbjs.baidu.com 111.206.76.49 80

www.oracleimg.com 184.50.90.127 80

s.qhupdate.com 111.206.65.242 80

qzone-music.qq.com 58.251.139.169 80

qurl.f.360.cn 111.206.60.49 80

agent.sj.qq.com 112.65.192.47 80

short.weixin.qq.com 140.207.54.116 80

5.1.4 健康检查

健康检查功能用于检测 Web 服务器的工作状态。TopWAF 支持 ICMP、TCP、HTTP、HTTPS 类型的健康检查。配置健康检查功能对服务器组中每个成员服务器的状态进行检测，防止 TopWAF 将会话分发到已经失效的服务器，关于服务组的配置具体请参见 5.1.3 服务器组。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **健康检查**。

步骤2 点击『添加』，弹出“添加健康检查”窗口，如下图所示。

在配置健康检查时，各项参数的具体说明如下表所示。

参数	说明
名称	设置健康检查规则名称，字符形式，支持数字、字母、中文和特殊字符“_-*. ”，且长度不能大于 29 个字节。
健康检查类型	选择健康检查的类型。默认值：HTTP。 1）HTTP：检查 Web 服务器是否能够正常响应 TopWAF 的 HTTP 请求。 2）HTTPS：检查 Web 服务器是否能能够正常响应 TopWAF 的 HTTPS 请求。 3）ICMP：使用 ICMP 报文检查客户端到 Web 服务器是否路由可达。 4）TCP：检查 Web 服务器的 TCP 端口是否开放。
时间间隔（s）	设置 TopWAF 向 Web 服务器进行健康检查发送探测报文的时间间隔。数值类型，取值范围：1-600；单位：秒；默认值：10。
唤醒时间间隔（s）	设置健康检查的唤醒时间。数值类型，取值范围：1-600；单位：秒；默认值：10。当 TopWAF 成功探测到 Web 服务器健康状况正常后，将在设置的唤醒时间间隔后重新探测服务器的健康状况。
最大失败次数	设置健康检查的失败次数，默认值：3。当对从 TopWAF 到服务器的可达性检查失败次数超过该值后，TopWAF 将判断该服务器不可达。
路径	当设置“健康检查类型”为 HTTP 或 HTTPS 时，设置进行健康检查页面的 URI 地址。格式：以单斜线“/”开头的字符串，如“/index.htm”。

状态码	当设置“健康检查类型”为 HTTP 或 HTTPS 时，设置探测服务器健康检查状况正常后返回的状态码，如果健康检查返回的状态码非此处定义的状态码，则可判定服务器不可用。数值类型：取值范围：100-600；默认值：200。 说明： 一般情况下，如果探测服务器正常时，即会返回 200 的状态码，如果没有特殊需求，请勿修改此处的状态码，以免 TopWAF 不能正常判断 Web 服务器健康状态。

步骤3 参数配置完成后，点击【确定】按钮，完成健康检查的配置。

CLI 方式

waf health-check add name <*mstring*> [**type** <icmp|http|https|tcp>] [**interval** <*num*>] [**up-interval** <*num*>] [**max-fail** <*num*>] [**path** <*mstring*>] [**status** <*num*>]

命令描述：

添加健康检查策略。

可使用 **waf health-check delete name** <*mstring*>命令删除健康检查策略。

可使用 **waf health-check modify name** <*mstring*>] [**type** <icmp|http|https|tcp>] [**interval** <*num*>] [**up-interval** <*num*>] [**max-fail** <*num*>] [**path** <*mstring*>]命令修改健康检查策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置健康检查策略名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
type <icmp|http|https|tcp>	可选项，设置健康检查类型。ICMP 三层检查|HTTP 七层检查|HTTPS 七层检查|TCP 四层检查
interval <*num*>	可选项，设置健康检查探测报文的发送时间间隔。数值类型，单位：秒；默认值：10。
up-interval <*num*>	可选项，设置健康检查的唤醒时间。当 TopWAF 成功探测到服务器健康状况正常时，将在设置的唤醒时间间隔后重新探测服务器的健康状况。数值类型，单位：秒；默认值：10。
max-fail <*num*>	可选项，设置健康检查的失败次数，当对从 TopWAF 到服务器的可达性检查失败次数超过该值后，TopWAF 将

参数	说明
	判断该服务器不可达。数值类型，默认值：3。
path <*mstring*>	可选项，“type”设置为 http 时，设置进行健康检查页面的 URI 地址。字符串类型，注意：不能以“\\”结尾或不包含“<script>”字符串。
status <*num*>	可选项，设置健康检查返回的状态码。数值类型，单位：秒；取值范围：100-600；默认值：200。

命令示例：

添加名称为 *health*，检查类型为 http，检查周期为 20 秒，唤醒时间为 100 秒，最大失败次数为 4，路径为/test 的健康检查策略。

TopsecOS# **waf health-check add name** *health* **type** http **interval** *20* **up-interval** *100* **max-fail** *4* **path** /test

waf health-check show [**name** <*mstring*>]

命令描述：

查看健康检查策略配置。

参数说明：

参数	说明
name <*mstring*>	可选项，设置健康检查策略名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

显示所有的服务器健康检查配置信息。

TopsecOS# **waf health-check show**

Name: health

Type: http

Interval: 20

Up Interval:	100
Max fail:	4
Url:	/test

waf health-check clean <cr>

命令描述：

清除所有的健康检查策略配置。

5.1.5 爬虫

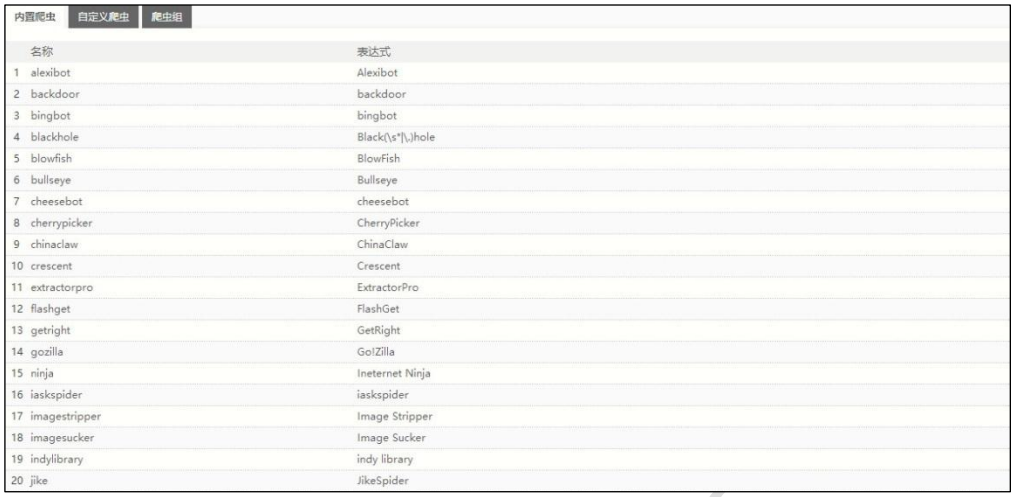
TopWAF 通过爬虫防护模块限制恶意爬虫访问 Web 网站。TopWAF 通过正则表达式来表示爬虫的 User-Agent 首部，进而可以标识爬虫。每个爬虫对象由其名称唯一标识，管理员可以通过在 TopWAF 上定义爬虫对象来标识爬虫。

TopWAF 的爬虫对象包括系统内置爬虫对象和管理员自定义的爬虫对象，通过对象组的方式对爬虫对象进行分类组织管理。爬虫防护策略则通过爬虫组与 HTTP 请求报文的 User-Agent 首部进行匹配，从而识别相应的爬虫。关于爬虫防护策略的配置具体请参见 5.2.9 爬虫防护，本节介绍如何配置爬虫、爬虫组。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **爬虫**。

步骤2 激活“内置爬虫”页签，可查看系统内置的爬虫对象，如下图所示。



步骤3 配置自定义爬虫对象。

1）激活“自定义爬虫”页签，点击『添加』，弹出“新建爬虫”窗口，如下图所示。

在添加爬虫对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置爬虫对象名称。名称只支持数字、字母、中文和特殊字符“-_*.”，且长度不能大于 29 个字节。
表达式	必选项，通过正则表达式设置爬虫对象的内容。点击『验证』，弹出“正则表达式验证器”窗口，管理员可通过该窗口验证相应字符串是否与正则表达式匹配。 说明： TopWAF 根据爬虫对象的表达式匹配 HTTP 请求的 User-Agent 首部内容，以确定蜘蛛或爬虫是否命中爬虫防护策略。

2）设置爬虫对象参数后，点击【确定】按钮完成配置。

步骤4 配置爬虫组。

1）激活“爬虫组”页签，点击『添加』，弹出“添加爬虫组”窗口，如下图所示。

在添加爬虫组时，各项参数的具体说明如下表所示。

参数	说明
组名称	必选项，设置爬虫组名称。名称只支持数字、字母、中文和特殊字符“-_*.”，且长度不能大于 29 个字节。
爬虫	必选项，点击『添加』在下拉列表中选择爬虫组中包含的爬虫对象。点击下拉列表中的『新建』，可新建爬虫对象。 说明： 每个爬虫组中最多支持 128 个爬虫对象。

2）设置爬虫组对象参数后，点击【确定】按钮完成配置。

CLI 方式

waf robots add name <*mstring*> **expression** <*mstring*>

命令描述：

添加爬虫对象。

可使用 **waf robots delete name** <*mstring*>命令删除爬虫对象。

参数说明：

参数	说明
name <*mstring*>	必选项，设置爬虫对象的名称。字符串类型，名称只支持数字、字母、中文和特殊字符“-_*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
expression <*mstring*>	必选项，设置爬虫对象的正则表达式。字符串类型。注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

添加名称为“baidu”，表达式为“baiduspider”的爬虫对象。

TopsecOS# **waf robots add name** *baidu* **expression** *baiduspider*

waf robots clean <cr>

命令描述：

清空管理员自定义的所有爬虫对象。

命令示例：

TopsecOS# **waf robots clean**

waf robots show [**name** <*mstring*>]

命令描述：

显示爬虫对象。

参数说明：

参数	说明
name <*mstring*>	可选项，指定爬虫对象的名称。字符串类型，名称只支持数字、字母、中文和特殊字符“-_*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

TopsecOS# **waf robots show**

name:bingbot

builtin_robots:yes

expression:bingbot

name:Yahoo

builtin_robots:yes

expression:(?:Yahoo! Slurp)|(?:crawler*yahoo)|(?:Yahoo! Site Explorer Feed Validator)

……

waf robots-group add name <*mstring*> [**robots** <*mstring*>]

命令描述：

添加爬虫组。

可使用 **waf robots-group delete name** <*mstring*>命令删除爬虫对象。

参数说明：

参数	说明
name <*mstring*>	必选项，设置爬虫组名称。字符串类型，名称只支持数字、字母、中文和特殊字符“-_*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
robots <*mstring*>	可选项，指定待添加到爬虫组中的爬虫对象。字符串类型，表示爬虫对象的名称。不同的爬虫对象间用逗号“,”隔开，例如：“robot1,robot2”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

添加一个名称为“group01”，包含爬虫对象为“bingbot”和“Yahoo”的爬虫组。

TopsecOS# **waf robots-group add name** *group01* **robots** *bingbot, Yahoo*

waf robots-group clean <cr>

命令描述：

清空爬虫组。

命令示例：

TopsecOS# **waf robots-group clean**

waf robots-group show [**name** <*mstring*>]

命令描述：

显示爬虫组。

参数说明：

参数	说明
name <*mstring*>	可选项，指定待查看对象组的名称，字符串类型。注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

TopsecOS# **waf robots-group show**

Name: group01 robots:bingbot,360Spider

5.1.6 数据类型

TopWAF 内置了部分常见的数据类型，如字符串类型，数值类型，IP 地址类型等，还支持自定义参数类型和敏感数据类型。

- 自定义参数类型：用于识别或限制用户在 Web 网站表单中输入的参数类型。TopWAF 内置的数据类型和管理员自定义的参数类型，为自学习功能模块学习参数的依据，且参数类型学习结果可应用到 URI 例外策略中，关于自学习功能策略的配置具体请参见 5.2.12 自学习。
- 敏感数据类型：用于识别或限制服务器响应报文中的敏感数据。关于 TopWAF 对 Web 网站表单的参数类型进行控制，以及对 Web 网站返回给客户端的敏感数据进行保护的配置具体请参见 5.2.15 高级设置。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **数据类型**。

步骤2 查看内置数据类型。

激活“内置类型”页签，可查看系统内置的数据类型，如下图所示。

	名称	表达式
1	string	([\s\S]*)
2	number	(^\$?[-+]?([0-9]{1,3}[,'])([0-9]{3}[,'])*[0-9]{3}|[0-9]+)(\.[0-9]*)?([eE][-+]?[0-9]+)?$)|(^((\d?)|(
3	ascii	(^[\x21-\x47]$)\|(^[\x61-\x7a]$)
4	email	(^[_a-zA-Z0-9-]+(\.[_a-zA-Z0-9-]+)*@[a-zA-Z0-9-]+(\.[a-zA-Z0-9-]+)*\.([[0-9]{1,3}]|[a-zA-
5	postcode	^(?:0[1-7]|1[0-6]|2[0-7]|3[0-6]|4[1-7]|5[1-7]|6[1-7]|7[1-5]|8[1-5])\d{4}$
6	uri	(^((mailto\:|(news|(ht|f)tp(s?))\://){1}\S+)$)|(^(http|https|ftp)\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{
7	date	(^((0?[13578]|10|12)(-|\/)(([1-9])|(0[1-9])|([12])([0-9]?)|(3[01]?))(-|\/)((19)([2-9])(\d{1})|(20)(
8	chinese_character	^[\xb0-\xf7][\xa0-\xfe]+$
9	mobilephone	^(0|86|17951)?(13[0-9]|15[012356789]|18[0-9]|14[57])[0-9]{8}$
10	credit_card	^((5[1-5]\d{14})|(4\d{12}(\d{3})?)|(3[47]\d{13})|(6011\d{14}))$
11	ip	^(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\d
12	unix_device_name	^(eth[0-9]$)\|(^eth[0-9]:[1-9]$)
13	microsoft_product_key	^[A-Z1-9]{5}-[A-Z1-9]{5}-[A-Z1-9]{5}-[A-Z1-9]{5}-[A-Z1-9]{5}$
14	telephone	^(0[0-9]{2,3}\-)?([2-9][0-9]{6,7})+(\-[0-9]{1,4})?$

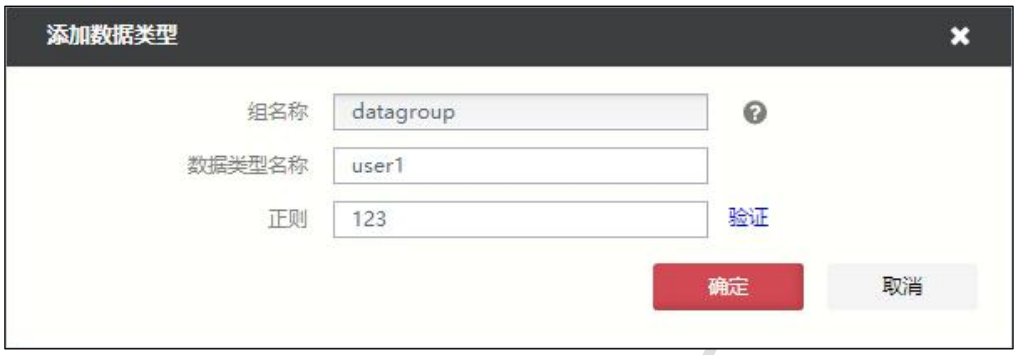
步骤3 配置参数类型。

1）激活“参数自定义类型”页签。

2）添加数据类型组。点击『添加』，弹出“添加数据类型组”窗口。输入数据类型组名称，点击【确定】按钮完成数据类型组的添加。

3）添加数据类型。

（a）点击数据类型组“添加”栏的图标“ ”，弹出“添加数据类型”窗口，如下图所示。

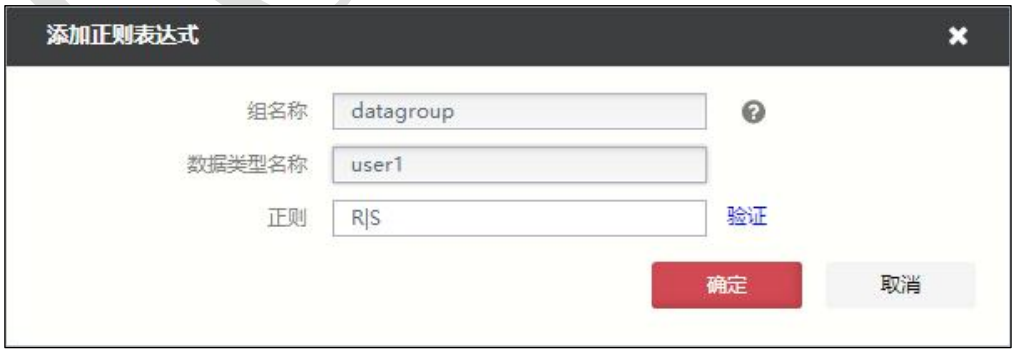


在配置数据类型时，各项参数的具体说明如下表所示。

参数	说明
组名称	显示标识数据类型组的名称。
数据类型名称	必选项，设置标识数据类型的名称。名称只支持数字、字母、中文和特殊字符“-_*.”。
正则	必选项，设置数据类型的正则表达式。点击『验证』，弹出“正则表达式验证器”窗口，管理员可通过该窗口验证相应字符串是否与正则表达式匹配。

参数配置完成后，点击【确定】按钮完成数据类型的添加。

（b）继续添加正则表达式条件到数据类型中。点击数据类型“添加”栏的图标“ ”，弹出“添加正则表达式”窗口，如下图所示。



配置正则表达式，点击【确定】按钮完成数据类型正则表达式的添加。

✧ 一个参数数据类型可添加多个正则表达式条件，参数数据类型的各正则表达式间的关系为逻辑“或”，即 HTTP 数据包满足参数数据类型中任意正则表

达式的条件，则命中该参数数据类型。

✧ 用户在添加完自定义类型后，需要在安全策略中引用该自定义数据类型才能生效，具体请参见 5.2.15 高级设置。

步骤4 配置敏感数据类型。

1）激活“敏感数据自定义类型”页签。

2）添加数据类型组。点击『添加』，弹出“添加数据类型组”窗口。输入数据类型组名称，点击【确定】按钮完成数据类型组的添加。

3）添加数据类型。

（a）点击数据类型组“添加”栏的图标“ ”，弹出“添加数据类型”窗口，如下图所示。

在配置数据类型时，各项参数的具体说明如下表所示。

参数	说明
组名称	显示标识数据类型组的名称。
数据类型名称	必选项，设置标识数据类型的名称。名称只支持数字、字母、中文和特殊字符“-_*.”。
校验类型	设置校验数据是否为合法信用卡、身份证、电话的校验算法，在下拉列表中选择校验类型，可选项：none、信用卡、身份证、电话，其中 none 表示不指定校验算法。
正则	必选项，设置数据类型的正则表达式。点击『验证』，弹出“正则表达式验证器”窗口，管理员可通过该窗口验证相应字符串是否与正则表达式匹配。

参数配置完成后，点击【确定】按钮完成数据类型的添加。

（b）继续添加正则表达式条件到数据类型中。点击数据类型“添加”栏的图标“ ”，弹出“添加正则表达式”窗口。

配置正则表达式，点击【确定】按钮，完成将数据类型正则表达式添加到已配置好的数据类型中。

- ✧ 数据同时匹配敏感数据类型的正则表达式和校验类型后，TopWAF 才将其确定为敏感数据。
- ✧ 一个敏感数据类型可添加多个正则表达式条件，敏感数据类型的各正则表达式间的关系为逻辑“或”，即 HTTP 数据包满足数据类型中任意正则表达式的条件，则命中该敏感数据类型。

CLI 方式

waf enumeration datatype <cr>

命令描述：

显示系统内置的数据类型。TopWAF 内置的数据类型具体如下表所示。

名称	正则表达式
string	([\s\S]*)

num	(^\$?[-+]?([0-9]{1,3}[,'][0-9]{3}[,'])*[0-9]{3}|[0-9]+)(\.[0-9]*)?([eE][-+]?[0-9]+)?$)\|(^((\d?)\|(([-+]?\d+\.?\d*)\|([-+]?\d*\.?\d+))\|(([-+]?\d+\.?\d*\,\ ?)*([-+]?\d+\.?\d*))\|(([-+]?\d*\.?\d+\,\ ?)*([-+]?\d*\.?\d+))\|(([-+]?\d+\.?\d*\,\ ?)*([-+]?\d*\.?\d+))\|(([-+]?\d*\.?\d+\,\ ?)*([-+]?\d+\.?\d*))$)
ascii	(^[\x21-\x47]$)\|(^[\x61-\x7a]$)
email	(^[_a-zA-Z0-9-]+(\.[_a-zA-Z0-9-]+)*@[a-zA-Z0-9-]+(\.[a-zA-Z0-9-]+)*\.(([0-9]{1,3})|([a-zA-Z]{2,3})|(aero|coop|info|museum|name))$)\|(^((\"[^\"\f\n\r\t\v\b]+\")\|([\w\!\#\$\%\&\'*\+\-\~\/\^\`\\|\{\}]+(\.[\w\!\#\$\%\&\'*\+\-\~\/\^\`\\|\{\}]+)*))@((\[(((25[0-5])\|(2[0-4][0-9])\|([0-1]?[0-9]?[0-9]))\.((25[0-5])\|(2[0-4][0-9])\|([0-1]?[0-9]?[0-9]))\.((25[0-5])\|(2[0-4][0-9])\|([0-1]?[0-9]?[0-9]))\ .((25[0-5])\|(2[0-4][0-9])\|([0-1]?[0-9]?[0-9]))\])\|(((25[0-5])\|(2[0-4][0-9])\|([0-1]?[0-9]?[0-9]))\.((25[0-5])\|(2[0-4][0-9])\|([0-1]?[0-9]?[0-9]))\.((25[0-5])\|(2[0-4][0-9])\|([0-1]?[0-9]?[0-9]))\.((25[0-5])\|(2[0-4][0-9])\|([0-1]?[0-9]?[0-9])))\|((([A-Za-z0-9\-])+\.)+[A-Za-z\-]+))$)|(^(?:[a-zA-Z0-9_'^&/+-])+(?:\.(?:[a-zA-Z0-9_'^&/+-])+)*@(?:(?:\[?(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))\.){3}(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\]?)|(?:[a-zA-Z0-9-]+\.)+(?:[a-zA-Z]){ 2,}\.?)$)
postcode	^(?:0[1-7]|1[0-6]|2[0-7]|3[0-6]|4[1-7]|5[1-7]|6[1-7]|7[1-5]|8[1-5])\d{4}$
uri	(^((mailto\:|(news|(ht|f)tp(s?))\://){1}\S+)$)\|(^(http\|https\|ftp)\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(:[a-zA-Z0-9]*)?/?([a-zA-Z0-9\-\._\?\,\'/\\\+&%\$#\=~])*$)|(^([a-zA-Z0-9]([a-zA-Z0-9\-]{0,61}[a-zA-Z0-9])?\.)+[a-zA-Z]{2,6}$)
date	^(?=\d)(?:(?:31(?!.(?:0?[2469]|11))|(?:30|29)(?!.0?2)|29(?=.0?2.(?:(?:(?:1[6-9]|[2-9]\d)?(?:0[48]|[2468][048]|[13579][26])|(?:(?:16|[2468][048]|[3579] [26])00)))(?:|$))\|(?:2[0-8]\|1\d\|0?[1-9]))([-./])(?:1[012]\|0?[1-9])\1(?:1[6-9]\|[2-9]\d)?\d\d(?:(?=\x20\d)\x20\|$))?(((0?[1-9]|1[012])(:[0-5]\d){0,2}(\x20[AP]M))|([01]\d|2[0-3])(:[0-5]\d){1,2})?$
chinese_character	^[\xb0-\xf7][\xa0-\xfe]+$
mobilephone	^(0|86|17951)?(13[0-9]|15[012356789]|18[0-9]|14[57])[0-9]{8}$
credit_card	^((5[1-5]\d{14})|(4\d{12}(\d{3})?)|(3[47]\d{13})|(6011\d{14}))$
ip	^(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])$
unix_device_name	^(eth[0-9]$)\|(^eth[0-9]:[1-9]$)
microsoft_product_key	^[A-Z1-9]{5}-[A-Z1-9]{5}-[A-Z1-9]{5}-[A-Z1-9]{5}-[A-Z1-9]{5}$
telephone	^(0[0-9]{2,3}\-)?([2-9][0-9]{6,7})+(\-[0-9]{1,4})?$

命令示例：

TopsecOS# **waf enumeration datatype**

name : string

regex : ([\s\S]*)

name : num

regex : (^\$?[-+]?([0-9]{1,3}[,']([0-9]{3}[,'])*[0-9]{3}|[0-9]+)(\.[0-9]*)?([eE][-+]?[0-9]+)?$)|(^((\d?)|(([-+]?\d+\.?\d*)|([-+]?\d*\.?\d+))|(([-+]?\d+\.?\d*\,\ ?)*([-+]?\d+\.?\d*))|(([-+]?\d*\.?\d+\,\ ?)*([-+]?\d*\.?\d+))|(([-+]?\d+\.?\d*\,\ ?)*([-+]?\d*\.?\d+))|(([-+]?\d*\.?\d+\,\ ?)*([-+]?\d+\.?\d*)))$)

……

waf datatype-group add name <*mstring*> **group-type** <sensitive|input>

命令描述：

自定义数据类型组。

可使用 **waf datatype-group delete name** <*mstring*>命令删除自定义数据类型组。

参数说明：

参数	说明
name <*mstring*>	必选项，设置数据类型组名称，字符串类型。名称只支持数字、字母、中文和特殊字符“-_*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
group-type <sensitive|input>	设置数据类型组的类型，可选项：敏感数据类型|输入类型。

命令示例：

添加一个名称为 datagroup1 的敏感数据类型。

TopsecOS# **waf datatype-group add name** *datagroup1* **group-type** *sensitive*

waf datatype-group show [**name** <*mstring*>]

命令描述：

显示数据类型组。

参数说明：

参数	说明
name <*mstring*>	可选项，指定待查看数据类型组的名称。字符串类型。注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

TopsecOS# **waf datatype-group show**

Group name:datagroup1 group-type:sensitive

waf datatype-group clean <cr>

命令描述：

清空所有数据类型组。

命令示例：

TopsecOS# **waf datatype-group clean**

waf datatype add group <*mstring*> **name** <*mstring*> **regex** <*mstring*> [**verify-type** <none|credit|phone|identification>]

命令描述：

添加数据类型。

可使用 **waf datatype delete group** <*mstring*> **name** <*mstring*>命令删除自定义数据类型。

参数说明：

参数	说明
group <*mstring*>	必选项，指定待添加的数据类型所属的数据类型组，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
name <*mstring*>	必选项，设置数据类型名称。名称只支持数字、字母、中文和特殊字符“-_*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
regex <*mstring*>	必选项，设置数据类型的正则表达式，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
verify-type <none|credit|phone|identification>	如果添加敏感数据类型，该参数可选。设置敏感数据的校验算法。无|信用卡|电话|身份证，默认为 none。

命令示例：

添加一个名称为“tel”、类型为“电话号码”的敏感数据类型到数据类型组“datagroup1”中。

TopsecOS# **waf datatype-group add name** *datagroup1* **group-type** sensitive

TopsecOS# **waf datatype add group** *datagroup1* **name** *tel* **regex** *^(0|86|17951)?(13[0-9]|15[012356789]|18[0-9]|14[57])[0-9]{8}$* **verify-type** phone

waf datatype add-regex group <*mstring*> **name** <*mstring*> **regex** <*mstring*>

命令描述：

添加数据类型条件。

可使用 **waf datatype delete-regex group** <*mstring*> **name** <*mstring*> **regex** <*mstring*>命令删除自定义数据类型条件。

参数说明：

参数	说明
group <*mstring*>	必选项，指定待添加条件的数据类型组名称，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
name <*mstring*>	必选项，指定数据类型名称，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
regex <*mstring*>	必选项，设置条件的正则表达式，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

为数据类型组“datagroup1”添加名称分别为 tel 和 sen01 的敏感数据类型。

TopsecOS# **waf datatype-group add name** *datagroup1* **group-type** sensitive

TopsecOS# **waf datatype add group** *datagroup1* **name** *tel* **regex** *^(0|86|17951)?(13[0-9]|15[012356789]|18[0-9]|14[57])[0-9]{8}$* **verify-type** phone

TopsecOS# **waf datatype add-regex group** *datagroup* **name** *sen01* **regex** (^[\x21-\x47]$)|(^[\x61-\x7a]$)

waf datatype clean group <*mstring*>

命令描述：

清空自定义数据类型。

参数说明：

参数	说明
group <*mstring*>	必选项，指定待清空数据类型的数据类型组，字符串类型。注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

清空数据类型组“datagroup”中的所有数据类型。

TopsecOS# **waf datatype clean group** *datagroup*

5.1.7 错误页面

错误页面是 TopWAF 拦截恶意请求后返回给客户端的页面。管理员可以自定义错误页面的内容，使错误页面的风格和被保护站点保持一致。

HTTP 响应头中包含了状态码信息，可以根据不同的状态码定制不同的错误页面。HTTP 状态码被分成了五大类，可根据状态码的起始位进行区分。

- 1XX（1 开头）：为信息性状态码，表示请求已被接受，需要继续处理。这类响应是临时响应，只包含状态行和某些可选的响应头信息。
- 2XX（2 开头）：为成功状态码，表示请求已被服务器接收、理解、并接受。
- 3XX（3 开头）：为重定向状态码，表示需要客户端采取进一步的操作才能完成请求。通常，这些状态码用来重定向，后续的请求地址（重定向目标）在本次响应的 Location 域中指明。
- 4XX（4 开头）：为客户端状态码，表示客户端可能发生了错误，妨碍了服务器的处理。
- 5XX（5 开头）：为服务器状态码，表示服务器在处理请求的过程中有错误或者异常状态发生，也有可能是服务器意识到以当前的软硬件资源无法完成对请求的处理。

常用的状态码及其含义如下表所示。

状态码		原因短语	说明
①信息	100	Continue	客户端应当继续发送请求。
	101	Switching Protocols	服务器已经理解了客户端的请求，并将通过 Upgrade 消息头通知客户端采用不同的协议来完成这个请求。
②成功	200	OK	请求已成功。
	201	Created	请求已经被实现。
	202	Accepted	服务器已接受请求，但尚未处理。
	203	Non-Authoritative Information	服务器已成功处理了请求，但返回的实体头部元信息不是在原始服务器上有效的确定集合，而是来自本地或者第三方的拷贝。
	204	No Content	无内容，服务器成功处理了请求，但不需要返回任何实体内容，并且希望返回更新了的元信息。
	205	Reset Content	重置内容，服务器成功处理了请求，且没有返回任何内容。但是与 204 响应不同，返回此状态码的响应要求请求者重置文档视图。
	206	Partial Content	服务器已经成功处理了部分 GET 请求。
③重定向	300	Multiple Choices	多路选择，被请求的资源有一系列可供选择的回馈信息，每个都有自己特定的地址和浏览器驱动的商议信息。用户或浏览器能够自行选择一个首选的地址进行重定向。
	301	Moved Permanently	永久转移，被请求的资源已永久移动到新位置，并且将来任何对此资源的引用都应该使用本响应返回的若干个 URI 之一。

状态码		原因短语	说明
	302	Found	暂时转移，请求的资源现在临时从不同的 URI 响应请求。由于这样的重定向是临时的，客户端应当继续向原有地址发送以后的请求。
	303	See Olher	对应当前请求的响应可以在另一个 URI 上被找到，而且客户端应当采用 GET 的方式访问那个资源。
	304	Not Modified	未修改，如果客户端发送了一个带条件的 GET 请求且该请求已被允许，而文档的内容（自上次访问以来或者根据请求的条件）并没有改变，则服务器应当返回这个状态码。
	305	Use Proxy	使用代理，被请求的资源必须通过指定的代理才能被访问。
	307	Temporary Redirect	临时转移，请求的资源现在临时从不同的 URI 响应请求。
④客户端错误	400	Bad Request	错误请求。1）语义有误，当前请求无法被服务器理解。2）请求参数有误。
	401	Unauthorized	当前请求需要用户验证。
	403	Forbidden	服务器已经理解请求，但是拒绝执行它。
	404	Not Found	请求失败，请求所希望得到的资源未被在服务器上发现。
	405	Method Not Al10wed	请求行中指定的请求方法不能被用于请求相应的资源。
	406	Not Acceptable	请求的资源的内容特性无法满足请求头中的条件，因而无法生成响应实体。
	407	Proxy Authentication Required	需要代理认证，与 401 响应类似，只不过客户端必须在代理服务器上进行身份验证。
	408	Request Timeout	请求超时。客户端没有在服务器预备等待的时间内完成一个请求的发送。
	409	Conflict	冲突，由于和被请求的资源的当前状态之间存在冲突，请求无法完成。
	410	Gone	被请求的资源在服务器上已经不再可用，而且没有任何已知的转发地址。
	411	Length Require	服务器拒绝在没有定义 Content-Length 头的情况下接受请求。
	412	Precondition Failed	服务器在验证在请求的头字段中给出先决条件时，没能满足其中的一个或多个。
	413	Request Entity Too Large	服务器拒绝处理当前请求，因为该请求提交的实体数据大小超过了服务器愿意或者能够处理的范围。
	414	Request Entity Too Long	请求的 URI 长度超过了服务器能够解释的长度，因此服务器拒绝对该请求提供服务。
	415	Unsupported Media Type	对于当前请求的方法和所请求的资源，请求中提交的实体并不是服务器中所支持的格式，因此请求被拒绝。
	416	Requested Range	如果请求中包含了 Range 请求头，并且 Range 中指定的任何

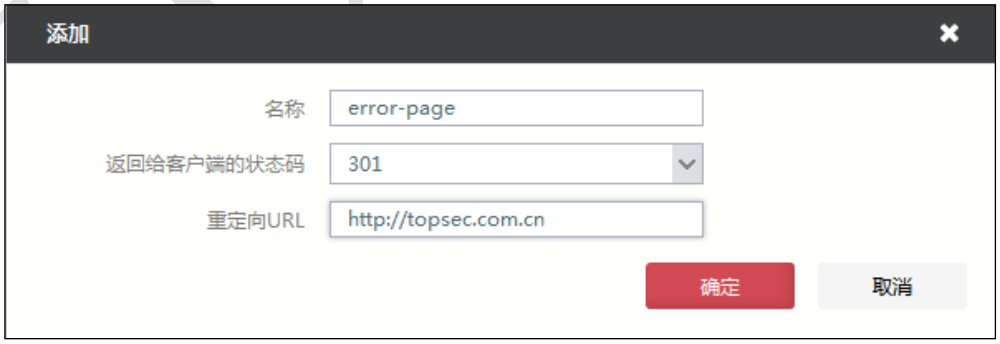
状态码		原因短语	说明
		Not Satisfiable	数据范围都与当前资源的可用范围不重合，同时请求中又没有定义 If-Range 请求头，那么服务器就应当返回 416 状态码。
⑤服务器错误	500	Internal Server Error	服务器内部错误，服务器遇到了一个未曾预料的状况，导致了它无法完成对请求的处理。
	501	Not Implemented	服务器不支持当前请求所需要的某个功能。
	502	Bad Gateway	网关失败，作为网关或者代理工作的服务器尝试执行请求时，从上游服务器接收到无效的响应。
	503	Service Unavailable	由于临时的服务器维护或者过载，服务器当前无法处理请求。这个状况是临时的，并且将在一段时间以后恢复。
	504	Gateway Timeout	作为网关或者代理工作的服务器尝试执行请求时，未能及时从上游服务器（URI 标识出的服务器，例如 HTTP、FTP、LDAP）或者辅助服务器（例如 DNS）收到响应。
	505	HTTP Version Not Supported	服务器不支持，或者拒绝支持在请求中使用的 HTTP 版本。

对于不同的状态码，管理员可进行不同的设置，对于以 3 开头的重定向状态码，可设置重定向的页面地址；对于以 4 和 5 开头的状态码，可自定义返回的错误页面。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **错误页面**。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。



在配置错误页面时，各项参数的具体说明如下表所示。

参数	说明
名称	设置错误页面名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
返回给客户端的状态码	选择返回给客户端的状态码。可选项：301、302、303、307、

参数	说明
	400-416、500-505。 以 3 开头：重定向状态码，需要指定跳转的页面地址。 以 4 开头：客户端错误状态码，需要指定返回的错误页面。 以 5 开头：服务器错误状态码，需要指定返回的错误页面。
重定向 URL	当设置“返回给客户端的状态码”为重定向状态码，即以 3 开头状态码时，设置重定向的界面 URL，当客户端访问服务器指定的地址时，将跳转到重定向 URL。
自定义错误页面	当设置“返回给客户端的状态码”为客户端错误或者服务器错误状态码，即以 4 或 5 开头状态码时，设置自定义的错误页面，当客户端访问服务器指定的地址时，将显示该自定义的错误页面。 1）文件：点击【选择文件】按钮，在管理主机中选择需要显示的错误页面，错误页面的大小，必须小于 1.2kB。 2）代码：直接拷贝错误页面的代码到文本编辑框中。

步骤3 配置完成后，点击【确定】按钮，完成错误页面的配置。

CLI 方式

waf error-page add name <*mstring*> **status** <*num*> {**contents** <*mstring*>|**file** <*mstring*>|**location** <*mstring*>}

命令描述：

添加错误页面。

可使用 **waf error-page delete name** <*mstring*>命令删除错误页面。

参数说明：

参数	说明
name <*mstring*>	必选项，设置错误页面名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
status <*num*>	必选项，设置状态码。数值类型，表示状态码。可选项：301、302、303、307、400-416、500-505。 以 3 开头：重定向状态码，需要指定跳转的页面地址。 以 4 开头：客户端错误状态码，需要指定返回的错误页面。

参数	说明
	以 5 开头：服务器错误状态码，需要指定返回的错误页面。
contents <*mstring*>	可选项，设置错误页面内容，当状态码为 4XX 或 5XX 时，可配置该参数。字符串类型，表示错误页面的内容。 注意：不能以“\\”结尾或不包含“<script>”字符串。
file <*mstring*>	可选项，设置错误页面文件，当状态码为 4XX 或 5XX 时，可配置该参数。字符串类型，表示错误页面文件。 注意：不能以“\\”结尾或不包含“<script>”字符串。
location <*mstring*>	可选项，设置重定向页面地址，当状态码为 3XX 时，可配置该参数。字符串类型，表示重定向的页面 URL 地址。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

添加名称为 *error-page* 的错误页面，当状态码返回 400 时，重定向到页面*/test*。

TopsecOS# **waf error-page add name** *error-page* **status** 302 **location** */test*

waf error-page show [**name** <*mstring*>]

命令描述：

查看错误页面配置。

参数说明：

参数	说明
name <*mstring*>	可选项，设置错误页面名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

显示错误页面 *error-page* 的配置信息。

TopsecOS# **waf error-page show name** *error-page*

Name : *error-page*

Status: 302

Location: /test

waf error-page clean <cr>

命令描述：

清除所有的错误页面。

waf enumeration errpage-status <cr>

命令描述：

查看 TopWAF 错误页面支持的状态码。

命令示例：

TopsecOS# **waf enumeration errpage-status**

status: 200 message: OK

status: 301 message: Moved Permanently

status: 302 message: Found

status: 303 message: See Other

status: 307 message: Temporary Redirect

status: 400 message: Bad Request

status: 401 message: Unauthorized

status: 403 message: Forbidden

status: 404 message: Not Found

status: 405 message: Method Not Allowed

status: 406 message: Not Acceptable

status: 408 message: Request Timeout

status: 409 message: Conflict

status: 410 message: Gone

status: 411	message: Length Required
status: 413	message: Request Entity Too Large
status: 414	message: Request-URI Too Long
status: 415	message: Unsupported Media Type
status: 416	message: Requested Range Not Satisfiable
status: 500	message: Internal Server Error
status: 501	message: Not Implemented

5.1.8 证书

为了检测 SSL 加密流量中的 Web 攻击，必须解密 SSL 流量，所以需要把被保护站点的证书导入 TopWAF。

✧ TopWAF 仅支持 PEM 格式服务器证书，并且证书文件中需要包含公钥和私钥。其他格式的证书可以转换格式后导入。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **证书**。

步骤2 添加服务器证书。

1）点击『添加』，弹出“添加”窗口。

2）配置服务器证书的参数。

在配置服务器证书时，各项参数的具体说明如下表所示。

参数	说明
证书名称	设置服务器证书名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
密码	设置该服务器证书文件的加密密码，保证服务器证书的安全。
证书文件	导入服务器证书文件。 文件：点击【选择文件】按钮，在管理主机中选择从 Web 服务器导出的服务器证书文件。证书文件大小不能超过 32KB。 粘贴：将 Web 服务器的证书文件的内容粘贴到输入框中。

3）配置完成后，点击【确定】按钮，完成服务器证书的导入。

步骤3 查看服务器证书。选中证书所在行，点击『详细』，可查看证书的详细信息。

步骤4 导出服务器证书。选中证书所在行，点击『导出』，可将保存在设备中的服务器证书保存到管理主机。

CLI 方式

waf certfile add name <*string*> [**password** <*mstring*>] **file** <*mstring*>

命令描述：

添加服务器证书到 TopWAF。

可使用 **waf certfile delete name** <*string*>命令删除证书。

可使用 **waf certfile modify name** <*string*> [**password** <*mstring*>] **file** <*mstring*>命令修改证书。

参数说明：

参数	说明
name <*string*>	必选项，设置服务器证书名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不包含“&\"\\'%<>”和空格。
password <*mstring*>	可选项，设置服务器证书密码，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
file <*mstring*>	必选项，设置证书文件名称，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

添加证书名称为 *cert1*，密码为 *pass12398*，证书文件 *cert-file1* 的证书到 TopWAF 中。

TopsecOS# **waf certfile add name** *cert1* **password** *pass12398* **file** *cert-file1*

waf certfile show <cr>

命令描述：

查看 TopWAF 中的服务器证书。

waf certfile clean <cr>

命令描述：

清除 TopWAF 中的服务器证书。

5.1.9 用户登录页面

为了拦截暴力登录，管理员需要在 TopWAF 上配置被保护站点登录页面的 URI 地址、认证方式、认证成功后的状态码、认证失败后的状态码等信息。TopWAF 支持 basic、get、form、digest 四种认证方式。用户登录页面添加后可在“暴力登录”策略中引用，关于暴力登录策略配置具体请参见 5.2.11 暴力登录。

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器对象** > **用户登录页面**。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。

在配置用户登录页面时，各项参数的具体说明如下表所示。

参数	说明
名称	设置用户登录页面名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
启用状态	设置是否开启用户登录页面。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
登录界面地址	设置登录界面文件的 url 目录，例如/login.asp。
认证方式	设置登录页面的认证方式。可选项：basic、form、get、digest。
认证成功状态码	设置登录信息认证成功后的返回的状态码，不同状态码返回的信息不同。当“认证方式”为 basic 或 digest 时，该参数有效。
认证失败状态码	设置登录信息认证失败后的返回的状态码，不同状态码返回的信息不同。当“认证方式”为 basic 或 digest 时，该参数有效。
用户名 key 值	设置登录页面用户名的验证 key 值。当“认证方式”为 get 或 form 时，该参数有效。
密码 key 值	设置登录页面密码的验证 key 值。当“认证方式”为 get 或 form 时，该参数有效。
登录成功响应头提示信息	设置当登录页面认证通过后，http 响应头的提示信息。
登录失败响应头提示信息	设置当登录页面认证失败后，http 响应头的提示信息。
登录成功响应体提示信息	设置当登录页面认证通过后，http 响应体的信息。
登录失败响应体提示信息	设置当登录页面认证失败后，http 响应体的信息。

配置完成后，点击【确定】按钮，完成服务器证书的导入。

步骤3 选中已添加的用户登录页面，点击『编辑』、『删除』，可执行相应的操作。

CLI 方式

waf login-page add auth-method <form|basic|digest|get> **failed-message** <*mstring*> **failed-status** <*num*> **form-password-field** <*mstring*> **form-user-field** <*mstring*> **name** <*mstring*> **rsp-header-failed-msg** <*mstring*> **rsp-header-success-msg** <*mstring*> **success-message** <*mstring*> **success-status** <*num*> **url** <*mstring*>

命令描述：

添加用户登录页面到 TopWAF。

可使用 **waf login-page delete name** <*mstring*>命令删除用户登录页面。

可使用 **waf login-page modify name** <*mstring*>命令修改用户登录页面。

参数说明：

参数	说明
auth-method <form|basic|digest|get>	必选项，设置用户认证方法。basic、form、get、digest
failed-message <*mstring*>	必选项，设置登陆失败提示信息。字符串类型，表示登陆失败提示信息。 注意：不能以“\\”结尾或不包含“<script>”字符串。
failed-status <*num*>	必选项，设置认证失败状态码。数值类型。
form-password-field <*mstring*>	必选项，设置 form|get 认证方式下认证时密码 key 值。字符串类型，表示密码 key 值。 注意：不能以“\\”结尾或不包含“<script>”字符串。
form-user-field <*mstring*>	必选项，设置 form|get 认证方式下认证时用户名 key 值。字符串类型，表示用户名 key 值。 注意：不能以“\\”结尾或不包含“<script>”字符串。
name <*mstring*>	必选项，设置登录页面名称。字符串类型，表示用户登录页面名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
rsp-header-failed-msg <*mstring*>	必选项，设置 form|get 认证失败时响应头信息。字符串类型，注意：不能以“\\”结尾或不包含“<script>”字符串。
rsp-header-success-msg <*mstring*>	必选项，设置 form|get 认证成功时响应头信息。字符串类型，注意：不能以“\\”结尾或不包含“<script>”字符串。

参数	说明
success-message <*mstring*>	必选项，设置登陆成功提示信息。字符串类型，注意：不能以“\\”结尾或不包含“<script>”字符串。
success-status <*num*>	必选项，设置认证成功状态码，数值类型。
url <*mstring*>	必选项，设置登录页面地址目录。字符串类型，注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

添加用户登录页面名称为 *login-page1*，登录界面地址为 */login.php*，认证方式为 *basic*，认证成功状态码为 *200* ，认证失败状态码为 *401*，的用户登录页面到 TopWAF 中。

TopsecOS# **waf login-page add name** *login-page1* **url** */login.php* **auth-method** *basic* **success-status** *200* **failed-status** *401*

waf login-page show <cr>

命令描述：

查看 TopWAF 中的用户登录页面。

5.2 安全策略

安全策略是 TopWAF 中最为复杂的策略配置，包含了多种防护功能模块，如协议合规、文件控制、访问控制、CSRF 防护等安全防护策略的配置。

针对不同的服务器可配置不同的安全策略，配置完成安全策略后，管理员可在服务器策略引用已配置好的安全策略，使安全策略生效，关于服务器策略的配置具体请参见 5.3 服务器策略。

5.2.1 安全策略

管理员可以根据实际需求添加不同的安全策略，可以新建安全策略，也可克隆系统内置的安全策略。系统内置三个安全策略，按照防护精准度降低顺序依次分别为“应用优先”、“标准策略”和“安全优先”，在内置安全策略中各配置项均有默认值，不允许修改。通常管理员基于此三个安全策略克隆出新的安全策略，然后在服务器策略中引用，以便于根据保护站点的实际情况修改安全策略。

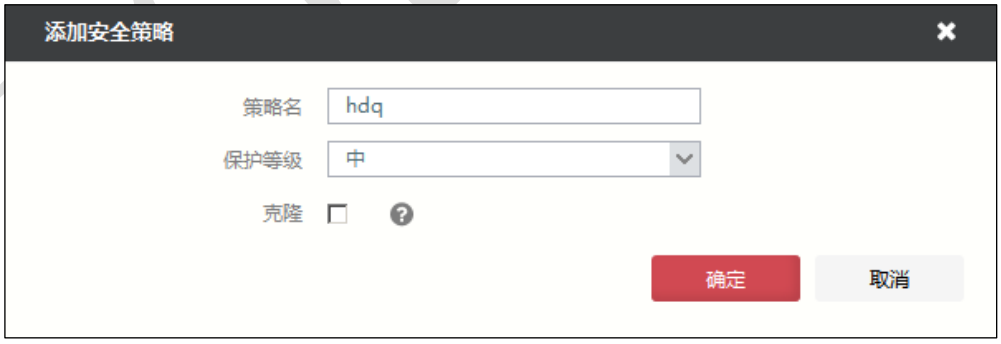
在创建好安全策略后，在 **Web 防护** > **安全策略** 下的功能参数均有默认取值，用户可根据实际的需求，进入相应的功能模块配置界面修改配置。具体操作步骤为：在页面上方“安全策略”下拉列表中选择需要配置的安全策略，Web 界面中将显示安全策略的当前配置参数，管理员可在该界面中配置安全策略，配置完成后点击【应用】按钮，即可完成安全策略的修改。

TopWAF 最多支持添加 128 条安全策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **安全策略**。

步骤2 点击『添加』，弹出“添加安全策略”窗口，如下图所示。



在配置安全策略时，各项参数的具体说明如下表所示。

参数	说明
策略名	设置策略名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
保护等级	设置安全策略的保护等级，可选项为：高、中、低。
克隆	勾选该选项，可以将已经配置好的策略克隆为新的策略。

参数	说明
被克隆的安全策略	当勾选“克隆”时，选择已经配置好的安全策略。

步骤3 参数配置完成后，点击【确定】按钮完成配置。

CLI 方式

waf security-policy add name <*mstring*> **{clone** <*string*>|[**input-group** <*mstring*>] [**max-argument-length** <*num*>] [**max-arguments** <*num*>] [**methods** <*mstring*>] [**upload-files** <*num*>] [**upload-size** <*string*>] [**protect-level** <high|middle|low>] [**max-formdata-length** <*num*>] [**download-size** <*string*>] [**multi-encoding** <on|off>] [**block-period** <*num*>] [**block-scanner-ip** <on|off>] [**firewall-link** <on|off>]**}**

命令描述：

添加安全策略，可以新建安全策略或者克隆已有的安全策略。

可使用 **waf security-policy delete name** <*mstring*>命令删除安全策略。

可使用 **waf security-policy modify name** <*mstring*>命令修改安全策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置安全策略名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
block-period <*num*>	动态阻断时长，单位为秒。
block-scanner-ip <on|off>	设置是否开启阻断扫描器 IP，可选项：开启|关闭。
firewall-link <on|off>	设置是否开启防火墙联动，可选项：开启|关闭。
clone <*string*>	可选项，克隆已经配置好的安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不包含“&\"\\'%<>”和空格。
input-group <*mstring*>	可选项，设置数组名称。字符串类型，表示数组名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
max-argument-length <*num*>	可选项，设置表单参数的最大长度。数值类型，单位：字节；取值范围：0-65535，0 表示不作限制；默认值：64k。

参数	说明
max-arguments <*num*>	可选项，设置最大表单参数个数。数值类型，取值范围：0-512，0 表示不作限制，默认值：20。
methods <*mstring*>	可选项，设置允许的请求方法。字符串类型，表示允许的请求方法，例如：“GET,POST,PUT”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
upload-files <*num*>	可选项，设置最大上传文件个数。数值类型，取值范围：0-128；默认值：5。
upload-size <*string*>	可选项，设置最大上传文件大小。数值类型，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：64K。 说明：单位不区分大小写。
protect-level <high|middle|low>	可选项，设置防护等级。高|中|低
max-formdata-length <*num*>	可选项，设置最大 x-www-form-urlencoded 表单长度，范围(0-32768)，0 代表不限制。数值类型。范围(0-32768)，0 代表不限制。
download-size <*string*>	可选项，设置最大下载文件大小，字符串类型，表示文件大小。如 1024，1k，2m，4G。
multi-encoding <on|off>	可选项，检测多重编码。开启|关闭。

命令示例：

新建名称为 *sec01* 的安全策略。

TopsecOS# **waf security-policy add name** *sec01*

克隆 *sec01* 安全策略为新的安全策略 *sp*。

TopsecOS# **waf security-policy add name** *sp* **clone** *sec01*

修改名称为 *sp* 安全策略允许的请求方法为 GET。

TopsecOS# **waf security-policy modify name** *sp* **methods** *GET*

waf security-policy show [**name** <*mstring*>]

命令描述：

查看安全策略配置信息。

参数说明：

参数	说明
name <*mstring*>	可选项，设置安全策略名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

显示“123”安全策略的详细配置信息。

TopsecOS# **waf security-policy show name** *123*

ID: 8295

Name: 123

Sensitive Group:

Input Group:

==Autolearn==

Skip Arguments:

Percent: 100

Deep Autolearn Enabled: off

Days: 7

==HTTP Constraint==

Enable: on

Request Header Length: 8192

Content-Length: 10485760

Body Length: 10485760

Request Line Length: 4096

Header Line Length: 4096

Cookie Num: 64

HEADER Num: 64

Header Name Length: 512

==Upload Files==

Upload policy enable: on

Max Upload Files: 5

Max File size: 10M

Match type: extension

Allow extensions: txt,pdf,docx,doc,docm,dot,dotx,dotm,wps,rtf,xls,xlsx,xlsm
,xlt,xltx,xltm,ppt,pptx,pptm,pps,ppsx,ppsm,pot,potm,potx,jpg,png,jpeg,gif,bmp,zi
p,rar,gz,tar,bz2,wav,mp3,swf,wma,$

Request body types:
any,application/x-www-form-urlencoded,multipart/form-data
,text/xml,application/json

==Download Files==

Download policy enable: on

Max Download File size: 10M

Download Match type: extension

Forbid extensions: bat,cfg,cs,csr,conf,dat,db,dll,ini,key,lnk,log,old,mdb,s
ql,swp,php~

Request body types:
any,application/x-www-form-urlencoded,multipart/form-data
,text/xml,application/json

==HTTP defence==

defence_xss: on

defence_sqli: on

```
defence_osi:                on
defence_rfi:                on
defence_dir:                on
defence_leakage:            on
defence_ldap:               on
defence_xpath:              on
defence_ssi:                on
defence_server:             on
defence_other:              on
defence_user:               on
defence_all:                on
==Others==
Methods:                    GET,POST,OPTIONS,HEAD
Max Arguments:              32
Max Argument Length:        2048
Max Formdata Length:        16384
Multi Encoding:             off
Protect Level:              middle
the num of acl polocy:      0
the num of exception polocy: 0
the num of csrf polocy:     0
para-limits enable:         on
anti-stealing-link enable:  off
robots-policy enable:       off
block scanner ip enable:    off
block period:               300
firewall-link enable:       off
```

waf rule-action reset security-policy <*string*> **ruleid** <*num*>

命令描述：

恢复安全策略的配置项为默认值。

参数说明：

参数	说明
security-policy <*string*>	安全策略名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。注意：不包含“&\"\\'%<>”和空格。
ruleid <*num*>	数值类型，表示安全策略序号，可使用 **waf security-policy show** [**name** <*mstring*>]查看。

waf server-policy clean <cr>

命令描述：

清除所有未被引用的安全策略。

5.2.2 访问控制

TopWAF 提供针对 URI 地址的精细访问控制，防止对 URI 地址的越权访问。例如用户访问网站内部不对外公开的目录，网站的后台管理界面，或者之前公布后来被隐藏但未删除的页面。

访问控制策略根据 URL 地址类型分为两类：一类是普通类型，使用字符串进行 URI 匹配；另外一类是正则类型，对符合正则表达式规则的多个地址进行 URI 匹配。所有普通类型的优先级高于正则类型的访问控制类型优先级，当一个 HTTP 请求 URI 匹配多条访问控制策略时，先按照配置顺序匹配普通类型再匹配正则类型。当第一条访问控制策略的动作生效时，如果该策略动作配置为继续或警告，会继续匹配后续访问控制策略，否则将忽略后续的访问控制策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **访问控制**。

步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 点击『添加』，弹出“添加访问控制”窗口，如下图所示。

在配置访问控制时，各项参数的具体说明如下表所示。

参数	说明
名称	设置策略名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
启用状态	设置是否启用访问控制功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
URI 路径类型	设置 URI 地址的类型。可选项：普通、正则。 普通类型：URI 指通过单个字符串来描述一个 URI 路径； 正则类型：URI 指通过单个字符串来描述一系列符合某个语法规则的 URI 路径。
URI 路径	URI 路径类型设置为“普通”时，该参数有效。设置 TopWAF 所保护的某个网站地址，格式：以单斜线“/”开头的字符串，如“/index.htm”。
URI 路径正则	URI 类型设置为“正则”时，该参数有效。使用正则表达式设置 TopWAF 所保护的一系列 Web 网站地址。
源地址过滤	设置访问控制源地址过滤，可输入 IP 或网段，支持 IPv4 和 IPv6。 如果勾选“取反”则表示仅当源地址访问该 URI 时，访问控制生效。
动作	设置对符合访问控制规则的 URL 地址的动作。 1）继续：进入下一条访问控制规则，判断对该访问进行的动作，访问不记录到攻击日志中。 2）允许：允许本次访问请求，忽略后续的所有的规则，并将访问记录到攻击日志中。 3）警告：进入下一条访问控制规则，判断对该访问进行的动作，访问记录到攻击日志中。 4）拒绝：拒绝本次访问请求，将访问记录到攻击日志中。 5）拒绝不记日志：拒绝本次访问请求，访问不记录到日志中。 6）临时跳转：由本次请求页面临时跳转到新的页面中，将访问记录到攻击日志中，再次接收到访问请求时，继续访问当前请求页面。

参数	说明
	7）永久跳转：由本次请求页面临时跳转到新的页面中，将访问记录到攻击日志中，再次接收到访问请求时，将访问新的页面。 说明： HTTP 请求报文命中访问控制策略产生的报警和日志信息均显示在攻击日志界面，关于攻击日志的查看具体请参见 4.2.1 日志查看。
跳转 URL	当“动作”设置为“临时跳转”或“永久跳转”时可设置该参数。 1）临时跳转：输入 URL 地址，当客户端访问非允许客户端访问的站点时，页面将跳转到该地址，仅该次访问进行跳转，后续还将访问原地址。 2）永久跳转：输入 URL 地址，当客户端访问非允许客户端访问的站点时，页面将跳转到该地址。

步骤4 参数配置完成后，点击【确定】按钮完成配置。

CLI 方式

waf acl-policy add name <*mstring*> **security-policy** <*mstring*> **type** <normal|regex> **url** <*mstring*> **action** <continue|allow|alert|deny|deny-nlog|temp-redirect|perm-redirect||block> [**redirect-url** <*mstring*>] **enable** <on|off> **filter** <*mstring*>

命令描述：

添加访问控制规则。

可使用 **waf acl-policy delete name** <*mstring*> **security-policy** <*mstring*>命令删除访问控制规则。

可使用 **waf acl-policy modify name** <*mstring*> **security-policy** <*mstring*>命令修改访问控制规则。

参数说明：

参数	说明
name <*mstring*>	必选项，设置访问控制策略名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
type <normal|regex>	必选项，设置 URI 地址类型。普通|正则

url <*mstring*>	必选项，设置 URI 地址。字符串类型。 当 type 类型为 normal 时：设置 TopWAF 所保护的某个网站地址，格式：以单斜线“/”开头的字符串，如“/index.htm”。 当 type 类型为 regex 时：URI 类型设置为“正则”时，该参数有效。使用正则表达式设置 TopWAF 所保护的一系列 Web 网站地址。 注意：不能以“\\”结尾或不包含“<script>”字符串。
action <continue|allow|alert|deny|deny-nlog|temp-redirect|perm-redirect|block>	必选项，匹配访问控制策略后执行的动作。继续|放行|警告|拒绝|拒绝并不记录日志|临时跳转|永久跳转
redirect-url <*mstring*>	可选项，跳转地址，当 action 类型为临时跳转或者永久跳转时可设置该参数。字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
enable <on|off>	必选项，是否启用访问控制规则。开启|关闭
filter <*mstring*>	匹配过滤条件。字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

在“sec01”安全策略中，添加并启用名称为 *url-acl* 的访问控制规则，实现放行访问普通类型的服务器地址*/normal*。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf acl-policy add name** *url-acl* **security-policy** *sec01* **url** */normal* **type** normal **enable** on **action** allow

waf acl-policy show name <*mstring*> **security-policy** <*mstring*>

命令描述：

查看访问控制策略配置信息。

参数说明：

参数	说明
name <*mstring*>	必选项，设置访问控制策略名称。字符串类型，支持数字、字母、

参数	说明
	中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

显示“sec01”安全策略中的 *url-acl* 访问控制规则。

TopsecOS # **waf acl-policy show name** *url-acl* **security-policy** *sec01*

Name: url-acl id: 8338 Enable: on type: normal filter:

Url: /normal Action: allow

waf acl-policy clean security-policy <*mstring*>

命令描述：

清除访问控制策略配置信息。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

waf acl-entry show <cr>

命令描述：

查看所有的访问控制配置信息。

命令示例：

显示“sec01”安全策略中的访问控制规则。

TopsecOS# **waf acl-entry show**

Name: jd id: 8227 Enable: on type: regex filter:

Url: \S+ Action: alert

Name: url-acl id: 8338 Enable: on type: normal filter:

Url: /normal Action: allow

waf acl-entry clean <cr>

命令描述：

清除访问控制配置信息。

5.2.3 协议合规

协议合规功能是对 HTTP 请求做协议合规检测，拦截异常请求，保障服务器安全稳定运行。

5.2.3.1 请求限制

请求限制是对 HTTP 头部的各个字段做合规性的限制。HTTP 请求头部包括起始行、包含属性的首部(headers)，以及包含数据的主体(body)部分。

请求头部的格式为：

<method><request-URL><version>

<headers>

<entity-body>

起始行（startline）

所有的 HTTP 报文都以起始行开始。请求报文的起始行为请求行，包含了方法、请求 URL 和 HTTP 版本。起始行字段具体说明如下表所示。

参数	说明
method	方法，客户端希望服务器对资源执行的动作。常见的方法有 GET、HEAD 和 POST 等。
request-URL	浏览器寻找信息时所需的资源位置。
version	报文所使用的 HTTP 版本，其格式为： HTTP/<major> <minor> 其中主要成本号（major）和次要版本号（minor）都是整数。
status	状态码由三位数字组成，这三位数字描述了请求过程中所发生的情况，便于程序进行差错处理。
reason-phrase	原因短语，数字状态码的可读版本，更便于人们阅读理解。

关于常见的状态码及原因短语的说明具体请参见 5.1.7 错误页面。

- 首部字段（headers）

起始行后面有零个或多个首部字段。HTTP 首部字段向请求和响应报文中添加了一些形式为“名称：取值”列表附加倍息。

- 主体（entity-body）

主体部分为可选项，其中包含了所有类型的数据，请求主体中包括了要发送给 Web 服务器的数据；响应主体中包含服务器要返回给客户端的数据。起始行和首部都是文本形式且都是结构化的，而主体则不同，主体中可以包含任意的二进制数据（比如文本、图片、视频、音频、软件程序）。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **协议合规**，激活“请求限制”页签，如下图所示。

步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置请求限制参数。

在配置请求限制时，各项参数的具体说明如下表所示。

参数	说明
启用状态	设置是否启用 HTTP 报文协议合规功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
最大请求头长度	设置 HTTP 请求报文中起始行和首部的最大长度，单位：字节；取值范围：0-8192；默认值：8192。
最大 Content_Length 值	设置 HTTP 请求报文主体的最大长度，单位：字节；取值范围：0-1048576000；默认值：10485760。
最大 Body 长度	当 HTTP 请求报文中无 Content_Length 参数时，可使用该参数限制报文主体的最大长度，单位：字节；取值范围：0-1048576000；默认值：10485760。
最大请求行长度	HTTP 报文请求行的最大长度，单位：字节；取值范围：0-4096；默认值：4096。
最大 header 行长度	设置 HTTP 请求首部每行“名称：取值”的最大长度，单位：字节；取值范围：0-4096；默认值：4096。

参数	说明
最多 Cookies 个数	设置保存的最大 Cookies 个数，取值范围：0-256；默认值：64。
最多 Header 头个数	HTTP 请求首部“名称：取值”最大个数，取值范围：0-256；默认值：64。
最多 Header 名称长度	设置 HTTP 请求首部名称的最大长度，取值范围：0-512；默认值：512。

步骤4 参数配置完成后，点击【应用】按钮完成配置。

CLI 方式

waf request-limits modify security-policy <*mstring*>] [**enable** <on|off>] [**header-length** <*num*>] [**content-length** <*num*>] [**body-length** <*num*>] [**request-line-length** <*num*>] [**header-line-length** <*num*>] [**cookies-number** <*num*>] [**header-number** <*num*>] [**header-name-length** <*num*>]

命令描述：

修改协议合规参数。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.15.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
enable <on|off>	可选项，设置是否启用请求参数限制功能。开启|关闭
header-length <*num*>	可选项，设置 HTTP 请求报文中起始行和首部的最大长度。数值类型，单位：字节；取值范围：0-8192；默认值：8192。
content-length <*num*>	可选项，设置 HTTP 请求报文主体的最大长度。数值类型，单位：字节；取值范围：0-1048576000；默认值：10485760。
body-length <*num*>	可选项，当 HTTP 请求报文中无 Content_Length 参数时，可设置该参数限制报文主体的最大长度。数值类型，单位：字节；取值范围：0-1048576000；默认值：10485760。
request-line-length	可选项，设置请求报文起始行长度。
num5	数值类型，单位：字节；取值范围：0-4096；默认值：4096。
header-line-length <*num*>	可选项，设置 HTTP 请求首部“名称：取值”最大长度。数值类型，单位：字节；取值范围：0-4096；默认值：4096。
cookies-number <*num*>	可选项，设置保存的最大 Cookies 个数。数值类型，取值

参数	说明
	范围：0-256；默认值：64。
header-number <*num*>	可选项，设置 HTTP 请求首部“名称：取值”最大个数。数值类型，取值范围：0-256；默认值：64。
header-name-length <*num*>	可选项，设置 HTTP 请求首部名称的最大长度。数值类型，取值范围：0-512；默认值：512。

命令示例：

在“sec01”安全策略中，设置请求报文主体的长度最大为 *30000*。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf request-limits modify security-policy** *sec01* **body-length** *30000*

waf request-limits show security-policy <*mstring*>

命令描述：

查看协议合规参数。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

显示“sec01”安全策略中的协议合规配置信息。

TopsecOS# **waf request-limits show security-policy** *sec01*

Security Name: sec01

Enable: on

Request Header Length: 8192

Content-Length: 10485760

Body Length:	30000
Request Line Length:	4096
Header Line Length:	4096
Cookie Num:	64
HEADER Num:	64
Header Name Length:	512

waf enumeration methods <cr>

命令描述：

查看支持的 HTTP 请求方法。

命令示例：

TopsecOS# **waf enumeration methods**

method : GET

method : PUT

method : POST

method : DELETE

method : CONNECT

method : OPTIONS

method : TRACE

method : PATCH

method : PROPFIND

method : PROPPATCH

method : MKCOL

method : COPY

method : MOVE

method : LOCK

method : UNLOCK

method : VERSION_CONTROL

method : CHECKOUT

method : UNCHECKOUT

method : CHECKIN

method : UPDATE

method : LABEL

method : REPORT

method : MKWORKSPACE

method : MKACTIVITY

method : BASELINE_CONTROL

method : MERGE

method : HEAD

method : OTHERS

waf request-limits reset security-policy <*mstring*>

命令描述：

恢复协议合规参数为默认值。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

5.2.3.2 参数限制

参数限制功能可以根据不同的参数对客户端发起的请求进行过滤，对其中的参数进行合法性检查，提高 Web 应用系统的安全性。在 Web 应用系统中大部分参数类型和内容都比较确定，例如部分的参数为数字类型、布尔类型等，通过对参数的限制，可以防御已知或者未知的攻

击，提高 Web 服务器的安全性。参数限制功能可以对不同的请求内容进行限制，包括文件类型、表单参数、文件大小等，以下介绍在参数限制中的几个常见的概念。

- Mime 类型

MIME（Multipurpose Internet Mail Extensions，多用途互联网邮件扩展类型）用以说明作为实体的基本媒体类型，例如 HTML 文件、MicrosoftWord 文档或是 MPEG 视频等。客户端应用程序使用 MlME 类型来解释和处理其内容。MIME 类型由一个主媒体类型以及一个子类型组成，子类型用于进一步描述媒体类型，主媒体类型与子类型直接用斜线 间隔，例如“text/html”表示 HTML 的文本文件，“image/gif”表示 GIF 图片。

常见 MIME 类型的主媒体类型如下表所示。

参数	说明
application	应用程序特有的内容格式
audio	音频格式
image	图片格式
message	报文类型
model	三维模型格式
multipart	多部分对象集合
text	文本格式
video	适配电影格式

常见的 MIME 类型与扩展名的对应关系如下表所示。

扩展名	MIME 类型	扩展名	MIME 类型
.atom	application/atom+xml	.midi	audio/midi
.jar	application/java-archive	.mp3、.mpga	audio/mpeg
.hqx	application/mac-binhex40	.gif	image/gif
.doc、.rtf、.wiz、.dot	application/msword	.jpe、.jpeg、.jfif、.jpg	image/jpeg
.pdf	application/pdf	.png、.pnz	image/png
.ps、.ai、.eps	application/postscript	.svg	image/svg+xml
.rtf	application/rtf	.tiff、.tif	image/tiff
.xla、.xlc、.xlt、.xlw	application/vnd.ms-excel	.wbmp	image/vnd.wap.wbmp
.xls	application/vnd.ms-excel	.ico	image/x-icon

扩展名	MIME 类型	扩展名	MIME 类型
.ppa、.pps、.pwz、.pot、.ppt	application/vnd.ms-powerpoint	.css	text/css
.wmlc	application/vnd.wap.wmlc	.html、.hts、.stm	text/html
.cco	application/x-cocoa	.sor、.sol、.txt	text/plain
.xht、.xhtm、.xhtml	application/xhtml+xml	.jad	text/vnd.sun.j2me.app-descriptor
.jnlp	application/x-java-jnlp-file	.wml、.htt	text/vnd.wap.wml
.js	application/x-javascript	.htc	text/x-component
.pm	application/x-perl	.cml、.dcd、.ent、.mtx、.rdf、.tsd、.wsdl、.xml、.xq、.xquery、.xsl、.biz、.dtd、.fo、.math、.mml、.spp、.svg、.tld、.vml、.vxml、.xdr、.xql、.xsd、.xslt	text/xml
.rar	application/x-rar-compressed	.3gp	video/3gpp
.swf	application/x-shockwave-flash	.mp4、.mpg4	video/mp4
.sit	application/x-stuffit	.mpg、.mpv2	video/mpeg
.tcl	application/x-tcl	.mov	video/quicktime
.der、.cer、.crt	application/x-x509-ca-cert	.m4v	video/x-m4v
.xpi	application/x-xpinstall	.asf、.asx	video/x-ms-asf
.zip	application/zip	.wmv	video/x-ms-wmv

- 请求方法

请求方法在 HTTP 请求报文的首行，是客户端希望服务器对资源执行的动作，是一个单独的词，比如 GET、HEAD 或 POST。

常用的请求方法及其作用如下表所示。

参数	说明
GET	请求指定的页面信息，并返回实体主体。
POST	请求服务器接受所指定的文档作为对所标识的 URI 的新的从属实体。
HEAD	只请求页面的首部。
PUT	从客户端向服务器传送的数据取代指定的文档的内容。

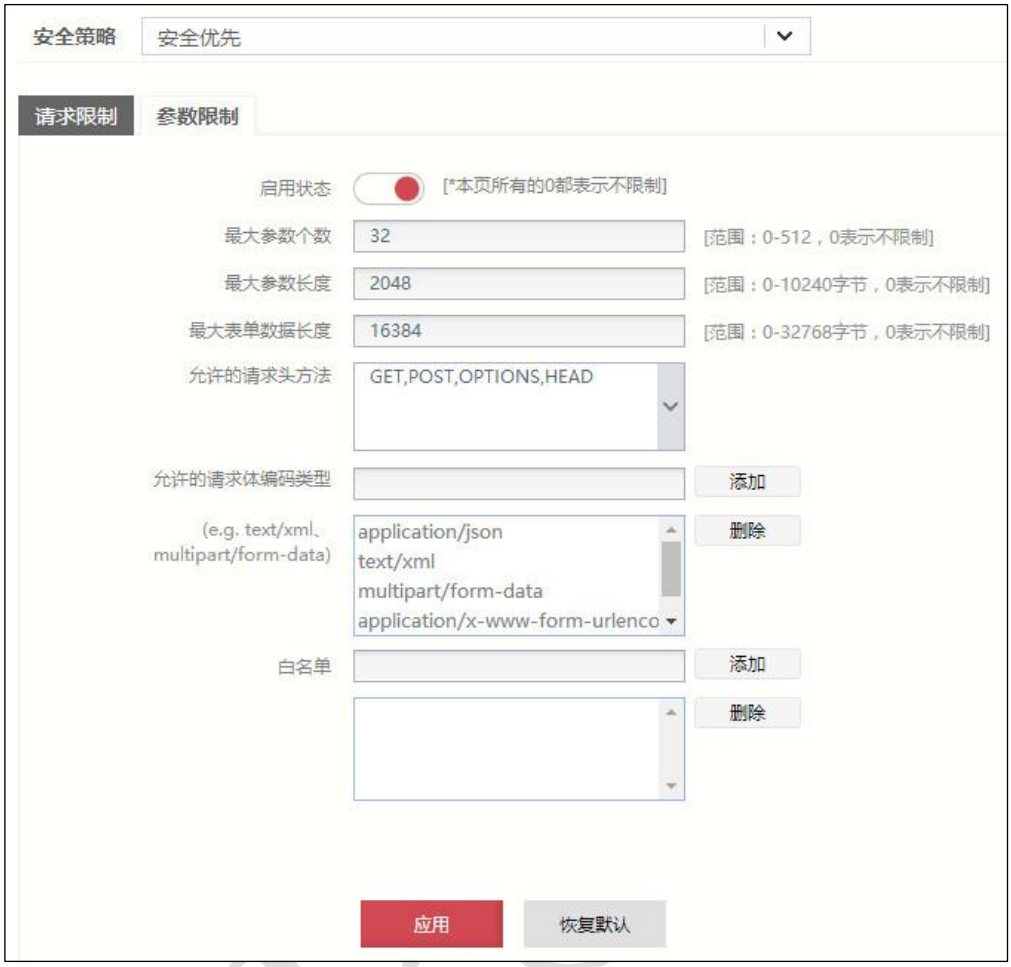
参数	说明
DELETE	请求服务器删除指定的页面。
OPTIONS	允许客户端查看服务器的性能。
CONNECT	用于代理进行传输，如使用 SSL。
TRACE	用于远程诊断服务器。
PATCH	实体中包含一个表，表中说明与该 URI 所表示的原内容的区别。
PROPFIND	获取资源的属性。
PROPPATCH	设置资源的属性。
MKCOL	创建集合（文件夹）。
COPY	请求服务器将指定的页面拷贝至另一个网络地址。
MOVE	请求服务器将指定的页面移至另一个网络地址。
LOCK	锁定资源。
UNLOCK	将之前锁定的资源解锁。

- 表单

HTML 表单用于搜集不同类型的用户输入。表单中填好的数据通常会被浏览器使用 GET 或 POST 请求发送给服务器，服务器解析表单内容，根据请求内容返回响应报文。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **协议合规**，激活“参数限制”页签，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置参数限制参数。

在配置参数限制时，各项参数的具体说明如下表所示。

参数	说明
启用状态	设置是否启用参数限制策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
最大参数个数	设置用户提交表单参数的最大个数，取值范围：1-512。
最大参数长度	设置用户提交的每个表单参数的最大长度，单位：字节；取值范围：0-65535；默认值：1024。
最大表单数据长度	设置用户提交的每个表单数据的最大长度，单位：字节；取值范围：0-32768 字节。
允许的请求头方法	选择允许的请求头方法。
允许的请求体编码类型	设置请求报文中允许的文件类型，支持 Mime 类型，点击【添加】按钮完成设置。
白名单	设置参数白名单，输入白名单参数，点击【添加】按钮完成白名单添加，可添加多条参数白名单。如果一个参数命中了

参数	说明
	参数白名单，后续将不会再用这个参数去进行规则匹配。

步骤4 参数配置完成后，点击【应用】按钮完成配置。

CLI 方式

waf parameter-limits modify security-policy <*mstring*>] [**enable** <on|off>][**max-arguments** <*num*>] [**max-argument-length** <*num*>] [**max-formdata-length** <*num*>] [**methods** <*mstring*>] [**request-body-types** <*mstring*>] [**whitelist-args** <*mstring*>]

命令描述：

修改参数限制参数。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
enable <on|off>	可选项，设置是否启用请求参数限制功能。开启|关闭
max-arguments <*num*>	可选项，设置最大表单参数个数。数值类型，取值范围：0-512；默认值：20。
max-argument-length <*num*>	可选项，设置每个表单的最大参数长度。数值类型，单位：字节；取值范围：0-65535；默认值：64。
max-formdata-length <*num*>	可选项，设置最大表单数据长度。数值类型，单位：字节；取值范围：0-32768 字节。
methods <*mstring*>	可选项，设置允许的请求方法。字符串类型，表示允许的请求方法；默认值：“GET,POST,OPTIONS,HEAD”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
request-body-types <*mstring*>	可选项，设置请求报文中允许的文件类型。字符串类型，MIME 类型格式：“主类型/子类型”，支持多输入形式，多个输入间用逗号分隔，如“image/gif,image/jpeg”。默认值：“image/gif,image/jpeg,application/pdf,application/octet-stream”。可使用 **waf enumeration mime-type** <cr>命令查看 TopWAF 支持的 MIME 类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
whitelist-args	可选项，设置白名单参数，逗号分隔。字符串类型，设置参数

参数	说明
<*mstring*>	白名单，多个参数用逗号分隔。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

在“sec01”安全策略中，修改请求报文表单参数最多为 *12* 个。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf parameter-limits modify security-policy** *sec01* **max-arguments** *12*

waf parameter-limits show security-policy <*mstring*>

命令描述：

查看参数限制参数。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

显示“69.200”安全策略的参数限制配置信息。

TopsecOS# **waf parameter-limits show security-policy** *69.200*

Security-Policy Name: 69.200

Enable: off

Max-Arguments: 32

Max-Argument-Length: 2048

Max-Formdata-Length: 16384

Methods: GET,POST,OPTIONS,HEAD

```
Request-Body-Types:
ny,application/x-www-form-urlencoded,multipart/form-data,text/xml,application/json
whitelist-args:
```

waf parameter-limits reset security-policy <*mstring*>

命令描述：

恢复参数限制参数为默认值。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

waf enumeration mime-type <cr>

命令描述：

查看 TopWAF 支持的 MIME 类型。

命令示例：

```
TopsecOS# waf enumeration mime-type
mime : any
mime : text/html
mime : text/css
mime : text/xml
mime : text/mathml
mime : text/plain
mime : text/vnd.sun.j2me.app-descriptor
mime : text/vnd.wap.wml
mime : text/x-component
```

mime : image/gif

mime : image/jpeg

mime : image/pjpeg

mime : image/png

mime : image/x-png

mime : image/tiff

mime : image/vnd.wap.wbmp

mime : image/x-icon

mime : image/x-jng

mime : image/bmp

mime : image/x-ms-bmp

mime : image/svg+xml

mime : image/webp

mime : application/x-javascript

mime : application/atom+xml

mime : application/rss+xml

mime : application/java-archive

mime : application/mac-binhex40

mime : application/msword

mime : application/pdf

mime : application/postscript

mime : application/rtf

mime : application/vnd.ms-excel

mime : application/vnd.ms-powerpoint

mime : application/vnd.wap.wmlc

mime : application/vnd.google-earth.kml+xml

mime : application/vnd.google-earth.kmz

mime : application/x-7z-compressed

mime : application/x-cocoa

mime : application/x-java-archive-diff

mime : application/x-java-jnlp-file

mime : application/x-makeself

mime : application/x-perl

mime : application/x-pilot

mime : application/x-rar-compressed

mime : application/x-redhat-package-manager

mime : application/x-sea

mime : application/x-shockwave-flash

mime : application/x-stuffit

mime : application/x-tcl

mime : application/x-x509-ca-cert

mime : application/x-xpinstall

mime : application/xhtml+xml

mime : application/zip

mime : application/octet-stream

mime : audio/midi

mime : audio/mpeg

mime : audio/ogg

mime : audio/x-m4a

mime : audio/x-realaudio

mime : video/3gpp

mime : video/mp4

mime : video/mpeg

mime : video/quicktime

mime : video/webm

mime : video/x-flv

mime : video/x-m4v

mime : video/x-mng

```
mime : video/x-ms-asf
mime : video/x-ms-wmv
mime : video/msvideo
mime : video/x-msvideo
mime : video/avi
```

waf enumeration methods <cr>

命令描述：

查看 TopWAF 支持的请求方法。

命令示例：

```
TopsecOS# waf enumeration methods
method : GET
method : PUT
method : POST
method : DELETE
method : CONNECT
method : OPTIONS
method : TRACE
method : PATCH
method : PROPFIND
method : PROPPATCH
method : MKCOL
method : COPY
method : MOVE
method : LOCK
method : UNLOCK
method : VERSION_CONTROL
method : CHECKOUT
```

method : UNCHECKOUT

method : CHECKIN

method : UPDATE

method : LABEL

method : REPORT

method : MKWORKSPACE

method : MKACTIVITY

method : BASELINE_CONTROL

method : MERGE

method : HEAD

method : OTHERS

5.2.4 文件控制

5.2.4.1 文件上传限制

文件上传限制功能用于检查用户上传的文件，防止恶意用户利用文件上传功能攻击 Web 服务器，例如上传 webshell 脚本控制服务器、上传大尺寸的垃圾文件占用服务器空间。TopWAF 支持检查客户端上传服务器的文件扩展名、个数、大小、Mime 类型等参数。扩展名的限制是防止上传 webshell 的有效方法，因为 Web 服务器会依据文件扩展名关联脚本解析器，如果扩展名不对，即使文件内容是 webshell 它也不会被解析，产生不了危害。

- Mime 类型

MIME（Multipurpose Internet Mail Extensions，多用途互联网邮件扩展类型）用以说明作为实体的基本媒体类型，例如 HTML 文件、MicrosoftWord 文档或是 MPEG 视频等。客户端应用程序使用 MlME 类型来解释和处理其内容。MIME 类型由一个主媒体类型以及一个子类型组成，子类型用于进一步描述媒体类型，主类型与子类型直接用斜线 间隔，例如“text/html”表示 HTML 的文本文件，“image/gif”表示 GIF 图片。

常见 MIME 类型的主媒体类型如下表所示。

参数	说明
application	应用程序特有的内容格式
audio	音频格式
image	图片格式
message	报文类型
model	三维模型格式
multipart	多部分对象集合
text	文本格式
video	适配电影格式

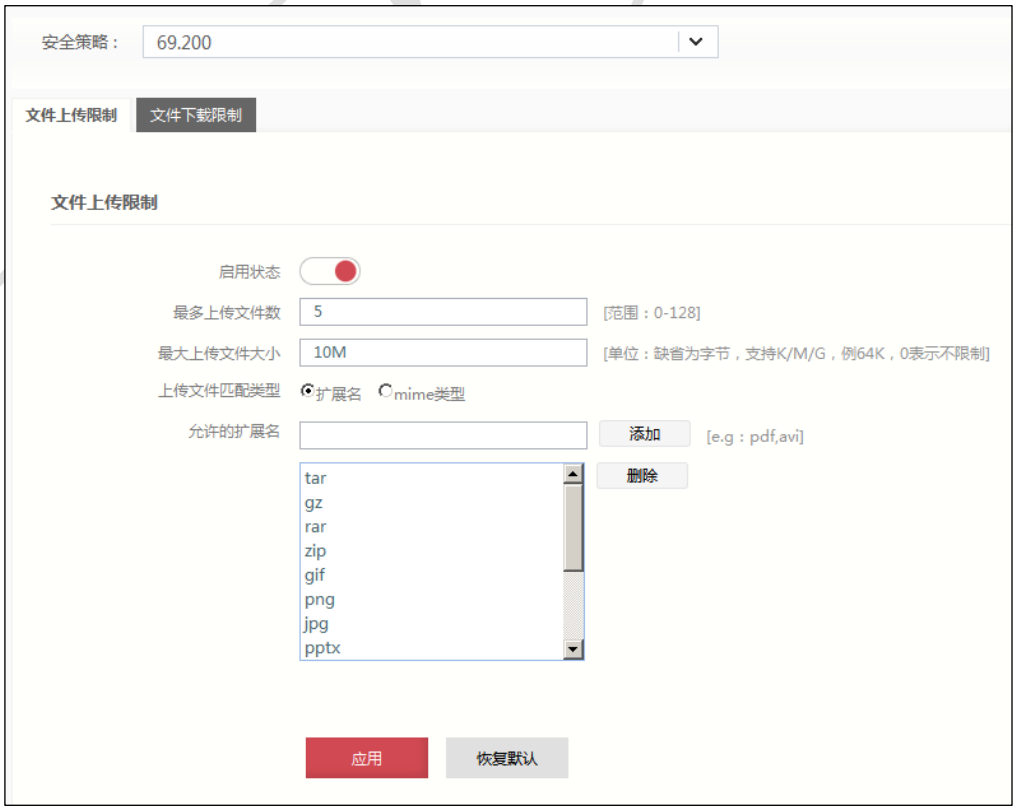
常见的 MIME 类型与扩展名的对应关系如下表所示。

扩展名	MIME 类型	扩展名	MIME 类型
.atom	application/atom+xml	.midi	audio/midi
.jar	application/java-archive	.mp3、.mpga	audio/mpeg
.hqx	application/mac-binhex40	.gif	image/gif
.doc、.rtf、.wiz、.dot	application/msword	.jpe、.jpeg、.jfif、.jpg	image/jpeg
.pdf	application/pdf	.png、.pnz	image/png
.ps、.ai、.eps	application/postscript	.svg	image/svg+xml
.rtf	application/rtf	.tiff、.tif	image/tiff
.xla、.xlc、.xlt、.xlw	application/vnd.ms-excel	.wbmp	image/vnd.wap.wbmp
.xls	application/vnd.ms-excel	.ico	image/x-icon
.ppa、.pps、.pwz、.pot、.ppt	application/vnd.ms-powerpoint	.css	text/css
.wmlc	application/vnd.wap.wmlc	.html、.hts、.stm	text/html
.cco	application/x-cocoa	.sor、.sol、.txt	text/plain
.xht、.xhtm、.xhtml	application/xhtml+xml	.jad	text/vnd.sun.j2me.app-descriptor
.jnlp	application/x-java-jnlp-file	.wml、.htt	text/vnd.wap.wml
.js	application/x-javascript	.htc	text/x-component
.pm	application/x-perl	.cml、.dcd、.ent、.mtx、.rdf、.tsd、.wsdl、.xml、.xq、.xquery、.xsl、.biz、.dtd、.fo、.math、.mml、.	text/xml

扩展名	MIME 类型	扩展名	MIME 类型
		spp、.svg、.tld、.vml、.vxml、.xdr、.xql、.xsd、.xslt	
.rar	application/x-rar-compressed	.3gp	video/3gpp
.swf	application/x-shockwave-flash	.mp4、.mpg4	video/mp4
.sit	application/x-stuffit	.mpg、.mpv2	video/mpeg
.tcl	application/x-tcl	.mov	video/quicktime
.der、.cer、.crt	application/x-x509-ca-cert	.m4v	video/x-m4v
.xpi	application/x-xpinstall	.asf、.asx	video/x-ms-asf
.zip	application/zip	.wmv	video/x-ms-wmv

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **文件控制**，激活“文件上传限制”页签，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置文件上传限制参数。

在配置文件上传限制参数时，各项参数的具体说明如下表所示。

参数	说明
启用状态	设置是否开启文件上传限制策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
最多上传文件数	设置通过 Web 服务器上传的文件最大个数，整数形式，取值范围：0-128，其中 0 表示不作限制；默认值：5。
最大上传文件大小	设置通过 web 服务器上传的文件限制大小，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：10M。 说明：单位不区分大小写。
上传文件匹配类型	设置允许上传的文件类型。 扩展名：设置文件类型的扩展名，如 PDF 文档的扩展名为“.pdf”。 Mime 类型：设置文件的 MIME 类型，格式为“主类型/子类型”。 关于 Mime 类型、常见的文件扩展名与 MIME 类型的对应关系具体请参见 5.2.3.2 参数限制。
允许的拓展名/mime 类型	设置允许上传的文件的拓展名/mime 类型。在右侧的文本框中输入扩展名/mime 类型后，点击右侧的【添加】按钮，将输入的拓展名/mime 类型添加到列表中。

步骤4 参数配置完成后，点击【应用】按钮完成配置。

CLI 方式

waf upload-policy modify security-policy <*mstring*> [**enable** <on|off>] [**upload-files** <*num*>] [**upload-size** <*string*>] [**match-types** <extension|mime>] [**upload-types** <*mstring*>]

命令描述：

修改文件上传限制规则。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
enable <on|off>	可选项，设置是否启用文件上传限制限制功能。开启|关闭，默认值：关闭。

参数	说明
upload-files <*num*>	可选项，设置最大上传文件个数。数值类型，取值范围：0-128，其中 0 表示不作限制；默认值：5。
upload-size <*string*>	可选项，设置最大上传文件大小。字符串类型，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：10M。 说明：单位不区分大小写。
match-type <extension|mime>	可选项，设置上传文件匹配类型，扩展名|MIME。 MIME 类型格式：“主类型/子类型”，支持多输入形式，多个输入间用逗号分隔，如“image/gif,image/jpeg”。 扩展名：设置文件类型的扩展名，如 PDF 文档的扩展名为“pdf”。 默认值： “image/gif,image/jpeg,application/pdf,application/octet-stream”。
[**upload-types** <*mstring*>]	设置允许上传的文件类型，如'pdf,avi'或'application/pdf,video/x-msvideo'。

命令示例：

在“sec01”安全策略中，启用文件上传限制规则。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf upload-policy modify security-policy** *sec01* **enable** on

waf upload-policy show security-policy <*mstring*>

命令描述：

查看文件上传限制配置信息。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

显示“sec01”安全策略的文件上传限制配置信息。

TopsecOS# **waf upload-policy show security-policy** *sec01*

Security-Policy Name: sec01

Enable: off

Upload-Files: 5

Upload-Size: 64k

Match-type: extension

Allow extensions:

waf upload-policy reset security-policy <*mstring*>

命令描述：

恢复文件上传限制配置信息为出厂配置。

参数说明：

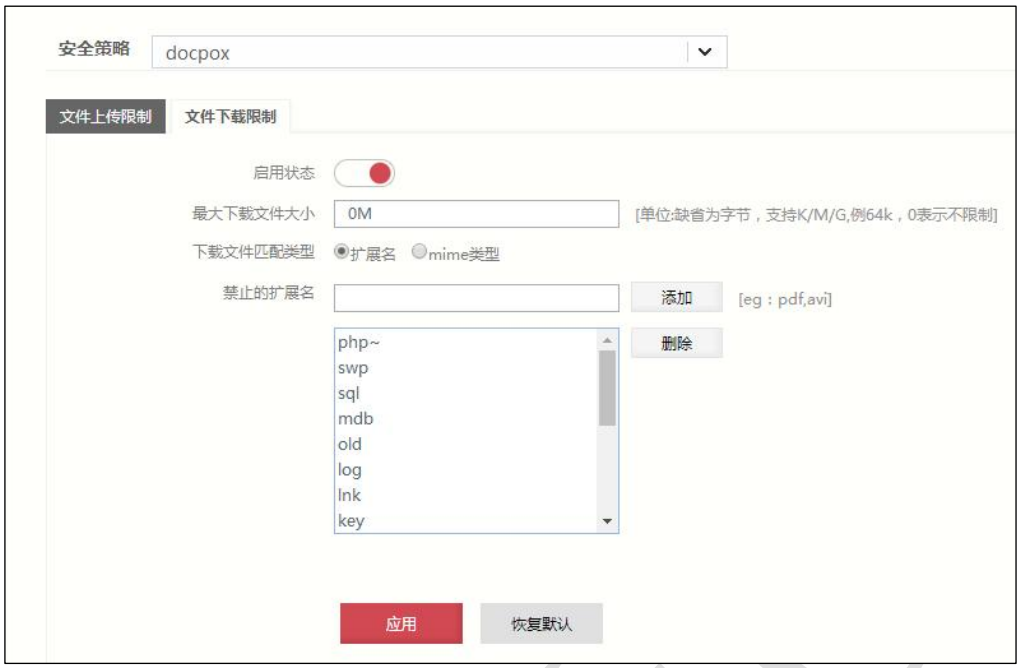
参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

5.2.4.2 文件下载限制

文件下载限制功能用于检查用户下载的文件，防止敏感文件泄漏（比如包含用户信息的数据库文件）。TopWAF 支持检查客户端下载服务器的文件大小、类型等参数。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **文件控制**，激活“文件下载限制”页签，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置文件下载限制参数。

在配置文件下载限制参数时，各项参数的具体说明如下表所示。

参数	说明
启用状态	设置是否开启文件下载限制策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
最大下载文件大小	设置通过 web 服务器下载的文件限制大小，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：10M。 说明：单位不区分大小写。
下载文件匹配类型	设置禁止下载的文件类型。 扩展名：设置文件类型的扩展名，如 PDF 文档的扩展名为“.pdf”。 Mime 类型：设置文件的 MIME 类型，格式为“主类型/子类型”。 关于 Mime 类型、常见的文件扩展名与 MIME 类型的对应关系具体请参见 5.2.3.2 参数限制。
禁止扩展名/mime 类型	设置禁止下载的文件的拓展名/mime 类型。在右侧的文本框中输入扩展名/mime 类型后，点击右侧的【添加】按钮，将输入的拓展名/mime 类型添加到列表中。

步骤4 参数配置完成后，点击【应用】按钮完成配置。

CLI 方式

waf download-policy modify security-policy <*mstring*> [**enable** <on|off>] [**download-size** <*string*>] [**match-type** <extension|mime>][**forbid-types** <*mstring*>]

命令描述：

修改文件下载限制规则。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
enable <on|off>	可选项，设置是否启用文件下载限制限制功能。开启|关闭，默认值：关闭。
download-size <*string*>	可选项，设置最大下载文件大小。字符串类型，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：10M。 说明：单位不区分大小写。
match-type <extension|mime>	可选项，设置下载文件匹配类型，扩展名|mime。 MIME 类型格式：“主类型/子类型”，支持多输入形式，多个输入间用逗号分隔，如“image/gif,image/jpeg”。 扩展名：设置文件类型的扩展名，如 PDF 文档的扩展名为“pdf”。 默认值： “image/gif,image/jpeg,application/pdf,application/octet-stream”。
forbid-types <*mstring*>	可选项，设置不允许下载文件类型。字符串类型，表示禁止下载的文件拓展名。 注意：不能以“\\”结尾或不包含“<script>”字符串。

waf download-policy show security-policy <*mstring*>

命令描述：

查看文件下载限制配置信息。

参数说明：

参数	说明
security-policy	必选项，设置安全策略名称。关于安全策略的配置具体请

参数	说明
<*mstring*>	参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

显示“hdq”安全策略的文件下载限制配置信息。

```
TopsecOS# waf download-policy show security-policy hdq
Security-Policy Name:       hdq
Enable:                     on
Download-Size:              10M
Match-type:                 extension
Forbid extensions:      bat,cfg,cs,csr,conf,dat,db,dll,ini,key,lnk,log,old,mdb,sql,swp,php~
```

waf download-policy reset security-policy <*mstring*>

命令描述：

恢复文件下载限制配置信息为出厂配置。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

5.2.5 URI 例外

URI 例外用于对特定的 URI 单独配置防护策略，而不使用安全策略中的默认值。每个安全策略最多可以创建 128 条 URI 例外策略。与访问控制策略类似，URI 例外同样支持普通和正则两种 URI 类型。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **URI 例外**。

步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 点击『添加』，弹出“添加 URI 例外”窗口，如下图所示。

在配置 URI 例外基本参数时，各项参数的具体说明如下表所示。

参数	说明
名称	设置 URI 例外名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
是否开启此策略	设置是否开启 URI 策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
是否开启协议合规检查	设置是否开启协议合规检查。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
例外 URI 路径类型	设置 URI 地址的类型。可选项：普通、正则。 普通类型：URI 指通过单个字符串来描述一个 URI 路径； 正则类型：URI 指通过单个字符串来描述一系列符合某个语法规则的 URI 路径。
例外 URI 路径	URI 路径类型设置为“普通”时，该参数有效。设置 TopWAF 所保护的某个网站地址，格式：以单斜线“/”开头的字符串，如“/index.htm”。
URI 路径正则	URI 类型设置为“正则”时，该参数有效。使用正则表达式设置 TopWAF 所保护的一系列 Web 网站地址。
描述	设置 URI 例外策略的描述信息。

步骤4 配置 URI 例外防御策略。激活“防护策略”页签，如下图所示。

在配置 URI 例外基本参数时，各项参数的具体说明如下表所示。

参数		说明
防御设置	防御	设置开启的防御类型。可选项：XSS 防护、SQL Injection 防护、目录遍历防护、RFI 防护、OS Command Injection 防护、Information leakage 防护、网页扫描防护、自定义防护策略、LDAP 注入防护、SSI 注入防护、XPath 注入防护、Web 服务器漏洞防护、WebShell 防护、其它规则防护，关于防御类型的说明具体请参见 5.2.6 防护策略。
	请求方法	勾选请求方法。点击『添加』，可添加 URI 例外规则允许的请求方法，关于请求方法的描述具体请参见 5.2.3.2 参数限制。
参数限制	最大参数个数	设置用户提交表单的最大个数，取值范围：0-512，其中 0 表示不作限制；默认值：20。
	最大参数长度	设置用户提交的每个表单中参数名称的最大长度，单位：字节；取值范围：0-10240，其中 0 表示不作限制；默认值：64。
	最大表单数据长度	设置用户提交的每个表单中参数取值的最大长度，单位：字节；取值范围：0-32768，其中 0 表示不作限制；默认值：16384。
	参数限制	点击『添加』，添加限制的参数。 参数名：设置参数名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。 最大长度：设置参数的最大长度。 数据类型：选择参数的数据类型，可选项 string（字符串）、

参数		说明
		number（数值）、ascii（ASCII 码）、email（邮件地址）、postcode（邮编）、uri（URI 地址）、date（日期）、Chinese_character（汉字）、mobilephone（手机号码）、credit_card（信用卡号）、ip（IP 地址）、unix_device_name、microsoft_product_key、telephone（电话号码）。 是否必选：设置该参数是否是必选参数。 说明： 数据类型除了系统内置的参数类型外，还支持自定义的数据类型，关于自定义数据类型具体请参见 5.1.6 数据类型。用户在添加完自定义类型后，需要在安全策略中引用该自定义数据类型才能生效，具体请参见 5.2.15 高级设置。
上传限制	上传限制策略方式	设置是否启用文件上传规则。可选项：使用全局默认值、启用自定义设置。默认为“使用全局默认值”，设置为关闭时，将不对上传的文件信息进行限制。
	最多上传文件数	设置通过 Web 服务器上传的文件最大个数，整数形式，取值范围：0-128，其中 0 表示不作限制；默认值：5。
	最大上传文件大小	设置通过 web 服务器上传的文件限制大小，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：64K。 说明：单位不区分大小写。
	上传文件匹配类型	设置允许上传的文件类型。可选项：扩展名、mime 类型。 扩展名：设置文件类型的扩展名，如 PDF 文档的扩展名为“.pdf”。 Mime 类型：设置文件的 MIME 类型，格式为“主类型/子类型”。 关于 Mime 类型、常见的文件扩展名与 MIME 类型的对应关系具体请参见 5.2.3.2 参数限制。
下载限制	下载限制策略方式	设置是否启用文件下载规则。可选项：使用全局默认值、启用自定义设置。默认为“使用全局默认值”，设置为关闭时，将不对上传的文件信息进行限制。
	最大下载文件大小	设置通过 web 服务器下载的文件限制大小，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：64K。 说明：单位不区分大小写。
	下载文件匹配类型	设置允许下载的文件类型。可选项：扩展名、mime 类型。 扩展名：设置文件类型的扩展名，如 PDF 文档的扩展名为“.pdf”。 Mime 类型：设置文件的 MIME 类型，格式为“主类型/子类型”。 关于 Mime 类型、常见的文件扩展名与 MIME 类型的对应关系具体请参见 5.2.3.2 参数限制。

步骤5 参数配置完成后，点击【确定】按钮完成配置。

CLI 方式

waf exception add name <*mstring*> **security-policy** <*mstring*> **type** <normal|regex> **url** <*mstring*> [**enable** <on|off>] [**defence** <*mstring*>] [**description** <*mstring*>] [**constraint** <on|off>] [**arguments** <*mstring*>] [**max-arguments** <*num*>] [**max-argument-length** <*num*>] [**methods** <*mstring*>] [**upload-enable** <on|off |default>] [**upload-max-files** <*num*>] [**upload-max-size** <*string*>] [**match-type** <mime|extension>] [**allow-types** <*mstring*>] [**max-formdata-length** <*num*>] [**whitelist-enable** <on|off|default>] [**whitelist-args** <*mstring*>] [**download-enable** <on|off|default>] [**download-forbid-types** <*mstring*>][**download-match-type** <extension|mime>][**download-max-size** <*string*>]

命令描述：

添加 URI 例外。

可使用 **waf exception delete name** <*mstring*> **security-policy**<*mstring*>命令删除 URI 例外。

可使用 **waf exception modify name** <*mstring*> **security-policy** <*mstring*>命令修改 URI 例外。

参数说明：

参数	说明
name <*mstring*>	必选项，设置 URI 例外名称。字符串类型，表示 URI 例外名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
type <normal|regex>	必选项，设置 URI 地址类型。普通|正则
url <*mstring*>	必选项，设置 URI 地址。字符串类型，表示 URI 地址， 当 type 类型为 normal 时：设置 TopWAF 所保护的某个网站地址，格式：以单斜线“/”开头的字符串，如“/index.htm”。 当 type 类型为 regex 时：URI 类型设置为“正则”时，该参数有效。使用正则表达式设置 TopWAF 所保护的一系列 Web 网站地址。

参数	说明
	注意：不能以“\\”结尾或不包含“<script>”字符串。
enable <on|off>	可选项，设置是否开启 URI 例外。开启|关闭
defence <*mstring*>	可选项，设置 URI 攻击防御类型。字符串类型，可选参数 xss|sqli|osi|rfi|lfi|dir|leak|other|user|robots|scanner，默认值：关闭 csrf 攻击防御，开启 xss|sqli|osi|rfi|lfi|dir|leak|other|user|robots|scanner 攻击防御。
desciption <*mstring*>	可选项，设置 URI 例外的描述信息。字符串形式，表示 URI 例外的描述信息。 注意：不能以“\\”结尾或不包含“<script>”字符串。
constraint <on|off>	可选项，设置是否开启请求参数限制功能。开启|关闭，默认值：开启。
arguments <*mstring*>	可选项，设置限制参数。串类型，表示限制参数，格式为：“参数名,最大长度,数据类型,是否必选”，如“length,200,string,1”表示名为 length 的参数，最大长度为 200，字符串类型，必选参数。 注意：不能以“\\”结尾或不包含“<script>”字符串。
max-arguments <*num*>	可选项，设置最大表单参数个数。数值类型，取值范围：0-512，其中 0 表示不作限制；默认值：20。
max-argument-length <*num*>	可选项，设置每个表单的最大参数长度。数值类型，单位：字节；取值范围：0-10240，其中 0 表示不作限制；默认值：64。
methods <*mstring*>	可选项，设置允许的请求方法。字符串类型，表示允许的请求方法，默认值：GET,POST,OPTIONS,HEAD。 注意：不能以“\\”结尾或不包含“<script>”字符串。
upload-enable <on|off|default>	可选项，设置是否启用文件上传限制限制功能。开启|关闭|使用全局默认值，默认值：使用全局默认值。
upload-max-files <*num*>	可选项，设置最大上传文件个数。数值类型，取值范围：0-128，其中 0 表示不作限制；默认值：5。
upload-max-size <*string*>	可选项，设置最大上传文件大小。数值类型，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：64K。 说明：单位不区分大小写。
match-type <mime|extension>	可选项，设置上传文件匹配类型。MIME 类型|扩展名，默认值：MIME 类型。
allow-types <*mstring*>	可选项，设置允许的文件类型。字符串类型，表示允许的文件类型。 MIME 类型格式：“主类型/子类型”，支持多输入形式，多个输入间用逗号分隔，如“image/gif,image/jpeg”。 扩展名：设置文件类型的扩展名，如 PDF 文档的扩展名为“pdf”。 默认值： “image/gif,image/jpeg,application/pdf,application/octet-stream”。

参数	说明
	注意：不能以“\\”结尾或不包含“<script>”字符串。
max-formdata-length <*num*>	可选项，设置最大 x-www-form-urlencoded 表单长度，范围(0-32768)，0 代表不限制。数值类型，取值范围 0-32768，0 代表不限制。
whitelist-enable <on|off|default>	可选项，设置白名单参数检查是否开启。开启|关闭|使用全局默认值，默认值：使用全局默认值。
whitelist-args <*mstring*>	可选项，设置白名单参数，逗号分隔，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
download-enable <on|off|default>	设置下载限制策略方式，可选项：开启|关闭|默认。
download-forbid-types <*mstring*>	设置禁止文件类型，如'pdf,avi'或'application/pdf,video/x-msvideo'
download-match-type <extension|mime>	设置下载文件匹配类型，可选项：扩展名|mime 类型。
download-max-size <*string*>	最大下载文件大小,如 1024,1k,2m,4G。

命令示例：

在“sec01”安全策略中，添加并启用名称为 ur-ex 的 URI 例外规则，实现对普通类型的 URI 地址/test 的 XSS 攻击的防御，并设置该规则的描述信息为 *test*。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf exception add name** *url-ex* **security-policy** *sec01* **enable** on **defence** *xss* **type** normal **url** /test **desciption** *test*

waf exception show [**name** <*mstring*>] **security-policy** <*mstring*>

命令描述：

查看 URI 例外配置信息。

命令示例：

显示“sec01”安全策略中，名称为 *url-ex* 的 URI 例外规则配置信息。

TopsecOS# **waf exception show name** *url-ex* **security-policy** *sec01*

ID: 8127

name: url-ex

enable: on

url: /test

type: normal

methods: GET,POST,OPTIONS,HEAD

defence: xss,scanner,sqli,osi,rfi,dir,leak,ldap,other,xpath,ssi,serv

er,user

constraint: on

upload: default

arguments:

max arguments: 20

max argument length: 64

max formdata length: 16384

upload-max-files: 5

upload-max-size: 64k

match-type: mime

allow-types: 'image/gif,image/jpeg,application/pdf,application/octet-str

eam'

description:

whitelist-enable: default

whitelist-args:

waf exception clean security-policy *<mstring>*

命令描述：

清除所有的 URI 例外配置。

命令示例：

清除“sec01”安全策略中的所有 URI 例外配置。

TopsecOS# **waf exception clean security-policy** *sec01*

命令示例：

在“sec01”安全策略的 URI 例外规则 *url-ex* 中，添加名称为 num，最大长度为 100 的数值类型，并设置为必选项。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf exception add name** *url-ex* **security-policy** *sec01* **type** normal **url** /test

TopsecOS# **waf exception add-argument name** *url-ex* **security-policy** *sec01* **argument** *num* **max-argument-length** *100* **datatype** *num* **require** *yes*

waf exception clean-argument name <*mstring*> **security-policy** <*mstring*>

命令描述：

清除 URI 例外中的参数限制规则。

命令示例：

清除“sec01”安全策略的 URI 例外规则 *url-ex* 所有配置信息。

TopsecOS# **waf exception clean-argument name** *url-ex* **security-policy** *sec01*

waf exception add-upload name <*mstring*> **security-policy** <*mstring*> **upload-type** <*mstring*>

命令描述：

添加 URI 例外文件上传限制规则。

可使用 **waf exception delete-upload name** <*mstring*> **security-policy**<*mstring*> **upload-type** <*mstring*>命令删除 URI 例外文件上传限制规则。

可使用 **waf exception modify-upload name** <*mstring*> **security-policy** <*mstring*> **upload-type** <*mstring*>命令修改 URI 例外文件上传限制规则。

命令示例：

在“sec01”安全策略的 URI 例外规则 url-ex 中添加文件上传限制，限制仅支持上传 PDF 格式文件。

TopsecOS#**waf security-policy add name** *sec01*

TopsecOS#**waf exception add name** *url-ex* **security-policy** *sec01* **type normal url** /test

TopsecOS#**waf exception add-upload name** *url-ex* **security-policy** *sec01* **upload-type** *pdf*

5.2.6 防护策略

TopWAF 的防护策略针对 Web 应用安全漏洞实施防护，如 SQL 注入、XML 注入、XSS 等。TopWAF 支持常见的 XSS（Cross Site Scripting，跨站脚本）攻击、SQL Injection 攻击、OS Command Injection 攻击、RFI（Remote File Include，远程文件包含）攻击、本地文件包含）攻击、目录遍历攻击、Information leakage 攻击，网页恶意扫描攻击、LDAP 注入防护、SSI 注入防护、XPath 注入防护、Web 服务器漏洞防护、Webshell 防护等，并支持根据用户实际需求自定义攻击防御策略。

1）XSS 攻击：XSS 是一种经常出现在 Web 应用中的计算机安全漏洞，它允许攻击者将代码植入到提供给其它用户使用的页面中。攻击者可以利用 XSS 攻击对服务器造成各种危害，例如盗取各类用户帐号、控制企业数据、盗窃企业重要的具有商业价值的资料、非法转账、强制发送电子邮件、控制受害者机器向其它网站发起攻击等。

2）SQL Injection 攻击：SQL 注入是发生于应用程序数据库的安全漏洞。在输入的数据中注入 SQL 指令，在设计不良的程序当中忽略了检查用户输入数据的合法性，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，这些注入进去的查询指令就会被数据库服务器误认为是正常的 SQL 指令而运行，入侵者可根据程序返回的结果，获得某些他想得知的数据，甚至可以破坏数据库内容。

3）OS Command Injection 攻击：操作系统命令注入攻击，如果未对用户输入进行限制，攻击者可以在 HTML 代码中输入操作系统调用命令，并在操作系统上作为正常指令执行，此时将发生操作系统命令注入攻击。

4）RFI（Remote File Include，远程文件包含）：RFI 允许用户上传图像或者文件。但是在这些看似无害的文件或图片上传实际上可能包含某种形式的恶意有效载荷，这有可能导致攻击者破坏服务器。RFI 漏洞可能带来的损坏要远远超过 SQL 注入攻击，在注入攻击中，攻击者只是针对数据库，而 RFI 攻击会使攻击者能够提取数据，攻击者可能获得对网站的控制。

5）LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议），是一种在线目录访问协议，主要用于目录中资源的搜索和查询。LDAP 注入攻击和 SQL 注入攻击相似，利用用户引入的参数生成 LDAP 查询。一个安全的应用在构造和将查询发送给服务器前应该净化用户传入的参数。在有漏洞的环境中，这些参数没有得到合适的过滤，因而攻击者可以注入任意恶意代码。控制用于目录搜索服务的过滤器，在应用中插入了非法的查询内容，如果没有对用户输入内容就提交查询时，就会产生 LDAP 注入攻击，使 LDAP 目录的信息遭到泄露或者破坏。

6）目录遍历：目录遍历是 HTTP 所存在的一个安全漏洞，它使得攻击者能够访问受限制的目录，并在 Web 服务器的根目录以外执行命令。

7）信息泄露：信息泄露是指攻击者使用获取到系统的配置信息或者调试信息，进而了解系统的内部架构，据此找到系统漏洞并制定攻击计划。

8）网页扫描：网页扫描可以自动侦察系统安全，找出系统的安全弱点。通过对 TCP 的端口和服务的侦察，然后将信息记录下来，提供目标的安全分析报告。

9）xPath 注入：xPath 注入攻击针对 XML 数据信息的一种注入攻击，利用 XPath 解析器的松散输入和容错特性，能够在 URL、表单或其它信息上附带恶意的 XPath 查询代码，以获得权限信息的访问权并更改这些信息。XPath 注入攻击是针对 Web 服务应用新的攻击方法，允许

攻击者在事先不知道 XPath 查询相关知识的情况下，通过 XPath 查询得到一个 XML 文档的完整内容。

10）SSI 注入：SSI 注入攻击式一种针对服务器端的攻击，攻击者发送代码到 Web 应用程序里，代码在服务器本地运行。用户输入的数据被插入到服务器端的 HTML 文件前执行，导致对所有用的输入验证失败。

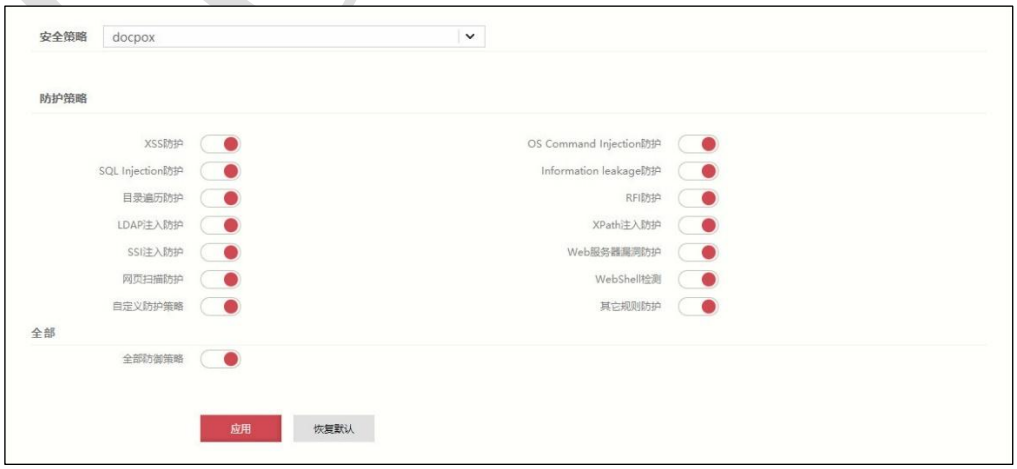
11）Web 服务器漏洞：很多 WEB 服务器有 BUG，对于协议解析处理不当，容易被恶意攻击者利用，开启 Web 服务器漏洞防护功能，可以阻止利用服务器漏洞进行的恶意攻击访问，保护服务器安全。

12）WebShell：是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将 asp 或 php 后门文件与网站服务器 WEB 目录下正常的网页文件混在一起，然后就可以使用浏览器来访问 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的。

防护策略指定了安全策略需要防护的攻击类型，在 TopWAF 中，规则库中所有的规则根据防护的攻击类型被分类，当防护策略启用了某类防护，则对应的规则在 HTTP 会话处理中将被执行，关于规则库的描述具体请参见 5.2.13 规则库。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **防护策略**，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置防护策略参数。

在配置防护策略时，各项参数的具体说明如下表所示。

参数	说明
XSS 防护	设置是否启用 XSS 防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
OS Command Injection 防护	设置是否启用 OS 命令注入防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
SQL Injection 防护	设置是否启用 SQL Injection 防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
Information leakage 防护	设置是否启用信息泄露防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
目录遍历防护	设置是否启用目录遍历防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
RFI 防护	设置是否启用 RFI 防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
LDAP 注入防护	设置是否启用 LDAP 注入防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
xPath 注入防护	设置是否启用 xPath 注入防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
SSI 注入防护	设置是否启用 SSI 注入防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
Web 服务器漏洞防护	设置是否启用 Web 服务器漏洞防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
网页扫描防护	设置是否启用网页恶意扫描防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
WebShell 防护	设置是否启用 WebShell 防护功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
其它规则防护	设置是否开启其他类型的防护规则。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。关于其他类型的防护规则具体请参见 5.2.13 规则库。
自定义防护策略	设置是否启用管理员自定义的防护策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。关于自定义防护策略的描述具体请参见 5.2.14 自定义策略。
全部防御策略	设置是否启用全部的防御策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。

步骤4 参数配置完成后，点击【应用】按钮，完成防护策略的配置。点击【恢复默认】按钮，将防护策略的配置恢复为出厂的默认配置。

CLI 方式

waf defence-policy modify security-policy <*mstring*> [**xss** <on|off>] [**sqli** <on|off>] [**osi** <on|off>] [**rfi** <on|off>] [**dir** <on|off>] [**user** <on|off>] [**scanner** <on|off>] [**ssi** <on|off>] [**xpath** <on|off>] [**ldap** <on|off>] [**leakage** <on|off>] [**webshell** <on|off>] [**server** <on>] [**other** <on|off>] [**all** <on|off>]

命令描述：

修改防护策略中的防御模块的开启状态。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
xss <on|off>	设置是否开启防跨站脚本攻击。开启|关闭，默认值：开启。
sqli <on|off>	设置是否开启防 SQL 注入攻击。开启|关闭，默认值：开启。
osi <on|off>	设置是否开启防系统命令注入攻击。开启|关闭，默认值：开启。
rfi <on|off>	设置是否开启防远程文件包含攻击。开启|关闭，默认值：开启。
dir <on|off>	设置是否开启防目录遍历攻击。开启|关闭，默认值：开启。
user <on|off>	设置是否开启用户自定义攻击防御规则。开启|关闭，默认值：开启。
scanner <on|off>	设置是否开启防恶意扫描攻击。开启|关闭，默认值：开启。
ssi <on|off>	设置是否开启 SSI 攻击防护。开启|关闭，默认值：开启。
xpath <on|off>	设置是否开启 xPath 攻击防护。开启|关闭，默认值：开启。
ldap <on|off>	设置是否开启 LDAP 攻击防护。开启|关闭，默认值：开启。
leakage <on|off>	设置是否开启 Web 服务器漏洞防护攻击。开启|关闭，默认值：开启。
webshell <on|off>	设置是否开启 webshell 防护。开启|关闭，默认值：关闭。
server <on|off>	设置是否开启 Web 服务器漏洞防护。开启|关闭，默认值：开启。
other <on|off>	设置是否开启其他规则。开启|关闭，默认值：开启。
all <on|off>	设置是否开启所有的防护。开启|关闭，默认值：关闭。

命令示例：

开启“sec01”安全策略中的所有防御模块。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf defence-policy modify security-policy** *sec01* **all** on

waf defence-policy show security-policy <*mstring*>

命令描述：

查看防护策略中的防御模块的开启状态。

命令示例：

查看“sec01”安全策略的防护模块的开启状态。

```
TopsecOS# waf defence-policy show security-policy sec01
Cross Site Script defence:              on
Web Scanner defence:                    on
SQL Injection defence:                  on
OS Command Injection defence:           on
Remote File Inclusion defence:          on
LDAP Inclusion defence:                 on
Directory Traversal defence:            on
Information Leakage defence:            on
XPath Injection defence:                on
SSI Injection defence:                  on
WEB Server Bugs defence:                on
Other Rule defence:                     on
User defined policy defence:            on
Webshell defence:                       on
All defence types above:                on
```

waf defence-policy reset security-policy <*mstring*>

命令描述：

恢复防护策略中的防御模块的开启状态为默认配置。缺省情况下，关闭 webshell 防护功能，其他功能均为开启。

命令示例：

恢复“sec01”安全策略中的防御策略配置为默认配置。

TopsecOS# **waf defence-policy reset security-policy** *sec01*

waf enumeration attack-type <cr>

命令描述：

查看 TopWAF 的支持的攻击防御类型。

命令示例：

TopsecOS# **waf enumeration attack-type**

Attack name: ATTACK_XSS Description: 跨站脚本攻击

Attack name: ATTACK_SCANNER Description: 漏洞扫描攻击

Attack name: ATTACK_SQLI Description: SQL 注入攻击

Attack name: ATTACK_OSI Description: 操作系统命令注入攻击

Attack name: ATTACK_RFI Description: 远程文件包含攻击

Attack name: ATTACK_DIR Description: 路径遍历攻击

Attack name: ATTACK_LEAKAGE Description: 信息泄露攻击

Attack name: ATTACK_LDAP Description: LDAP 注入攻击

Attack name: ATTACK_OTHER Description: 其他攻击

Attack name: ATTACK_XPATH Description: XPath 注入攻击

Attack name: ATTACK_SSI Description: SSI 注入攻击

Attack name: ATTACK_SERVER Description: Web 服务器漏洞攻击

Attack name:	ATTACK_WEBSHELL	Description: Webshell 检测	
Attack name:	ATTACK_USER	Description: 用户自定义规则命中	
Attack name:	ATTACK_ANOMALIES	Description: 协议异常	
Attack name:	ATTACK_VIOLATIONS	Description: 协议违规	
Attack name:	ATTACK_POLICY	Description: 用户策略限制	
Attack name:	ATTACK_ROBOTS	Description: Robots 防护	
Attack name:	ATTACK_CSRF	Description: 跨站请求伪造攻击	
Attack name:	ATTACK_COOKIE	Description: Cookie 篡改攻击	
Attack name:	ATTACK_ANTI_STEALING	Description: URL 盗窃攻击	
Attack name:	ATTACK_ACL	Description: ACL URL 命中	
Attack name:	ATTACK_BRUTE_FORCE	Description: 暴力破解攻击	

5.2.7 防盗链

盗链是指在自己的页面上展示一些并不在自己服务器上的内容。通常的做法是通过技术手段获得他人服务器上的资源地址，绕过别人的资源展示页面，直接在自己的页面上向最终用户提供此内容。比较常见的是一些小网站盗用大网站的资源（图片、音乐、视频、软件等），对于这些小网站来说，通过盗链的方法可以减轻自己服务器的负担，因为真实的空间和流量均是来自别人的服务器，但是这会加重大网站服务器的负担。

防盗链是防止别人通过一些技术手段绕过本站的资源展示页面，盗用本站的资源，让绕开本站资源展示页面的资源链接失效的技术。开启防盗链功能后，因为屏蔽了那些盗链的间接资源请求，从而可以大大减轻服务器及带宽的压力。

- 盗链产生原因

一般浏览器获取完整的页面并不是一次全部从服务器传送到客户端。如果请求的是一个带有许多文字、图片和其它信息的页面，那么最先的一个 HTTP 请求被传送回来的是这个页面的文本。然后通过客户端的浏览器对这段文本的解释执行，发现其中还有指向图片的链接，那么客户端的浏览器会再发送一条 HTTP 请求。当这个请求被处理后图片文件会被传送到客户

端，然后浏览器会将图片安放到页面的正确位置，就这样一个完整的页面也许要经过发送多条 HTTP 请求才能够被完整的显示。

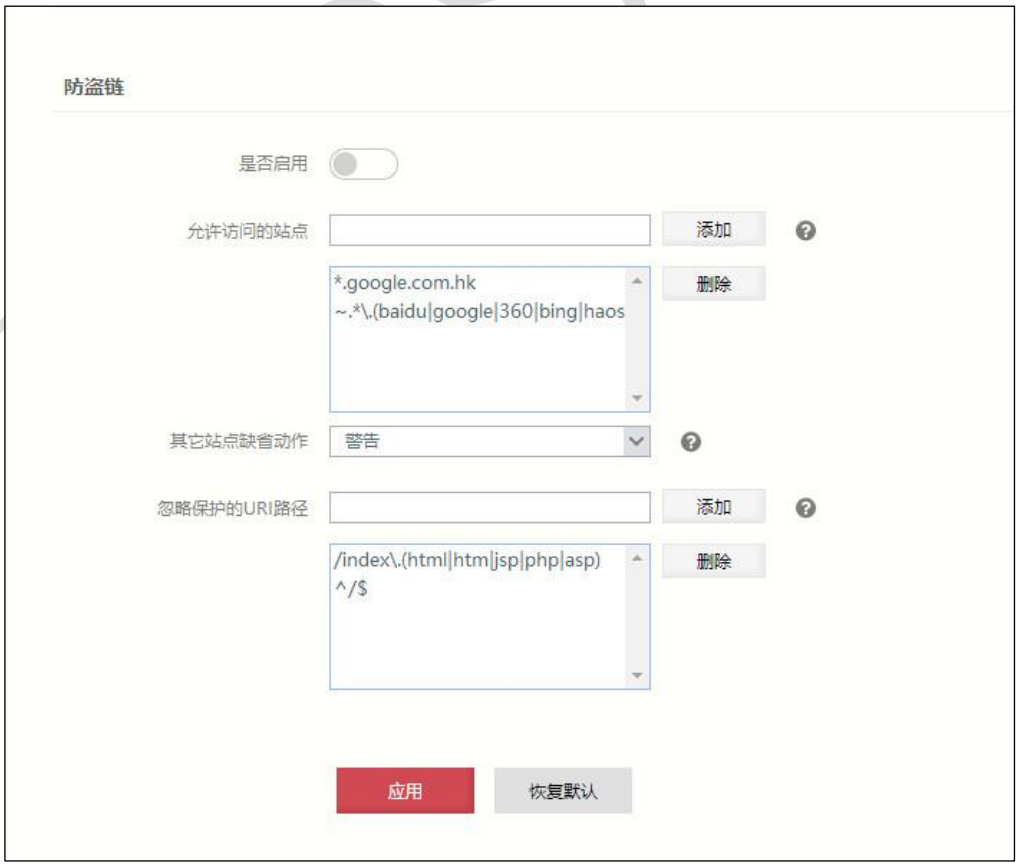
在这个过程中就会产生盗链问题：一个网站中如果没有起始页面中的信息，例如图片信息，但是它将这个资源的地址连接到别的网站，获取到资源。这样没有任何资源的网站盗用了别的网站的资源来展示给浏览者，提高了自己的访问量，而大部分浏览者又不会很容易地发现。

- 防盗链原理

在 HTTP 协议中，有一个请求头部字段叫 Referer，采用 URL 的格式来表示从哪儿链接到当前的网页或文件。即网站通过 Referer 字段可以检测目标网页访问的来源网页，如果是资源文件，则可以跟踪到显示它的网页地址。因此可以通过检测请求报文中的 Referer 字段，判断页面的来源页面是否是本网站，如果来源不是本网站可以进行阻止或者返回指定的页面。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **防盗链**，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置防盗链参数。

在配置防盗链时，各项参数的具体说明如下表所示。

参数	说明
是否启用	设置是否启用防盗链功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
允许访问的站点	添加允许访问的站点 host 地址，TopWAF 将不对该站点进行防盗链防护。点击【添加】按钮，完成添加。站点的 host 地址支持域名和 IP 地址形式，地址格式支持普通形式（可含有通配符“*”），正则表达式形式（以“~”起始的正则表达式字符串）。例如 “www.baidu.com”，表示允许来自百度地址的访问； “*.baidu.com”表示运行来自百度所有域名的访问； https://www.baidu.com 表示只允许来自百度 https 安全站点的访问； “www\.(google|baidu)\.com”，正则表达式形式，表示允许来自 www.google.com 或 www.baidu.com 站点的访问。
其他站点缺省动作	设置除了允许客户端访问的站点外的站点的缺省处理动作。可选项：警告、拒绝、拒绝不记日志、临时跳转、永久跳转和错误页面；默认值：警告。 1）警告：进入下一条访问控制规则，判断对该访问进行的动作，访问记录到攻击日志中。 2）拒绝：拒绝本次访问请求，将访问记录到攻击日志中。 3）拒绝不记日志：拒绝本次访问请求，访问不记录到日志中。 4）临时跳转：由本次请求页面临时跳转到新的页面中，将访问记录到攻击日志中，再次接收到访问请求时，继续访问当前请求页面。 5）永久跳转：由本次请求页面临时跳转到新的页面中，将访问记录到攻击日志中，再次接收到访问请求时，将访问新的页面。 6）错误页面：返回错误页面并记录攻击日志，关于错误页面的配置具体请参见 5.1.7 错误页面。 说明： HTTP 请求报文命中访问控制策略产生的报警和日志信息均显示在攻击日志界面，关于攻击日志的查看具体请参见 4.2.1 日志查看。
跳转 URL/错误页面名称	当“其他站点缺省动作”设置为“临时跳转”、“永久跳转”或“错误页面”时可设置该参数。 1）临时跳转：输入 URL 地址，当客户端访问非允许客户端访问的站点外时，页面将跳转到该地址，仅该次访问进行跳转，后续还将访问原地址。 2）永久跳转：输入 URL 地址，当客户端访问非允许客户端访问的站点时，页面将跳转到该地址。 3）错误页面：通过下拉列表选择已经配置的错误页面，当客户端访问非允许客户端访问的站点时，页面将跳转到该错误页面，关于错误页面的配置具体请参见 5.1.7 错误页面。
忽略保护的 URI 路径	添加忽略保护的 URI 地址，不对该地址进行防盗链保护，该地址为服务器策略保护的的网站根路径下的地址，为正则表达式格式，对

参数	说明
	符合正则表达式规则的多个 URI 地址进行匹配，地址以“/”斜线起始，例如“/index.html”。点击【添加】按钮，完成添加。

步骤4 参数配置完成后，点击【应用】按钮，完成防盗链的配置；点击【恢复默认】按钮恢复出厂配置。

CLI 方式

waf anti-stealing-link add-site security-policy <*string*> **site** <*mstring*>

命令描述：

添加防盗链功能允许客户端访问的站点。

可使用 **waf anti-stealing-link delete-site security-policy** <*string*> **site** <*mstring*>

命令删除防盗链功能允许客户端访问的站点。

可使用 **waf anti-stealing-link modify-site security-policy** <*string*> **site** <*mstring*> 命令修改防盗链功能允许客户端访问的站点。

参数说明：

参数	说明
security-policy <*string*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略名称，支持数字、字母、中文和特殊字符“_-*.”。 注意：不包含“&\"\\'%<>”和空格。
site <*mstring*>	必选项，设置允许客户端访问的站点地址。字符串类型。。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

在“sec01”安全策略中，允许客户端访问/site 站点。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf anti-stealing-link add-site security-policy** *sec01* **site** */site*

waf anti-stealing-link add-skip-path security-policy <*string*> **path** <*mstring*>

命令描述：

添加忽略保护的站点。

可使用 **waf anti-stealing-link delete-skip-path security-policy** <*string*> **path** <*mstring*>命令删除忽略保护的站点。

可使用 **waf anti-stealing-link modify-skip-path security-policy** <*string*> **path** <*mstring*>命令修改忽略保护的站点。

命令示例：

在“sec01”安全策略中，对站点/site 不进行防盗链保护。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf anti-stealing-link add-skip-path security-policy** *sec01* **path** */site*

waf anti-stealing-link modify security-policy <*string*> [**enable** <on|off>] [**action** <alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage|block>] [**action-data** <*mstring*>]

命令描述：

修改防盗链全局设置参数。

参数说明：

参数	说明
security-policy <*string*>	必选项，设置安全策略名称。关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不包含“&\"\\'%<>”和空格。
enable <on|off>	可选项，设置是否启用防盗链功能。开启|关闭
action <alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage|block>	可选项，设置其他站点的防护动作。警告|拒绝|拒绝不记日志|临时跳转|永久跳转|错误页面|锁定，默认值：alert。
action-data <*mstring*>	可选项，设置跳转页面。当“action”设置为“temp-redirect”、“perm-redirect”、“errpage”时设

参数	说明
	置该参数。 1）action 设置为 temp-redirect：输入 URL 地址，当客户端访问非允许客户端访问的站点时，页面将跳转到该地址，仅该次访问进行跳转，后续还将访问原地址。 2）action 设置为 perm-redirect：输入 URL 地址，当客户端访问非允许客户端访问的站点时，页面将跳转到该地址。 3）action 设置为 errpage：通过下拉列表选择已经配置的错误页面，当客户端访问非允许客户端访问的站点时，页面将跳转到该错误页面。

命令示例：

修改“sec01”安全策略中防盗链功能为开启状态，并指定动作为 alert。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf anti-stealing-link modify security-policy** *sec01* **action** alert **enable** on

waf anti-stealing-link show security-policy <*mstring*>

命令描述：

查看防盗链功能的配置信息。

命令示例：

查看“sec01”安全策略中，防盗链功能的配置信息。

TopsecOS# **waf anti-stealing-link show security-policy** *sec01*

Security-Policy Name: sec01

Enabled: on

Action: alert

Action-Data:

Site:

/site

Skip list:

/test

waf anti-stealing-link reset security-policy *<mstring>*

命令描述：

恢复防盗链功能的配置为默认设置。缺省情况下，关闭防盗链保护功能，其他未允许的站点的动作为警告，允许访问的站点为~.*\.(baidu|google|360|bing|haosou|sogou|soso|yahoo|youdao)\.com，*.google.com.hk，忽略保护的 URI 路径为^/$，/index\.(html|htm|jsp|php|asp)。

5.2.8 CSRF 策略

- CSRF 攻击原理

HTTP 协议是无状态系统，为避免用户每次与 Web 网站交互信息均需进行身份认证，HTTP 协议头部定义了承载用户相关信息的 Cookie。Cookie 是 Web 服务器为了辨别用户身份、实现会话跟踪的方式，通常只包含 Web 服务器为了进行跟踪用户而产生的独特识别码。用户首次访问 Web 网站时，Web 服务器对用户赋予独有的 Cookie 并返回给用户，用户浏览器会记录服务器返回的 Cookie 内容，在 Cookie 有效时间内，用户通过该浏览器再次访问 Web 网站，会将 Cookie 及 HTTP 请求内容发送给 Web 服务器，Web 服务器根据 Cookie 验证用户身份及状态，并直接确定用户的授权范围。

因此，Web 服务器通过 Cookie 验证用户身份机制，只能保证一个请求是来自于某个用户的浏览器，但却无法保证该请求是用户授权操作，即在 Cookie 有效时间内，只要用户没有退出已认证的 Web 服务器，攻击者如果迫使用户浏览器向已认证 Web 服务器执行某种操作时，Web 服务器均视为合法，最终可实现在攻击者并没有破解用户账号的情况下对用户账号执行恶意操作。

CSRF（Cross-site request forgery，跨站请求伪造）攻击，指攻击者利用网站对合法用户的网页浏览器的信任，劫持用户当前已登录的 Web 应用程序的会话，迫使用户浏览器将伪造的 HTTP

请求（包括该用户的会话 Cookie 和其他认证信息）发送到已登录的 Web 应用程序，执行非用户本意的操作。CSRF 攻击过程具体如下：

1）用户打开浏览器访问受信任网站 A，输入用户名/密码等信息登录网站 A；

2）用户信息通过验证后，网站 A 生成 Cookie 并发送给用户，用户接收到 Cookie 后保存在浏览器中，此后，用户每次访问网站 A 均携带 Cookie 信息，在 Cookie 有效时间内，用户通过网站 A 执行某种操作无需再次通过账号认证；

3）用户在退出网站 A 之前，使用同一浏览器访问网站 B（网站 B 已被攻击者植入恶意伪造请求代码）；

4）用户触发网站 B 恶意应用程序或链接时，网站 B 向用户返回恶意操作行为请求报文；

5）用户浏览器在接收到恶意请求报文后，根据网站 B 的请求，在用户完全不知情的情况下携带 Cookie 信息，向网站 A 发起请求，而网站 A 并不能识别该请求并非用户授权行为，导致攻击者的任意非法攻击行为可以被执行。

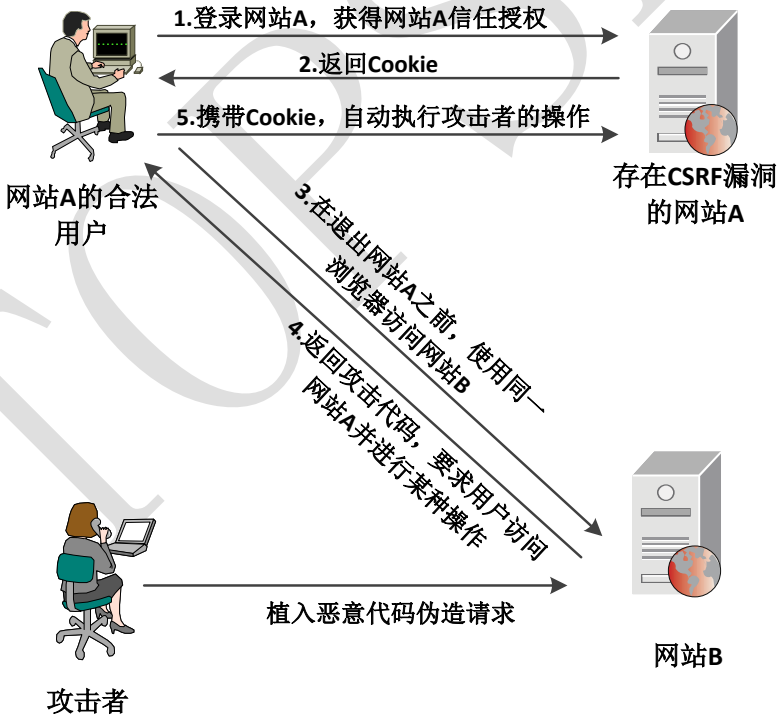


图 5-2 CSRF 攻击流程示意图

- 防御 CSRF 攻击

HTTP 报头中有一个 Referer 字段，Referer 字段记录了 HTTP 请求的来源地址。正常情况下，Web 网站相应页面的 HTTP 请求来自于该页面的上级链接页面，例如，访问网上银行的转账页面，首先必须先登录网银，然后点击页面上相应按钮才进入转账页面。

攻击者如果对网站实施 CSRF 攻击，只能在被其控制的网站构造请求，当用户浏览器通过攻击者的指令自动发送请求到某合法 Web 网站时，HTTP 请求报头的 Referer 字段记录的内容为攻击者所控制网站的 URL，而并非为该合法 Web 网站的 URL。

基于 HTTP 报文的特征和 CSRF 攻击的特点，天融信 TopWAF 通过验证用户 HTTP 请求的 Referer 字段实现对 CSRF 攻击进行抵御。TopWAF 如果发现访问网站的 HTTP 请求的 Referer 字段记录的URL 为非本网站的URL，则判定发送该HTTP 请求的用户可能遭受攻击者的CSRF 攻击，根据 CSRF 策略的动作处理该 HTTP 请求。本节介绍如何配置 CSRF 策略。

✧ 一个安全策略中，最多支持 128 条 CSRF 策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **CSRF 策略**。

步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 点击『添加』，弹出“添加 CSRF 策略”，如下图所示。

在添加 CSRF 防御策略时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置 CSRF 策略的名称。名称只支持数字、字母、中文和特殊字符“-_*.”。
是否启用	设置是否启用 CSRF 策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
URI 路径类型	设置 URI 地址的类型。可选项：普通、正则；默认值：普通。 普通类型 URI 指通过单个字符串来描述一个 URI 路径； 正则类型 URI 指通过单个字符串来描述一系列符合某个语法规则的 URI 路径。
URI 路径	URI 路径类型设置为“普通”时，该参数有效。设置 TopWAF 所保护的网站的地址，格式：以单斜线“/”开头的路径字符串，如 /index.htm。
URI 路径正则	URI 类型设置为“正则”时，该参数有效。使用正则表达式设置 TopWAF 所保护的一系列 Web 网站地址。
请求方法	设置客户端向 Web 服务器获取资源的方式，可选项：GET、POST、全部；默认值：GET。 “GET”用于客户端从服务器获取某个资源； “POST”用于客户端向服务器发送表单数据； “全部”表示包括 GET 和 POST。
Referer 匹配方法	设置 TopWAF 检查用户 HTTP 请求报头的 Referer 字段的方法，可选项：普通、正则；默认值：普通。 “普通”指 CSRF 策略中所配置的“Referer 值”与 HTTP 请求报头中的 Referer 字段值完全相同，HTTP 请求报文才命中该策略； “正则”指 HTTP 请求报头中的 Referer 字段符合“Referer 正则”定义的规则，则 HTTP 请求报文命中该策略。

参数	说明
Referer 值	“Referer 匹配方法”设置为“普通”时，该参数有效。设置 CSRF 策略与 HTTP 请求报头中 Referer 字段进行匹配的基准 Referer 值。
Referer 正则	“Referer 匹配方法”设置为“正则”时，该参数有效。设置 CSRF 策略与 HTTP 请求报头中 Referer 字段进行匹配的基准 Referer 正则表达式。
其他 Referer 的动作	设置 CSRF 策略与 HTTP 请求报头的 Referer 字段值不匹配时，TopWAF 对该 HTTP 请求报文所执行的操作。可选项：警告、拒绝、拒绝不记日志、临时跳转、永久跳转、错误页面；默认值：警告。 1）警告：生成报警信息，并继续匹配后续策略确认是否放行该 HTTP 请求报文。 2）拒绝：拒绝 HTTP 请求报文并记录日志。 3）拒绝不记日志：拒绝 HTTP 请求报文但不记录日志。 4）临时跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，但新的 HTTP 访问请求发起时仍旧访问原网站。 5）永久跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，新的 HTTP 访问请求发起时，直接访问重定向之后的网站。 6）错误页面：返回错误页面并记录攻击日志，关于错误页面的配置具体请参见 5.1.7 错误页面。 说明： HTTP 请求报文命中 CSRF 防护策略产生的报警和日志信息均显示在攻击日志界面，关于攻击日志的查看具体请参见 4.2.1 日志查看。
跳转 URL/错误页面名称	“其他 Referer 的动作”参数设置为临时跳转/永久跳转时，设置重定向的目标 URL 地址，例如 http://www.topsec.com.cn。 “其他 Referer 的动作”参数设置为错误页面时，设置已定义的错误页面，关于错误页面的定义具体请参见 5.1.7 错误页面。
描述	输入对 CSRF 策略进行简单描述的信息。

步骤4 点击【确定】按钮完成 CSRF 策略的添加。

CLI 方式

waf csrf-policy add security-policy <*mstring*> **name** <*mstring*> **enable** <on|off> **type** <normal|regex> **url** <*mstring*> **method** <get|post|get_post> **operater** <equal|match> **referer** <*mstring*> [**action** <alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage|block>] [**action-data** <*mstring*>] [**description** <*mstring*>]

命令描述：

添加 CSRF 防护策略。

可使用 **waf csrf-policy delete security-policy** < *mstring* > **name** < *mstring* >命令删除 CSRF 防护策略。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置待添加 CSRF 防护策略的安全策略。关于安全策略的添加具体请参见 5.2.1 安全策略。字符串类型，表示安全策略的名称。
name <*mstring*>	必选项，设置 CSRF 防护策略的名称。字符串类型。名称只支持数字、字母、中文和特殊字符“-_*.”。
enable <on|off>	必选项，设置是否启用 CSRF 防护策略。是|否
type <normal|regex>	必选项，设置 URL 地址格式类型。普通|正则表达式
url <*mstring*>	必选项，设置 Web 网站 URL 地址，字符串类型。 说明： **type** 参数设置为 normal 时，URL 地址格式：以单斜线“/”开头的路径字符串，如/index.htm； **type** 参数设置为 regex 时，URL 地址格式为正则表达式。
method <get|post|get_post>	必选项，设置客户端向被保护 Web 网站获取资源的方式。GET|POST|全部
operater <equal|match>	必选项，设置 TopWAF 匹配 HTTP 请求报文 Referer 字段的方式。等于|匹配。 “等于”表示 HTTP 请求报文的 Referer 字段的内容与 CSRF 策略所配置的 Referer 参数完全相同，则命中规则； “匹配”表示 HTTP 请求报文的 Referer 字段的内容符合 CSRF 策略所配置的 Referer 参数的正则表达式条件，则命中规则。
referer <*mstring*>	必选项，设置 TopWAF 匹配 HTTP 请求报头 Referer 字段的基准内容，字符串类型。 说明： **operater** 参数设置为 equal 时，配置普通字符串。 **operater** 参数设置为 match 时，配置正则表达式。
action <alert|deny|deny-nlog |temp-redirect|perm-redirect |errpage|block>	可选项，设置 TopWAF 对命中 CSRF 策略的 HTTP 请求报文执行的操作。报警|拒绝|拒绝不记录日志|临时跳转|永久跳转|错误页面|锁定
action-data <*mstring*>	字符串类型。**action** 参数设置为 temp-redirect|perm-redirect|errpage 时，该参数必选。 如果 **action** 参数设置为临时跳转|永久跳转，设置跳转的目的 URL 地址；如果 **action** 参数设置为错误页面，设置已

参数	说明
	定义错误页面的名称，关于错误页面的定义具体请参见 5.1.7 错误页面。
description <*mstring*>	可选项，设置对该 CSRF 策略的简单描述信息，字符串类型。

命令示例：

在“sec01”安全策略中添加名称为 csrf01 的 CSRF 策略，实现将 HTTP 请求报头中 Referer 字段不能与 www.topsec.com.cn 匹配，但请求*/www.topsec.com.cn/fwzc/fwjgjqlxfs/shenyang.htm* 页面的报文丢弃。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf csrf-policy add security-policy** *sec01* **name** *csrf01* **enable** on **type** normal **url** */www.topsec.com.cn/fwzc/fwjgjqlxfs/shenyang.htm* **method** get **operater** match **referer** */www.topsec.com.cn* **action** deny

waf csrf-policy show security-policy <*mstring*> [**name** <*mstring*>]

命令描述：

显示 CSRF 防护策略。

命令示例：

显示“sec01”安全策略中的 CSRF 防护策略。

TopsecOS# **waf csrf-policy show security-policy** *sec01*

name: csrf01

description:

type: normal

method: get

url: /www.topsec.com.cn/fwzc/fwjgjqlxfs/shenyang.htm

```
operater:          match
referer:           /www.topsec.com.cn
action:            deny
action-data:
enable:            on
```

waf csrf-policy clean security-policy *<mstring>*

命令描述：

清空 CSRF 防护策略。

命令示例：

清空“sec01”安全策略中的 CSRF 防护策略。

TopsecOS# **waf csrf-policy clean security-policy** *sec01*

waf csrf-policy reset security-policy *<string>*

命令描述：

重置 CSRF 防护策略。

命令示例：

重置“sec01”安全策略中的 CSRF 防护策略。

TopsecOS# **waf csrf-policy reset security-policy** *sec01*

5.2.9 爬虫防护

- 基本概念

爬虫，又称为 Robots（机器人）、蜘蛛等，为能够全自动探查 Web 事务的软件程序。机器人通过递归地对 Web 网站的各种信息进行遍历，获取其内容，并跟踪 Web 网站链接，对各 Web 网站数据进行处理，实现相应统计功能。目前互联网中网站众多，用户一般会通过搜索引擎实现对网站的搜索，而并非直接输入网站 URL 访问网站，因此搭建的网站如果需在互联网中提升知名度，必须支持搜索引擎等机器人对其进行探查。根据工作目的不同进行划分，机器人具有多种种类，例如：1）搜索引擎机器人，通过在各 Web 上游荡，自动搜集其所获取的所有文档等信息，并创建一个可供搜索的数据库；2）比价购物机器人，从在线购物网站的目录中收集 Web 页面，构建商品及其价格数据库；3）股票图形机器人每隔几分钟周期地向股票市场服务器发送 HTTP GET，以获取股市行情，构建股市价格趋势图。

Robots.txt 文件是每一个机器人探查网站时第一个需寻找和访问的文件，明确禁止或允许特定机器人可以访问哪些 URL 路径，目前几乎所有机器人都遵循 robots.txt 文件规则。机器人访问 Web 网站时，首先检查该站点根目录中是否存在 Robots.txt，如果不存在 Robots.txt 文件，则机器人可访问该 Web 网站的任意内容及链接；否则，机器人则将期望访问的 URL 按照一定的顺序与 robots.txt 文件的规则进行匹配，继而确定其可抓取的页面。

- Robots 攻击

虽然 Robots.txt 文件是国际互联网公认的道德规范，但部分恶意机器人并不遵守该规范，强制对不允许其访问的 Web 网站进行抓取，并通过一定的手段对 Web 网站实施攻击，最终可能对 Web 网站带来严重后果，常见的恶意机器人特点如下：

1）失控机器人

失控恶意机器人通过发送速率过快的 HTTP 请求，消耗 Web 网站大量负载，造成 Web 网站过载，导致 Web 网站不能响应正常机器人及用户的请求。

2）访问失效 URL 机器人

访问失效 URL 恶意机器人通过对大量已被 Web 网站管理员删除的 URL 发起请求，此情况不仅导致 Web 网站的错误日志中充满了机器人对不存在页面的访问请求，还会消耗 Web 网站提供出错页面的开销，降低其数据处理能力。

3）访问错误且超长 URL 的机器人

此类型恶意机器人通过对 Web 网站请求无意义且 URL 地址足够长的页面，此情况将严重降低 Web 网站的性能，使 Web 网站的日志杂乱不堪，甚至可能导致比较脆弱的 Web 网站崩溃。

4）访问隐私数据的机器人

此类型恶意机器人通过 Robots.txt 文件获取 Web 网站不公开的页面的 URL，并对该 URL 内容进行抓取，最终可能导致 Web 网站的隐私数据在互联网中泄露，严重侵犯 Web 网站的隐私权。

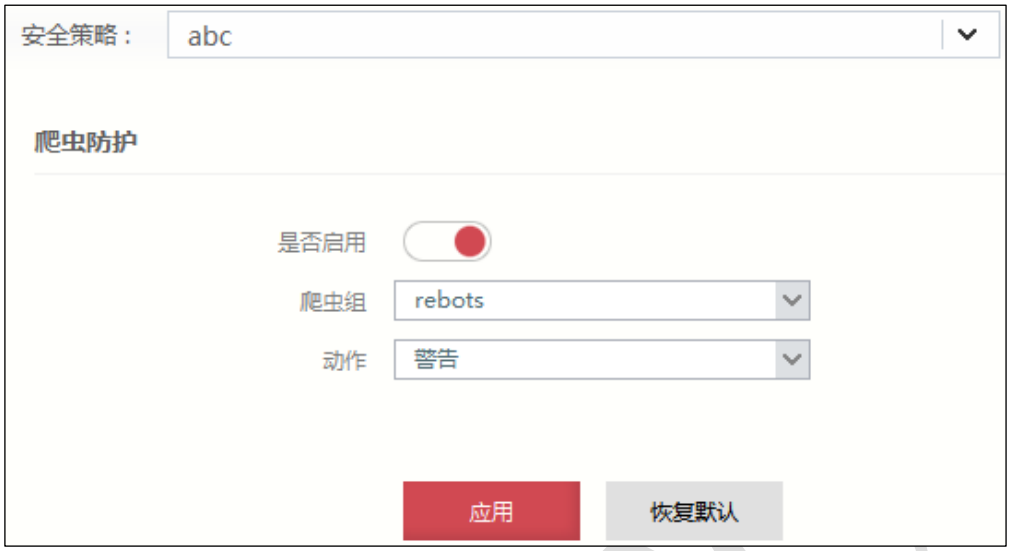
- 爬虫防护

为遏制恶意机器人对 Web 服务器进行攻击，天融信 TopWAF 产品提供了抵御恶意机器人访问其所保护 Web 服务器的爬虫防御功能。由于机器人身份由 HTTP 请求头的 User-Agent 字段标识，爬虫防护模块通过结合爬虫组有针对性地对 HTTP 请求的 User-Agent 字段进行分析，识别通过 TopWAF 访问 Web 服务器的机器人是否为恶意机器人，最终由管理员定义的策略动作决定是否放行相应机器人访问 Web 服务器。关于爬虫组的定义具体请参见 5.1.5 爬虫，本节介绍如何配置爬虫防护策略以保障 Web 服务器免受爬虫攻击。

✧ TopWAF 防护策略的爬虫防护开关处于开启状态，爬虫防护策略才有效，关于爬虫防护开关的开启具体请参见 5.2.6 防护策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **爬虫防护**，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置爬虫防护策略。

在配置爬虫防护策略时，各项参数的具体说明如下表所示。

参数	说明
是否开启	设置是否启用爬虫防护策略。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
爬虫组	选择已定义的爬虫组，或者在下拉列表中点击『新建』创建新的爬虫组，关于爬虫组的定义具体请参见 5.1.5 爬虫。
动作	设置 TopWAF 对 User-Agent 字段命中爬虫组的 HTTP 请求报文执行的操作。可选项：警告、拒绝、拒绝不记日志、临时跳转、永久跳转、错误页面。 1）警告：生成报警信息，并继续匹配后续策略确认是否放行该 HTTP 请求报文。 2）拒绝：拒绝 HTTP 请求报文并记录日志。 3）拒绝不记日志：拒绝 HTTP 请求报文但不记录日志。 4）临时跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，但新的 HTTP 访问请求发起时仍旧访问原网站。 5）永久跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，新的 HTTP 访问请求发起时，直接访问重定向之后的网站。 6）错误页面：返回错误页面并记录攻击日志，关于错误页面的配置具体请参见 5.1.7 错误页面。 说明： HTTP 请求报文命中爬虫防护策略产生的报警和日志信息均显示在攻击日志界面，关于攻击日志的查看具体请参见 4.2.1 日志查看。

参数	说明
跳转 URL/错误页面名称	处理动作设置为“临时跳转”、“永久跳转”、“错误页面”时，该参数有效。 “动作”参数设置为临时跳转/永久跳转时，设置重定向的目标 URL 地址，例如 http://www.topsec.com.cn。 “动作”参数设置为错误页面时，设置已定义的错误页面，关于错误页面的定义具体请参见 5.1.7 错误页面。

步骤4 点击【应用】按钮完成配置；点击【恢复默认】按钮恢复出厂配置。

CLI 方式

waf robots-policy modify security-policy <*mstring*> [**enable** <on|off>] [**robots** <*mstring*>] [**action** <alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage|block>] [**action-data** <*mstring*>]

命令描述：

设置爬虫防护策略。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，指定待设置爬虫防护策略的安全策略，关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略的名称。 注意：不能以“\\”结尾或不包含“<script>”字符串。
enable <on|off>	可选项，设置是否启用爬虫防护策略。是|否
robots <*mstring*>	可选项，绑定爬虫组。关于爬虫组的定义具体请参见 5.1.5 爬虫。字符串类型。表示爬虫组名称。 注意：不能以“\\”结尾或不包含“<script>”字符串。
action <alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage|block>	可选项，设置 TopWAF 对命中爬虫组的机器人执行的操作。报警|拒绝|拒绝不记录日志|临时跳转|永久跳转|错误页面|锁定。
action-data <*mstring*>	动作处理参数。当 **action** 参数设置为 temp-redirect|perm-redirect 时，该参数必选。设置跳转的目标 URL 地址。URL 地址字符串，如 http://www.topsec.com。 当 **action** 参数设置为 errpage 时，用与指定错误页面对象。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

添加一条爬虫规则，实现将搜索引擎 bingbot 和 Yahoo 访问 TopWAF 所保护网站的 HTTP 请求永久重定向到 http://www.topsec.com.cn。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf robots-group add name** *group01* **robots** *bingbot, Yahoo*

TopsecOS# **waf robots-policy modify security-policy** *sec01* **enable** on **robots** *group01* **action** perm-redirect **action-data** *http://www.topsec.com.cn*

waf robots-policy show security-policy <*mstring*>

命令描述：

显示爬虫防护策略。

命令示例：

显示“sec01”安全策略中的爬虫防护策略。

TopsecOS# **waf robots-policy show security-policy** *sec01*

Security-Policy Name: sec01

Enabled: on

Robots-group: group01

Action: perm-redirect

Action-Data: http://www.topsec.com.cn

waf robots-policy reset security-policy <*mstring*>

命令描述：

重置爬虫防护策略。

命令示例：

重置“sec01”安全策略中的爬虫防护策略。

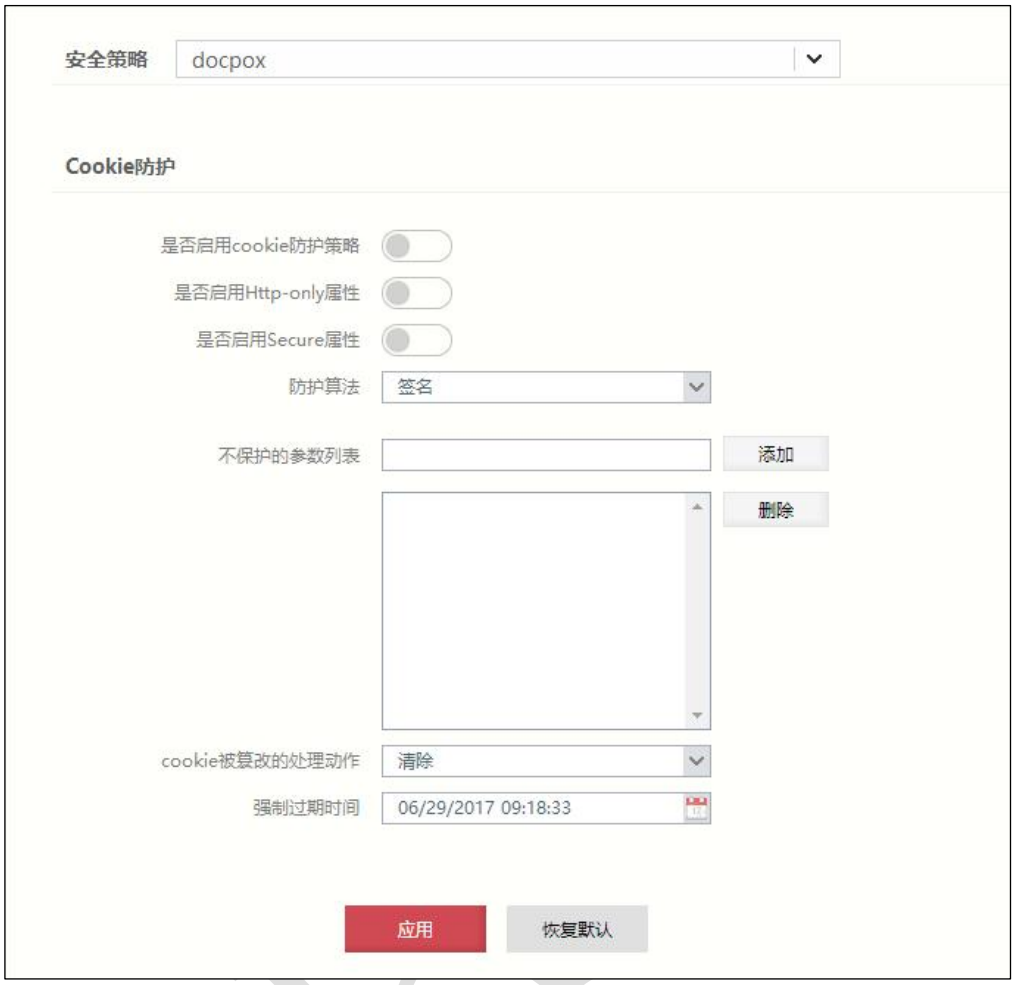
TopsecOS# **waf robots-policy reset security-policy** *sec01*

5.2.10 Cookie 防护

Cookies 最典型的应用是判定注册用户是否已经登录网站，用户可能会得到提示，是否在下一次进入此网站时保留用户信息以便简化登录手续，这些都是 Cookies 的功用。另一个重要应用场合是“购物车”之类处理。用户可能会在一段时间内在同一家网站的不同页面中选择不同的商品，这些信息都会写入 Cookies，以便在最后付款时提取信息。通常网站是用 Cookies 记住和验证用户的身份，若攻击者获取用户的 Cookies，则用户的账号、密码等信息都会被泄露。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **Cookie 防护**，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置 Cookie 防护策略。

在配置 Cookie 防护策略时，各项参数的具体说明如下表所示。

参数	说明
是否启用 cookie 防护策略	设置是否启用 cookie 防护功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。只有启用 cookie 防护策略才能在安全策略中生效。
是否启用 Http-only 属性	设置是否启用 Http-only 防止 cookie 盗用功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
是否启用 Secure 属性	设置是否启用 Cookie 的 Secure 属性。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。当 secure 属性设置为开启时，cookie 只有在 https 协议下才能上传到服务器，而在 http 协议下无法上传，保证安全性。
防护算法	设置 cookie 的加密方式。
不保护的参数列表	设置不保护的参数列表。 在“不保护的参数列表”文本框中输入参数名称或者可匹配参数名称的正则表达式，点击【添加】按钮即可将参数加入到参数列表中。
cookie 被篡改	设置 TopWAF 对命中 Cookie 防护策略的 HTTP 请求报文执行的操

参数	说明
的处理动作	作。可选项：清除、警告、拒绝、拒绝不记日志、临时跳转、永久跳转、错误页面。 1）清除：清除 cookie 文件。 2)警告:生成报警信息,并继续匹配后续策略确认是否放行该 HTTP 请求报文。 3）拒绝：拒绝 HTTP 请求报文并记录日志。 4）拒绝不记日志：拒绝 HTTP 请求报文但不记录日志。 5）临时跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，但新的 HTTP 访问请求发起时仍旧访问原网站。 6）永久跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，新的 HTTP 访问请求发起时，直接访问重定向之后的网站。 7）错误页面：返回错误页面并记录攻击日志，关于错误页面的配置具体请参见 5.1.7 错误页面。 说明： HTTP 请求报文命中 Cookie 防护策略产生的报警和日志信息均显示在攻击日志界面，关于攻击日志的查看具体请参见 4.2.1 日志查看。
跳转 URL	处理动作设置为“临时跳转”、“永久跳转”时，该参数有效。“动作”参数设置为临时跳转/永久跳转时，设置重定向的目标 URL 地址，例如 http://www.topsec.com.cn。
错误页面名称	处理动作设置为 “错误页面”时，该参数有效，设置已定义的错误页面，关于错误页面的定义具体请参见 5.1.7 错误页面。
强制过期时间	设置 Cookie 强制过期的时间。点击“”选择强制过期的截至时间。

步骤4 点击【应用】按钮完成 Cookie 防护策略的配置；点击【恢复默认】按钮恢复出厂配置。

CLI 方式

waf cookie-policy modify security-policy <*string*> **action**

<clear|alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage> **algorithm** <sign> **enable** <on|off>

force-expires <*mstring*> **http-only** <on|off> **secure** <on|off> **skip-arguments** <*mstring*>

action-data <*mstring*>

命令描述：

配置 Cookie 防护策略。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，指定待配置 Cookie 防护策略的安全策略，关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略的名称。 注意：不能以“\\”结尾或不包含“<script>”字符串。
action <clear|alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage|block>	设置 TopWAF 发现 Cookie 被篡改后的处理动作。清除|报警|拒绝|拒绝不记录日志|临时跳转|永久跳转|错误页面|锁定。
algorithm <sign>	防护算法，当前支持加密。
enable <on|off>	可选项，设置是否启用 Cookie 防护策略。开启|关闭
force-expires <*mstring*>	设置 Cookie 强制过期时间，字符串类型，如“2014-08-17 18:10:10”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
http-only <on|off>	是否启用 Http-only 属性，开启|关闭。
secure <on|off>	是否启用 Secure 属性，开启|关闭。
skip-arguments <*mstring*>	设置保护的参数名称，可为普通字符串或正则表达式，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
action-data <*mstring*>	设置发现 Cookie 被篡改后动作处理参数。当 **action** 参数设置为 temp-redirect|perm-redirect 时，该参数必选。设置跳转的目标 URL 地址。URL 地址字符串，如 http://www.topsec.com。 当 **action** 参数设置为 errpage 时，用与指定错误页面对象。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

在安全策略“sec01”中添加 Cookie 防护策略，启用 Http-only 属性。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf cookie-policy modify security-policy** *sec01* **http-only** on

waf cookie-policy show security-policy <*mstring*>

命令描述：

显示 Cookie 防护策略。

命令示例：

显示“sec01”安全策略中的 Cookie 防护策略。

```
TopsecOS# waf cookie-policy show security-policy sec01
Security Name:              sec01
Enable:                     on
Secure Enable:              off
Http-Only Enable:           off
Alogrithm:                  sign
Force Expires:              2017-06-27 09:18:33
Action:                     clear
Action Data:
White argument list:
```

waf cookie-policy reset security-policy *<mstring>*

命令描述：

重置 Cookie 防护策略。

命令示例：

重置“sec01”安全策略中的 Cookie 防护策略。

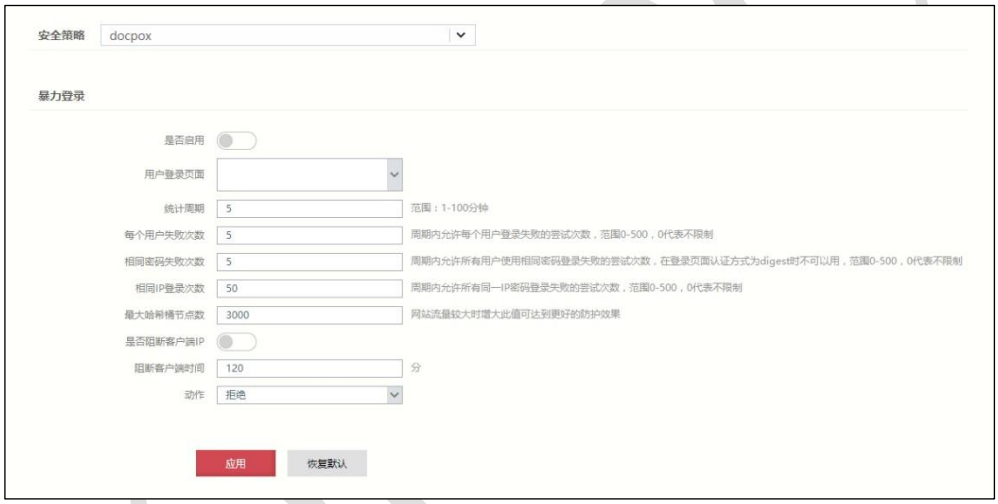
```
TopsecOS# waf cookie-policy reset security-policy sec01
```

5.2.11 暴力登录

所谓暴力登录就是攻击者无限次尝试用户名和密码，试图登录网站。如果不对密码认证失败做次数和时间限制，密码肯定会被尝试出来，极大的增加了网站的风险。为了防止对网站使用尝试猜解用户名和密码的攻击，TopWAF 对暴力登录做了策略限制，用户可以定义统计周期内用户名和密码的失败次数，以限制暴力登录攻击，提高网站的安全性。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **暴力登录**，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置暴力登录策略。

在配置暴力登录策略时，各项参数的具体说明如下表所示。

参数	说明
是否启用	设置是否启用暴力登录防护功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。只有启用暴力登录防护策略才能在安全策略中生效。
用户登录页面	设置用户登录页面。点击【新建】按钮可新建用户登录页面。关于用户登录页面的配置请参见 5.1.9 用户登录页面。
统计周期	设置统计用户登录信息的周期。范围：1-100；单位：分钟。
每个用户失败次数	设置周期内允许每个用户登录失败的尝试次数，范围 0-500，0 代表不限制。
相同密码失败次数	周期内允许所有用户使用相同密码登录失败的尝试次数，在登录页面认证方式为 digest 时不可以用，范围 0-500，0 代表不限制。
相同 IP 登录次	周期内允许所有同一 IP 密码登录失败的尝试次数，范围 0-500，0

参数	说明
数	代表不限制。
最大哈希桶节点数	设置最大哈希桶数。当网站流量较大时增大此值可达到更好的防护效果，范围 1000-20000。
是否阻断客户端 IP	设置是否启用客户端 IP 阻断功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
阻断客户端时间	设置阻断客户端时间，当“是否阻断客户端 IP”开关开启时，该参数生效。单位：分；取值范围：0-1440。
动作	设置 TopWAF 对暴力登录动作执行的操作。可选项：警告、拒绝、拒绝不记日志、临时跳转、永久跳转、错误页面。 1)警告：生成报警信息，并继续匹配后续策略确认是否放行该 HTTP 请求报文。 2）拒绝：拒绝 HTTP 请求报文并记录日志。 3）拒绝不记日志：拒绝 HTTP 请求报文但不记录日志。 4）临时跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，但新的 HTTP 访问请求发起时仍旧访问原网站。 5）永久跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，新的 HTTP 访问请求发起时，直接访问重定向之后的网站。 6）错误页面：返回错误页面并记录攻击日志，关于错误页面的配置具体请参见 5.1.7 错误页面。 说明： HTTP 请求报文命中暴力登录防护策略产生的报警和日志信息均显示在攻击日志界面，关于攻击日志的查看具体请参见 4.2.1 日志查看。
跳转 URL	处理动作设置为“临时跳转”、“永久跳转”时，该参数有效。“动作”参数设置为临时跳转/永久跳转时，设置重定向的目标 URL 地址，例如 http://www.topsec.com.cn。
错误页面名称	处理动作设置为 “错误页面”时，该参数有效，设置已定义的错误页面，关于错误页面的定义具体请参见 5.1.7 错误页面。

步骤4 点击【应用】按钮完成暴力登录策略的配置；点击【恢复默认】按钮恢复出厂配置。

CLI 方式

waf brute-force modify security-policy <*mstring*> **action**

<|alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage> **action-data** <*mstring*> **block-client-ip**

<on|off> **enable** <on|off> **login-page** <*mstring*> **max-bucket-size** <*num*> **max-ip-attempt** <*num*>

max-user-attempt <*num*> **period** <*num*> **block-period** <*num*> **max-password-attempt** <num>

命令描述：

配置暴力登录策略。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，指定待配置暴力登录策略的安全策略，关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略的名称。 注意：不能以“\\”结尾或不包含“<script>”字符串。
action < clear|alert|deny|deny-nlog| temp-redirect|perm-redirect| errpage|block>	设置 TopWAF 发现暴力登录后的处理动作。|报警|拒绝|拒绝不记录日志|临时跳转|永久跳转|错误页面|锁定。
action-data <*mstring*>	设置发现暴力登录后动作处理参数。当 **action** 参数设置为 temp-redirect|perm-redirect 时，该参数必选。设置跳转的目标 URL 地址。URL 地址字符串，如 http://www.topsec.com。 当 **action** 参数设置为 errpage 时，用与指定错误页面对象。 注意：不能以“\\”结尾或不包含“<script>”字符串。
block-client-ip <on|off>	设置是否锁定客户端 IP，开启|关闭。
enable <on|off>	可选项，设置是否启用暴力登录防护策略。开启|关闭
login-page <*mstring*>	设置用户登录页面名称，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
max-bucket-size <*num*>	设置跟踪记录的桶大小，数值类型。范围 1000-20000，默认 3000。
max-ip-attempt <*num*>	设置相同 IP 登录次数次数，数值类型。范围 0-500，0 代表禁用该项检查。
max-password-attempt <num>	设置相同 IP 登录次数次数，数值类型。范围 0-500，0 代表禁用该项检查。
max-user-attempt <*num*>	设置周期内每个用户登录失败尝试次数，数值类型。范围 0-500，0 代表禁用该项检查。
period <*num*>	设置统计周期，数值类型。单位：分钟；范围 1-100。
block-period <*num*>	设置阻断客户端时间周期，当 **block-client-ip** 设置为 on 时，该参数生效。数值类型。范围 0-1440，单位：分钟；0 代表永阻断。

命令示例：

在安全策略“sec01”中添加暴力登录策略，设定开启锁定客户端 IP。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf brute-force modify security-policy** *sec01* **block-client-ip** on

waf brute-force show security-policy <*mstring*>

命令描述：

显示暴力登录策略。

命令示例：

显示“sec01”安全策略中的暴力登录策略。

TopsecOS# **waf brute-force show security-policy** *sec01*

enable: off

period: 5

max-user-attempt: 5

max-password-attempt: 5

max-ip-attempt: 50

max-bucket-size: 3000

login-page:

action: deny

action_data:

block-client-ip: off

block-period: 120

waf brute-force reset security-policy <*mstring*>

命令描述：

重置暴力登录策略。

命令示例：

重置“sec01”安全策略中的暴力登录策略。

TopsecOS# **waf brute-force reset security-policy** *sec01*

5.2.12 自学习

如果服务器策略的自学习功能处于启用状态（关于自学习功能的启用具体请参见 5.3 服务器策略），天融信 TopWAF 则会对客户端与 Web 网站间交互的 HTTP 数据报文进行智能分析，学习 Web 网站支持的参数的长度、类型、隐藏、只读属性、请求方法等信息，并生成学习报告（关于自学习报告的查看具体请参见 5.4 自学习报告），最后自学习结果自动生成参数防护规则（关于参数防护规则的查看具体请参见 5.2.5URI 例外），实现 TopWAF 动态智能适应当前网络环境，精确规范用户在 Web 网站中提交信息的行为，保证 Web 服务器安全。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **自学习**，如下图所示。

步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置自学习策略。

在配置自学习策略时，各项参数的具体说明如下表所示。

参数	说明
不学习的参数	设置忽略学习的参数列表。 在“不学习的参数”文本框中输入参数名称或者可匹配参数名称的正则表达式，点击【添加】按钮即可将参数加入到参数列表中。
自学习阀值	设置参数学习匹配百分比，经过学习阶段后，超过此百分比的参数和方法才作为学习的结果。单位：%；取值范围：1-100。
自学习天数	设置自学习结果自动生成参数防护规则生效的时间。单位：天。

步骤4 点击【应用】按钮完成自学习策略的配置；点击【恢复默认】按钮恢复出厂配置。

CLI 方式

waf autolearn modify security-policy <*mstring*> [**skip-args** <*mstring*>] [**percent** <*num*>] [**days** <*num*>]

命令描述：

配置自学习策略。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，指定待配置自学习策略的安全策略，关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略的名称。 注意：不能以“\\”结尾或不包含“<script>”字符串。
skip-args <*mstring*>	可选项，设置不学习的参数名称，可为普通字符串或正则表达式，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
percent <*num*>	可选项，设置参数学习匹配百分比，经过学习阶段后，超过此百分比的参数和方法才作为学习的结果。单位：%；取值范围：1-100，数值类型。
days <*num*>	可选项，设置自学习结果转换为 URL 例外参数策略的时间。数值类型。单位：天。

命令示例：

在安全策略“sec01”中添加自学习策略，设定 TopWAF 对服务器与客户端交互的所有信息进行学习，且参数学习百分比大于 80%才作为自学习结果。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf autolearn modify security-policy** *sec01* **percent** *80*

waf autolearn show security-policy <*mstring*>

命令描述：

显示自学习策略。

命令示例：

显示“sec01”安全策略中的自学习策略。

TopsecOS# **waf autolearn show security-policy** *sec01*

Security-policy Name : sec01

Skip Arguments:

Percent: 80

```
Deep Autolearn Enabled:    off
```

waf autolearn reset security-policy *<mstring>*

命令描述：

重置自学习策略。

命令示例：

重置“sec01”安全策略中的自学习策略。

TopsecOS# **waf autolearn reset security-policy** *sec01*

5.2.13 规则库

TopWAF 提供两种规则库，一种是系统预定义规则库，另一种是管理员自定义规则库。关于自定义规则库的配置具体请参见 5.2.14 自定义策略。其中，天融信 TopWAF 预定义规则库分为应用规则库和核心规则库两种，共包含 16 大类上千种规则。

核心规则包含了对常见攻击的防护规则，这些攻击在多种语言、多种系统中普遍存在，往往不针对特定语言、特定服务器等，覆盖面较大。而这部分规则库涵盖了大部分这些攻击特征的防护，经过不断锤炼，生成了一些具有通用广泛适用特性的规则，就是核心规则。应用规则包含了一些特定 CMS 存在的攻击特征，如针对 phpwind、wordpress、discuzd 等攻击防护规则。

针对黑客攻击手段复杂多变的网络环境，天融信攻防实验室专家常年专注勘察网络攻击行为，一旦发现新的异常攻击行为，立刻研究如何抵御最新攻击，并更新 TopWAF 规则库。为及时抵御最新的攻击手段，保障用户网站的安全，管理员需及时升级最新规则库。关于规则库升级的操作具体请参见 8.2.5 规则库升级。TopWAF 将核心规则和应用规则分开显示，操作方

式类似，下面以核心规则库为例介绍如何查看预定义规则库，以及应用预定义规则库到安全策略中。

✧ TopWAF 防护策略相应攻击类型检测开关处于开启状态，规则库中的相应攻击类型规则才有效，关于防护策略攻击类型检测开关的开启具体请参见 5.2.6 防护策略。

步骤1 选择 **Web 防护** > **安全策略** > **规则库**，激活“核心规则”页签。

步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 查看/搜索规则库。

1）查看规则库。规则库界面如下图所示。

在查看核心规则库时，各项参数的具体说明如下表所示。

参数	说明
攻击类型	显示规则库中攻击类型名称。
ID	显示规则的 ID。
规则名称	显示规则名称。
严重程度	显示规则库所抵御的攻击的严重程度，包括：高、中、低。
精准度	显示该规则的精准度，表示该规则的正确率，精准度越高越不容易出现误报。包括：高、中、低。
动作	显示 TopWAF 对命中规则的 HTTP 数据报文所执行的操作，包括：继续、允许、警告、丢弃、阻断、阻断不记日志、临时跳转、永久跳转。
启用状态	显示规则库是否处于启用状态，“”表示启用，“”表示关闭。
操作	修改规则库描述信息、启用状态以及动作的图标。

2）查询规则库。在“全部”下拉列表中选择攻击类型，并在搜索文本框中输入关键字，点击搜索图标“”，规则库中规则的攻击类型匹配即可被筛选出来。如下图所示。

3）规则库排序。点击规则列表的“攻击类型”、“ID”、“规则名称”、“严重程度”、“精准度”、“动作”、“启用状态”，即可根据该栏的内容进行排列。

步骤4 修改规则。

1）双击规则列表，或单击规则“操作”栏的修改图标“”，弹出“编辑动作策略”窗口，如下图所示。

在修改规则时，各项参数的具体说明如下表所示。

参数	说明
ID	显示规则的 ID。
规则名称	显示规则的名称。
是否启用	设置是否启用规则。 “”表示开启状态，“”表示关闭状态，点击开关图标，可切换规则的状态。
精准度	显示规则的精准度。
规则描述	显示规则的详细描述信息。
动作	设置 TopWAF 对命中该规则的 HTTP 数据报文执行的操作，可选项：继续、允许、警告、丢弃、阻断、阻断不记日志、临时跳转、永久跳转。

参数	说明
	继续：继续匹配下一条规则，但不记录日志； 允许：允许通过 TopWAF，忽略所有规则； 警告：生成报警信息，并继续匹配下一条规则； 丢弃：丢弃数据包； 拒绝：拒绝 HTTP 请求报文并记录日志； 拒绝不记录日志：拒绝 HTTP 请求报文但不记录日志； 临时跳转：重定向并记录日志，表示将 HTTP 访问请求重定向到其它特定网站，但新的 HTTP 访问请求发起时仍旧访问原网站； 永久跳转：重定向并记录日志，表示将的 HTTP 访问请求重定向到其它特定网站，新的 HTTP 访问请求发起时，直接访问重定向之后的网站。 说明： HTTP 请求报文命中规则库产生的报警和日志信息均显示在攻击日志界面，关于攻击日志的查看具体请参见 4.2.1 日志查看。

2）参数设置完成后，点击【确定】按钮完成规则的修改。

步骤5 启用/禁用规则。点击规则启用状态栏的“”/“”按钮即可启用/禁用规则。

5.2.14 自定义策略

在整个 Web 网站运行过程中，一旦发现防护规则并未成功抵御某些恶性行为，管理员可以根据日志信息创建对应的自定义防护策略，此外，TopWAF 还支持根据漏洞扫描报告直接生成防护策略，有针对的抵御恶性行为，实现较为全面的防护，保证 Web 网站高效、可靠的运行。

5.2.14.1 自定义防护策略

TopWAF 支持管理员制定强大的自定义防护策略，自定义策略涵盖对 HTTP 报文的各部分内容特征进行灵活精准匹配的条件，管理员一旦掌握恶意行为的特征，即可配置抵御该恶意行为的规则。

为提高自定义策略匹配 HTTP 数据报文的效率，TopWAF 为管理员提供根据报文特征处于 HTTP 报文中的大致位置（请求头、请求体、应答头、应答体）制定规则的平台。管理员可在 TopWAF 中制定大量自定义策略，一条自定义策略可有多条规则条件组成，自定义策略中各规则条件间的关系为逻辑“与”，即 HTTP 数据报文满足某条自定义策略的所有条件才命中该自定义策略。本节介绍如何配置自定义策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **自定义策略**，激活“自定义防护策略”页签。

步骤2 从“安全策略”下拉列表中选择需要配置的安全策略，（系统预定义的“安全优先”、“标准策略”、“应用优先”不允许用户配置）。

步骤3 配置自定义防护策略基本信息。点击『添加』，弹出“添加自定义策略”窗口，如下图所示。

在配置自定义策略基本信息时，各项参数的具体说明如下表所示。

参数	说明
规则名称	必选项，设置标识该自定义策略的名称。名称只支持数字、字母、中文和特殊字符“-_*.”。
是否启用	设置是否启用策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
处理阶段	指定 HTTP 报文特征字段所处的位置，可选项：请求头、请求体、应答头、应答体。 自定义策略匹配 HTTP 报文时，TopWAF 根据策略的“处理阶段”只对 HTTP 报文的请求头/请求体/应答头/应答体进行匹配处理。
动作	设置 TopWAF 对命中策略的 HTTP 报文执行的动作，可选项：继续、允许、警告、拒绝、拒绝不记日志、临时跳转、永久跳转、错误页面。 1）继续：进入下一条访问控制规则，判断对该访问进行的动作，访问不记录到攻击日志中。 2）允许：允许本次访问请求，忽略后续的所有的规则，并将访问记录到攻击日志中。 3）警告：进入下一条访问控制规则，判断对该访问进行的动作，访问记录到攻击日志中。

参数	说明
	4）拒绝：拒绝本次访问请求，将访问记录到攻击日志中。 5）拒绝不记日志：拒绝本次访问请求，访问不记录到日志中。 6）临时跳转：由本次请求页面临时跳转到新的页面中，将访问记录到攻击日志中，再次接收到访问请求时，继续访问当前请求页面。 7）永久跳转：由本次请求页面临时跳转到新的页面中，将访问记录到攻击日志中，再次接收到访问请求时，将访问新的页面。 8）错误页面：由本次请求页面临时跳转到错误页面。
跳转 URL/错误页面名称	“动作”参数设置为临时跳转/永久跳转时，指定跳转的目标地址。 “动作”参数设置为错误页面时，选择已定义的错误页面，关于错误页面的定义具体请参见 5.1.7 错误页面。
日志信息	设置 HTTP 报文命中策略时 TopWAF 记录的日志内容。

步骤4 配置自定义策略条件。点击『添加』，展开条件设置界面，如下图所示。

在配置自定义策略条件时，各项参数的具体说明如下表所示。

参数	说明
变量	设置 HTTP 报文特征所处的变量字段，即 TopWAF 匹配 HTTP 报文的字段，此变量参数与该策略基本信息的“处理阶段”参数有关。 1）自定义策略的“处理阶段”参数设置为“请求头”/“请求体”时，

参数	说明
	支持的变量名称及其说明如下： ARGS：HTTP 请求中 GET/PUT 方法中的参数； ARG_COUNT：表单中的参数个数； GET_ARGS：GET 请求方法中的参数； ARGS_NAMES：参数对 name=value 中的 name 字段字符串，类此于 ARGS 之后跟随的值； POST_ARGS：POST 请求中的参数； POST_ARG_NAMES：仅仅适用于 POST 请求中的 ARGS_NAMES； GET_ARG_NAMES：仅仅适用于 GET 请求中的 ARGS_NAMES； FILES：POST 请求中，文件上传的文件名集合； FILES_SIZE_COMBIND：截取或者拦截的所有上传文件的总大小； FILES_SIZES：截取或者拦截的上传文件大小； UPLOAD_FILENAME：截取或者拦截的上传文件名； REQUEST_QUERY_STR：获取当前输入的 md5 哈希值总和； CLIENT_ADDRESS：客户端 IP； CLIENT_HOST：客户端 HOST； CLIENT_PORT：客户端端口； CLIENT_USER：登陆服务器的用户名； REQUEST_BODY：请求体； REQUEST_BODY_LENGTH：请求体长度； REQUEST_COOKIES：请求中的 COOKIE 数据； REQUEST_COOKIES_COUNT：请求中的 COOKIE 数量； REQUEST_COOKIES_NAMES：请求中 Cookie 中 name=value 中的 name 值； REQUEST_FILENAME：请求中的文件资源名； REQUEST_HEADERS：请求头； REQUEST_HEADERS_NAMES：请求头名称； REQUEST_LINE：请求行，例如 GET / HTTP/1.1； REQUEST_PROTOCOL：HTTP 协议号； REQUEST_URL：请求 URI； REQUEST_URI_RAW：包含域名的请求 URI； INPUT_BODY：请求中当前报文中的原始数据包； OUTPUT_BODY：响应中当前报文中的原始数据包； TX_STORE：交易记录集合； USER_ID：通过 setuid 设置的用户 ID； USERAGENT_IP：用户代理 IP； XML：XML。 2）自定义策略的“处理阶段”参数设置为“应答头”时，支持的变量名称及其说明如下： RESPONSE_CONTENT_LENGTH：响应体长度； RESPONSE_HEADERS：响应头； RESPONSE_HEADERS_NAMES：响应头名称； SERVER_IP：服务器 IP；

参数	说明
	SERVER_NAME：服务器名； SERVER_PORT：服务器端口； OUTPUT_BODY：响应中当前报文中的原始数据包； TX_STORE：交易记录集合； USER_ID：通过 setuid 设置的用户 ID； USERAGENT_IP：用户代理 IP； XML：XML。 3）自定义策略的“处理阶段”参数设置为“应答体”时，支持的变量名称及其说明如下： RESPONSE_BODY：响应体； RESPONSE_CONTENT_LENGTH：响应体长度； RESPONSE_HEADERS：响应头； RESPONSE_HEADERS_NAMES：响应头名称； SERVER_IP：服务器 IP； SERVER_NAME：服务器名； SERVER_PORT：服务器端口； OUTPUT_BODY：响应中当前报文中的原始数据包； TX_STORE：交易记录集合； USER_ID：通过 setuid 设置的用户 ID； USERAGENT_IP：用户代理 IP； XML：XML。
操作	设置 TopWAF 对 HTTP 报文相应变量与策略配置的表达式进行匹配的方法。 可选项：匹配、不匹配、起始于、不起始于、包含、不包含、包含词、不包含词、检测 SQLi、结束于、不结束于、等于、不等于、大于、大于等于、小于等于、小于、AC 匹配、字符串等于、字符串不等于、字符串匹配、字符串不匹配、长度范围、XML_DTD 验证、XML_Schema 验证、URL 编码验证、Utf8 编码验证、信用卡好验证、社保号验证、在集合内、不在集合内。
匹配表达式	设置 TopWAF 匹配 HTTP 报文的基准内容，该内容采用正则表达式表示。
转换函数	转换函数将 HTTP 报文的“变量”指定的信息经过相关函数转换，之后再和自定义策略的“表达式”进行匹配。例如 TopWAF 对接收到的 HTTP 请求报文的关键字段进行 lowercase 小写转换，之后再跟“表达式”比较，判断该报文是否命中规则。 DecodeBase64：使用 base64 对请求中的串解码； DecodeSqlHex：对 sql 中的 16 进制数进行解码； DecodeBase64Ext：类似 decodeBase64，但是会忽略无效字符； EncodeBase64：使用 base64 对请求中的串编码； compressWhitespace：将 tab 键、换行符转为空白字符，将多余的空格转为单一的空白字符； DecodeCss：对 CSS 样式编码字符的解码； DecodeEscapeSeq：对 ANSI 转义字符的解码；

参数	说明
	DecodeHex：对字符串使用 16 进制解码； EncodeHex：对字符串使用 16 进制编码； DecodeHtmlEntity：对 html 实体编码进行解码； DecodeJs：对 js 代码中的转义字符串进行解码； length：获取一个字符串的长度； tolower：获取字符串的所有小写表现方式； md5：获取当前输入的 md5 哈希值总和； none：移除当前规则的所有转换函数； regularPath：将路径的多个正斜杠替换为单一正斜杠并删除目录自引用； regularPathWin：当运行在 windows 平台时，替换反斜杠为正斜杠，其他同 normalistPath； parityEven7bit：计算前七个比特位的偶奇偶校验位并赋值给第 8 个比特位； parityOdd7bit：计算前七个比特位的奇奇偶校验位并赋值给第 8 个比特位； parityZero7bit：0 奇偶校验； removeNUlls：移除所有的 NULL 字符； removeWhitespace：移除字符串中的所有空白字符； replaceComments：将 C 语言注释替换为单一的空格字符，开放的/*（没有以*/结尾）也替换为空格字符； removeCommentsChar：移除通用注释字符（/*,*/,--,#）； removeComments：移除通用注释的所有匹配串，不仅仅是注释字符(/*…*/,--,#) ； replaceNulls：将 NULL 字符替换为空格； DecodeUrl：对 URL 编码字符进行解码； DecodeUrlUni：除了 urlDecode 操作外，还对 unicode 编码字符进行解码； EncodeUrl：对字符串进行 URL 编码格式的编码； utf8toUnicode：将 UTF8 编码转换成 Unicode 编码。 sha1：获取当前输入的 SHA1 哈希值总和； leftTrim：移除字符串开始的所有空白字符； rgithTrim：移除字符串结尾的所有空白字符； trim：移除字符串首部以及尾部的空白字符。

步骤5 条件设置完成后，点击【保存】按钮即可将该设置的条件添加到自定义策略中，再次点击『添加』，可为该策略添加新条件。

步骤6 策略所有条件设置完成后，点击【确定】按钮完成自定义策略的配置。

CLI 方式

waf user-policy add security-policy <*mstring*> **name** <*mstring*> [**enable** <on|off>] [**phase** <request_header|request_body|response_header|response_body>] [**action** <continue|allow|alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage|block>] [**action-data** <*mstring*>] [**log-message** <*mstring*>] [**variables** <*mstring*>] [**operator** <*mstring*>] [**expression** <*mstring*>] [**trfns** <*mstring*>]

命令描述：

添加自定义规则。

可使用 **waf user-policy delete security-policy** <*mstring*> **name** <*mstring*>命令删除。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，设置待添加自定义规则的安全策略，关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略的名称。 注意：不能以“\\”结尾或不包含“<script>”字符串。
name <*mstring*>	必选项，设置规则名称，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
enable <on|off>	可选项，设置是否启用规则，是|否。
phase <request_header|request_body|response_header|response_body>	可选项，设置规则特征处于 HTTP 报文的字段位置。请求头|请求体|应答头|应答体，默认值：请求头。
action <continue|allow|alert|deny|deny-nlog|temp-redirect|perm-redirect|errpage|block>	可选项，设置 TopWAF 对命中该自定义规则的 HTTP 报文执行的操作。继续|报警|拒绝|拒绝不记录日志|临时跳转|永久跳转|错误页面|阻断 IP。
action-data <*mstring*>	**action** 参数设置为 temp-redirect|perm-redirect|errpage 时，该参数必选。 如果 **action** 参数设置为临时跳转|永久跳转，设置跳转页面的目标 URL 地址； 如果 **action** 参数设置为错误页面，设置错误页面的名称，关于错误页面的定义具体请参见 5.1.7 错误页面，字符串类型。

参数	说明
	注意：不能以“\\”结尾或不包含“<script>”字符串。
log-message <*mstring*>	可选项，设置自定义规则命中 HTTP 报文提示的日志信息，字符串类型，默认值：user-defined policy log message。 注意：不能以“\\”结尾或不包含“<script>”字符串。
variables <*mstring*>	可选项，设置 TopWAF 匹配 HTTP 报文的具体变量，此变量参数与该策略的“处理阶段”有关。TopWAF 支持的变量具体请通过 **waf enumeration variables** [**phase** <request_header|request_body|response_header|response_body>]命令查询，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
operator <*mstring*>	可选项，设置 TopWAF 对 HTTP 报文进行策略匹配的方法。TopWAF 支持的规则匹配方法具体请通过 **waf enumeration operators** <cr>命令查询，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
expression <*mstring*>	可选项，设置自定义规则匹配 HTTP 报文的基准内容，该内容采用正则表达式表示，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
trfns <*mstring*>	可选项，转换函数对 HTTP 报文中的某些指定的变量内容进行适当的处理，字符串类型。TopWAF 将处理过后的 HTTP 报文与自定义规则的规则变量进行匹配。TopWAF 支持的转换函数具体请通过 **waf enumeration translate-functions** <cr>命令查询。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

在安全策略“sec01”中添加一条自定义规则“rule01”，实现 TopWAF 一旦发现 HTTP 报文请求头命中规则拒绝该 HTTP 请求。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf user-policy add security-policy** *sec01* **name** *rule01* **enable** on **phase** request_header **action** deny

waf user-policy add-condition security-policy <*mstring*> **name** <*mstring*> [**variables** <*mstring*>] [**operator** <*mstring*>] [**expression** <*mstring*>] [**trfns** <*mstring*>]

命令描述：

添加自定义规则的条件。

可使用 **waf user-policy delete-condition security-policy** <*mstring*> **name** <*mstring*> **condition-index** <*num*>命令删除，其中 **condition-index** 表示条件序列号，可通过 **waf user-policy show security-policy** <*mstring*> [**name** <*mstring*>]查看。

命令示例：

在安全策略“sec01”的自定义规则“rule1”中添加条件，规则条件为：移除用户登录服务器的用户名开始的所有空白字符，再与 xxx 进行匹配。

TopsecOS# **waf user-policy add-condition security-policy** *sec01* **name** *rule01* **variables** client_user **operator** eq **expression** *xxx* **trfns** lefttrim

waf user-policy show security-policy <*mstring*> [**name** <*mstring*>]

命令描述：

显示自定义规则。

命令示例：

显示安全策略“sec01”中的所有自定义规则。

TopsecOS# **waf user-policy show security-policy** *sec01*

RuleID: 8336

User Policy Name: rule01

Action: deny

Phase: request_header

Enable: on

log-message: user-defined policy log message

Rules:

waf user-policy clean security-policy <*mstring*>

命令描述：

清空自定义规则。

命令示例：

清空“sec01”安全策略中的所有自定义规则。

TopsecOS# **waf user-policy clean security-policy** *sec01*

waf user-policy clean-condition security-policy <*mstring*> **name** <*mstring*>

命令描述：

清除自定义规则的条件。

命令示例：

清除安全策略“sec01”中自定义规则名称为“rule01”的所有条件。

TopsecOS# **waf user-policy clean-condition security-policy** *sec01* **name** *rule01*

waf enumeration operators <cr>

命令描述：

该命令显示 TopWAF 支持的所有内置操作，具体如下：

操作名称	说明	操作名称	说明
match	匹配	mp	AC 匹配
notMatch	不匹配	strEqual	字符串等于
beginsWith	起始于	strNotEqual	字符串不等于
notBeginsWith	不起始于	strMatch	字符串匹配
contains	包含	strNotMatch	字符串不匹配

notContains	不包含	checkByteRange	长度范围
containsWord	包含词	checkDTD	XML_DTD 验证
notContainsWord	不包含词	checkSchema	XML_Schema 验证
detectSQLi	检测 SQLi	heckUrlEncoding	URL 编码验证
endsWith	结束于	checkUtf8Encoding	Utf8 编码验证
notEndsWith	不结束于	checkCC	信用卡号验证
eq	等于	checkSSN	社保号验证
neq	不等于	within	在集合内
gt	大于	notWithin	不在集合内
ge	大于等于	ipMatch	ip 匹配
le	小于等于	ipUnMatch	ip 不匹配
lt	小于		

命令示例：

TopsecOS# **waf enumeration operators**

name: match cn_name: 匹配 take_args: 1

name: notMatch cn_name: 不匹配 take_args: 1

name: beginsWith cn_name: 起始于 take_args: 1

name: notBeginsWith cn_name: 不起始于 take_args: 1

name: contains cn_name: 包含 take_args: 1

……

waf enumeration variables [phase

<request_header|request_body|response_header|response_body>]

命令描述：

该命令显示 TopWAF 支持的所有 HTTP 报文变量，HTTP 请求头、请求体、应答头、应答体的变量如下表所示。

request_header	request_body	response_header	response_body
args	args	response_content_length	response_body
arg_count	arg_count	response_headers	response_content_length
get_args	get_args	response_headers_names	response_headers

args_names	args_names	server_ip	response_headers_names
post_args	post_args	server_name	server_ip
get_arg_names	post_arg_names	server_port	server_name
request_query_str	get_arg_names	useragent_ip	server_port
client_ip	files	xml	output_body
client_host	files_size_combind	/	tx_store
client_port	files_sizes	/	user_id
client_user	upload_filename	/	useragent_ip
request_Cookies	request_query_str	/	xml
request_Cookies_count	client_ip	/	/
request_Cookies_names	client_host	/	/
request_filename	client_port	/	/
request_headers	client_user	/	/
request_headers_names	request_body	/	/
request_line	request_body_length	/	/
request_protocol	request_filename	/	/
request_url	input_body	/	/
request_uri_raw	useragent_ip	/	/
useragent_ip	xml	/	/
xml		/	/

命令示例：

显示 TopWAF 支持的 HTTP 请求体的变量。

```
TopsecOS# waf enumeration variables phase response_body
RESPONSE_BODY
RESPONSE_CONTENT_LENGTH
RESPONSE_HEADERS
RESPONSE_HEADERS_NAMES
SERVER_IP
SERVER_NAME
SERVER_PORT
OUTPUT_BODY
```

TX_STORE

USER_ID

USERAGENT_IP

XML

waf enumeration translate-functions <cr>

命令描述：

该命令显示 TopWAF 支持的转换函数。具体如下表所示。

函数名称	函数名称	函数名称	函数名称
decodeBase64	decodeHtmlEntity	parityOdd7bit	decodeUrlUni
decodeSqlHex	decodeJs	parityZero7bit	utf8toUnicode
decodeBase64Ext	length	removeNUlls	sha1
encodeBase64	tolower	removeWhitespace	leftTrim
compressWhitespace	md5	replaceComments	rgithTrim
decodeCss	none	removeCommentsChar	trim
DecodeEscapeSeq	regularPath	removeComments	
decodeHex	regularPathWin	replaceNulls	
encodeHex	parityEven7bit	decodeUrl	

命令示例：

TopsecOS# **waf enumeration translate-functions**

decodeBase64

decodeSqlHex

decodeBase64Ext

encodeBase64

compressWhitespace

decodeCss

DecodeEscapeSeq

……

5.2.14.2 漏洞扫描报告生成防护策略

TopWAF 支持虚拟补丁功能，即将 Web 网站的漏洞扫描报告自动生成防护策略，支持 appscan、w3af、topscanner 三种扫描报告类型。其中 appscan 为 IBM 开发的扫描器生成的扫描报告，w3af 为一种开源的扫描器生成的扫描报告，topscanner 为 TopWAF 自带的漏洞扫描功能生成的 XML 格式扫描报告，关于 TopWAF 漏洞扫描功能的配置具体请参见 5.7 报表策略

TopWAF 支持日报、周报、月报，支持中文、英文两种语言，通过引用邮件策略，可以将生成的 PDF 格式报表发送到指定邮箱，邮件策略的配置具体请参见 5.5 邮件策略。

TopWAF 最多支持添加 128 条报表策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **报表策略**。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。

在配置报表策略时，各项参数的具体说明如下表所示。

参数	说明
名称	设置报表策略名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。

参数	说明
定时发送计划时间表	设置定时发送告警信息的时间。 无：仅在有告警产生时发送告警邮件。 每日：通过设置“定时发送时间”参数，指定每日的指定时间发送报表信息。 每周：通过设置“星期集合”和“定时发送时间”参数，设置在指定的星期及时间发送报表信息。 每月：通过设置“日期集合”和“定时发送时间”参数，设置在指定的日期及时间发送报表信息。
报表语言	设置报表的语言，可选项：中文、英语。
邮件标题	设置告警邮件的标题，默认值：TopWAF 报表。
邮件内容	设置告警邮件的内容，默认值：TopWAF 报表信息。
邮件策略名	选择通过邮件发送告警信息的报表策略，关于邮件策略的配置具体请参见 5.5 邮件策略。

步骤3 参数配置完成后，点击【确定】按钮，完成报表策略的配置。

CLI 方式

waf report-policy add name <*mstring*> [**mail-policy** <*mstring*>] [**schedule** <none|daily|weekly|monthly>] [**weekdays** <*mstring*>] [**monthdays**<*mstring*>] [**attime** <*time*>] [**formats** <pdf>] [**title** <*mstring*>] [**body** <*mstring*>] [**language** <english|chinese>]

命令描述：

添加报表策略。

可使用 **waf report-policy delete** 命令删除报表策略。

可使用 **waf report-policy modify** 命令修改报表策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置报表策略名称。 字符串类型，支持数字、字母、中文和特殊字符“_-*.”，不以“\\”结尾且不包含“<script>”字符串。
mail-policy <*mstring*>	可选项，设置引用的邮件策略名称。 字符串类型，不以“\\”结尾且不包含“<script>”

参数	说明
	字符串。
schedule<none|daily|weekly|monthly>	可选项，设置定期发送告警计划（无|每日发送|每周发送|每月），默认为无，表示不定期发送告警信息。
weekdays <*mstring*>	可选项，设置 **schedule** 为每周发送时，设置该参数，设置每周定时发送时间。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。支持多输入形式，多个输入用逗号分隔，如“mon,tue”，表示星期一和星期二。
monthdays<*mstring*>	可选项，设置 **schedule** 为每月发送时，设置该参数，设置每月定时发送日期。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。支持多输入形式，多个输入用逗号分隔，如“1,22”，表示每月的 1 日和 22 日。
attime <*time*>	可选项，设置 **schedule** 为每日发送、每周发送或每月发送时，设置该参数，设置每日定时发送时间。 时间类型，表示每日定时发送时间，格式为：“hour:minute:second”，如 08:12:30。
formats <pdf>	可选项，设置报表文件的格式。 只能设置报表文件的格式为 pdf。
title <*mstring*>	可选项，设置邮件的标题。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-127。
body <*mstring*>	可选项，设置邮件内容。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-2047。
language <english|chinese>	可选项，设置报表使用的语言。英语|中文。

命令示例：

添加名称为 report 的报表策略，每周的周日和周一 12:00:00 定时发送报表。

TopsecOS# **waf report-policy add name** *report* **schedule** weekly **weekdays** mon,sun **attime** *12:00:00*

waf report-policy show [**name** <*mstring*>]

命令描述：

查看报表策略配置信息。

命令示例：

查看 report 报表策略的配置信息。

TopsecOS # **waf report-policy show name** *report*

Report Name : report

Time : 08:00:00

Schedule : monthly

Weekday :

Mondthday : 1

Formats : pdf

Report language : chinese

Title : TopWAF 报表

Body : TopWAF 报表信息。

Mail policy name :

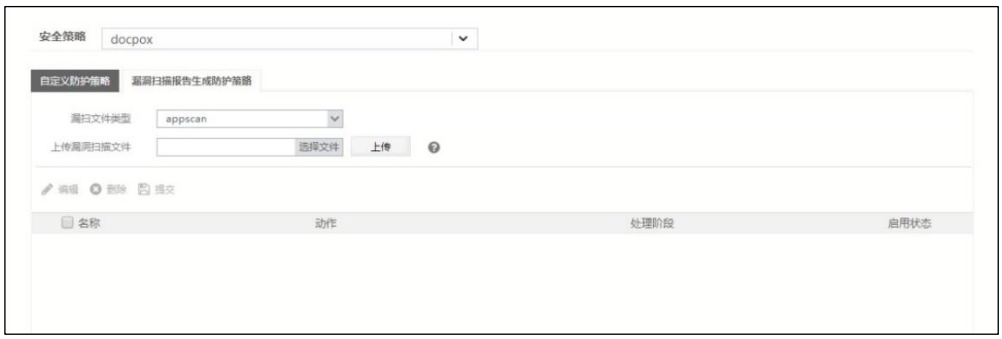
waf report-policy clean <cr>

命令描述：

清除报表策略配置信息。

。本节介绍如何将漏洞扫描报告生成防护策略。

步骤1 选择 **Web 防护** > **安全策略** > **自定义策略**，激活“漏洞扫描报告生成防护策略”页签，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 在“漏扫文件类型”下拉列表中选择漏洞报告类型，可选项：appscan、w3af、topscanner。

步骤4 点击【选择文件】选择管理主机中保存的漏洞扫描报告，点击【上传】按钮，TopWAF 则自动生成防护策略。

步骤5 点击『编辑』，可对自动生成的防护策略进行修改。

步骤6 点击“启用状态”栏的图标，可启用/禁用自动生成的防护策略。

5.2.15 高级设置

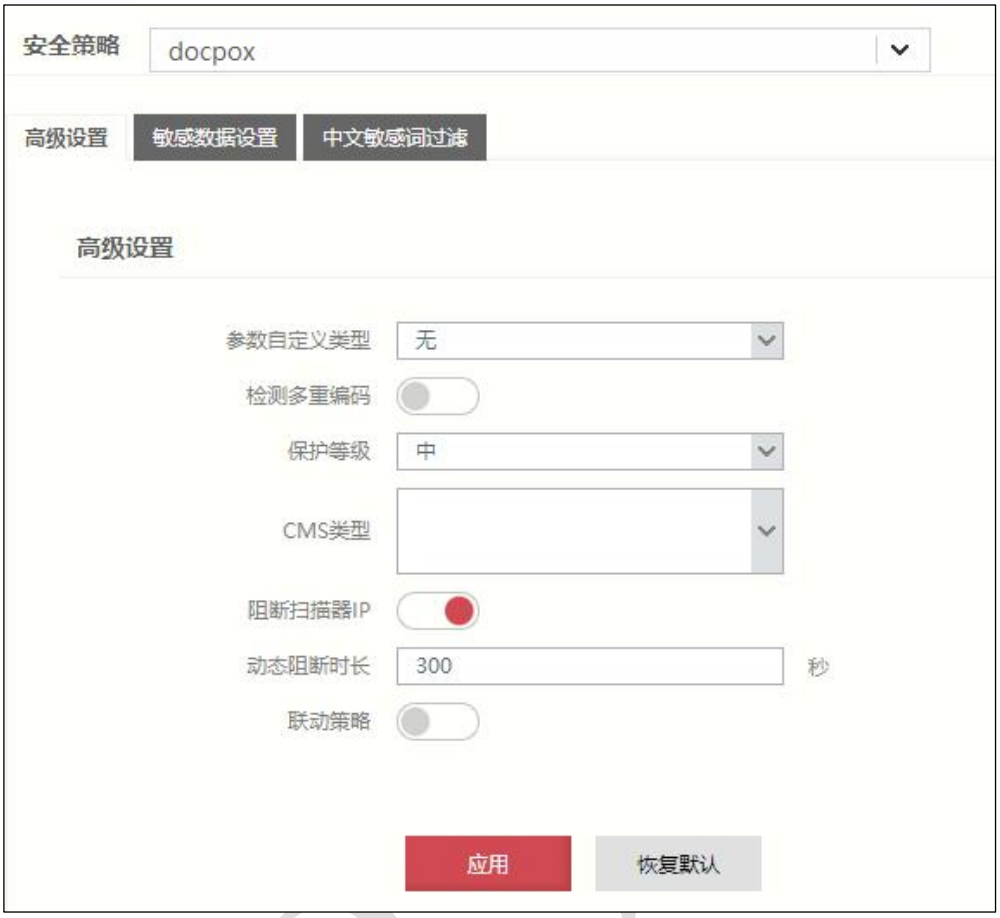
5.2.15.1 高级设置

高级设置包含一些不常用的高级功能，比如双重编码的检测、CMS 类型配置、是否阻断扫描器、是否启用联动策略等。

WEBUI 方式

在配置参数数据类型和敏感数据类型控制策略时，首先需定义参数数据类型和敏感数据类型，关于数据类型的定义具体请参见 5.1.6 数据类型。

步骤1 选择 **Web 防护** > **安全策略** > **高级设置**，激活“高级设置”页签，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置参数数据控制。

在配置参数数据控制时，各项参数的具体说明如下表所示。

参数	说明
参数自定义类型	选择已定义的参数数据类型，或点击下拉列表中的『新建』，新建参数数据类型，配置参数数据类型控制策略。
检测多重编码	设置是否开启检测多重编码功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。 多重编码攻击技术，可以使用十六进制形式将用户的请求参数编码转换多次。Web 服务器接受多种编码格式，接收到用户 HTTP 请求时，对报文解码第一重解码，并进行安全策略检查；后续的模块对请求报文进行数据处理并第二重及多重的编码，但是此时不进行安全性检查，如果在报文中包含有攻击报文，此时也无法进行安全防御，导致应用程序收到攻击甚至导致运行异常。 部分攻击者甚至使用 3 次或 3 次以上的编码转换来进行攻击，开启多重编码检查功能，可对多重的编码均进行安全防御检查，保护 Web 服务器安全。
保护等级	设置保护等级，可选项：高、中、低；默认值：中。 高：规则库中精准度为高、中、低的防御规则生效。 中：规则库中精准度为中、高的防御规则生效。

参数	说明
	低：规则库中精准度为高的防御规则生效。
CMS 类型	设置网站内容管理系统的类型，在下拉框中可以选择内容管理系统类型。
阻断扫描器 IP	设置是否开启阻断扫描器 IP 功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。开启后可以阻断扫描器对网站扫描的 IP，防护网站。
动态阻断时长	当“阻断扫描器 IP”项开启后，该参数有效，设置阻断该 IP 的时长。默认为 300 秒。
联动策略	设置是否开启联动策略功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。开启联动策略后，TopoWAF 如果与其他设备联动，将策略发送至联动的设备

步骤4 点击【应用】按钮完成配置；点击【恢复默认】按钮恢复出厂配置。

CLI 方式

waf security-policy modify name <*mstring*> **protect-level** <high|middle|low>

命令描述：

修改服务器保护等级。

参数说明：

参数	说明
name <*mstring*>	必选项，指定待修改的安全策略，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
protect-level <high|middle|low>	必选项，设置保护等级。高|中|低 高：规则库中精准度为高、中、低的防御规则生效。 中：规则库中精准度为中、高的防御规则生效。 低：规则库中精准度为高的防御规则生效。

命令示例：

在安全策略“sec01”中，修改服务器保护等级为高。

TopsecOS# **waf security-policy modify name** *sec01* **protect-level** high

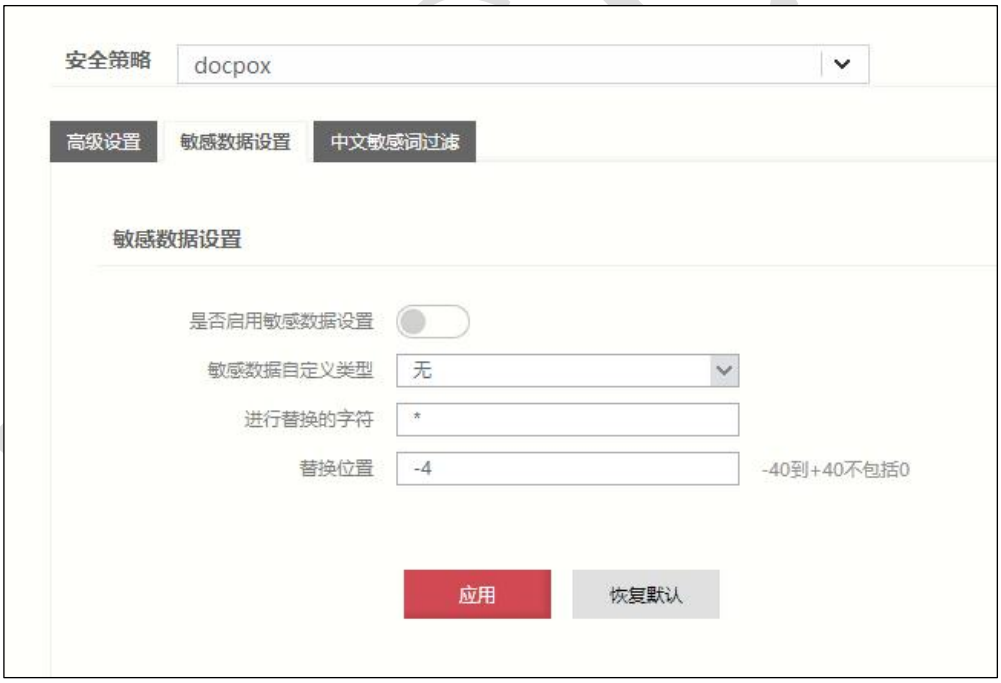
5.2.15.2 敏感数据设置

TopWAF 可以自定义敏感数据类型，如果对 Web 网站启用敏感数据控制策略，一旦发现 Web 服务器向客户端传递敏感数据，即根据敏感数据策略将敏感数据替换为其他特定字符。

WEBUI 方式

在配置敏感数据类型控制策略时，首先需定义敏感数据类型，关于数据类型的定义具体请参见 5.1.6 数据类型。

步骤1 选择 **Web 防护** > **安全策略** > **高级设置**，激活“敏感数据设置”页签，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置敏感数据处理策略。

在配置敏感数据处理策略时，各项参数的具体说明如下表所示。

参数	说明
是否启用敏感数据设置	设置是否启用敏感数据检查开关。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
敏感数据自定义	选择已定义的敏感数据类型，或点击下拉列表中的『新建』，新

参数	说明
类型	建敏感数据类型，配置敏感数据类型控制策略。关于敏感数据类型的配置具体请参见 5.1.6 数据类型。
进行替换的字符	设置替换敏感数据的字符。 说明：只支持输入一个字符。
替换位置	设置 TopWAF 对敏感数据进行替换的位置。取值范围：-40 到+40，不包括 0。 说明： 1）设置为 N（N 表示正数），表示 TopWAF 将敏感数据的前 N 位替换；设置为-N（N 表示正数），表示 TopWAF 将敏感数据后 N 位替换。 2）如果敏感数据位数小于该参数所设置的字符替换个数，TopWAF 则会将该匹配的敏感数据内容全部替换。

步骤4 点击【应用】按钮完成配置；点击【恢复默认】按钮恢复出厂配置。

CLI 方式

waf sensitive-policy modify security-policy <*string*> [**enable** <on|off>] [**sensitive-group** <*mstring*>] [**tochar** <*mstring*>] [**position** <*mstring*>]

命令描述：

配置敏感数据处理策略。

参数说明：

参数	说明
security-policy <*string*>	必选项，指定待配置敏感数据处理策略的安全策略，关于安全策略的配置具体请参见 5.2.1 安全策略。字符串类型，表示安全策略的名称。 注意：不包含“&\"\\'%<>”和空格。
enable <on|off>	可选项，设置是否启用敏感数据处理策略。是|否
sensitive-group <*mstring*>	可选项，设置已定义的敏感数据类型组名称，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
tochar <*mstring*>	可选项，设置 TopWAF 替换敏感数据的字符。字符串类型，只支持输入一个字符。
position <*mstring*>	可选项，设置 TopWAF 将特定字符替换敏感数据的开始位置。字符串类型，取值范围：-40 到+40，不包括 0。设置

参数	说明
	为正数 N，则将前 N 个字符替换；设置为负数 N，则将前 N 个字符替换。

命令示例：

在安全策略“sec01”中添加敏感数据策略，实现 TopWAF 发现敏感电话数据时，则将该电话号码的后面 4 位替换为****。

TopsecOS# **waf security-policy add name** *sec01*

TopsecOS# **waf datatype-group add name** *datagroup* **group-type** sensitive

TopsecOS# **waf datatype add group** *datagroup* **name** *tel* **regex**

‘^(0|86|17951)?(13[0-9]|15[012356789]|18[0-9]|14[57])[0-9]{8}$’ **verify-type** phone

TopsecOS# **waf sensitive-policy modify security-policy** *sec01* **enable** on

sensitive-group *datagroup* **tochar** * **position** *-4*

waf sensitive-policy show security-policy <*string*>

命令描述：

显示敏感数据处理策略。

命令示例：

显示“sec01”安全策略中的敏感数据处理策略。

TopsecOS# **waf sensitive-policy show security-policy** *sec01*

Security-Policy Name: sec01

Enable: on

Replace to Char: *

Position: -4

Sensitive-group: datagroup

waf sensitive-policy reset security-policy <*string*>

命令描述：

重置敏感数据处理策略。

命令示例：

重置安全策略“sec01”中敏感数据处理策略。

TopsecOS# **waf sensitive-policy reset security-policy** *sec01*

waf security-policy modify name <*mstring*> **protect-level** <high|middle|low>

命令描述：

修改服务器保护等级。

参数说明：

参数	说明
name <*mstring*>	必选项，指定待修改的安全策略，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。
protect-level <high|middle|low>	必选项，设置保护等级。高|中|低 高：规则库中精准度为高、中、低的防御规则生效。 中：规则库中精准度为中、高的防御规则生效。 低：规则库中精准度为高的防御规则生效。

命令示例：

在安全策略“sec01”中，修改服务器保护等级为高。

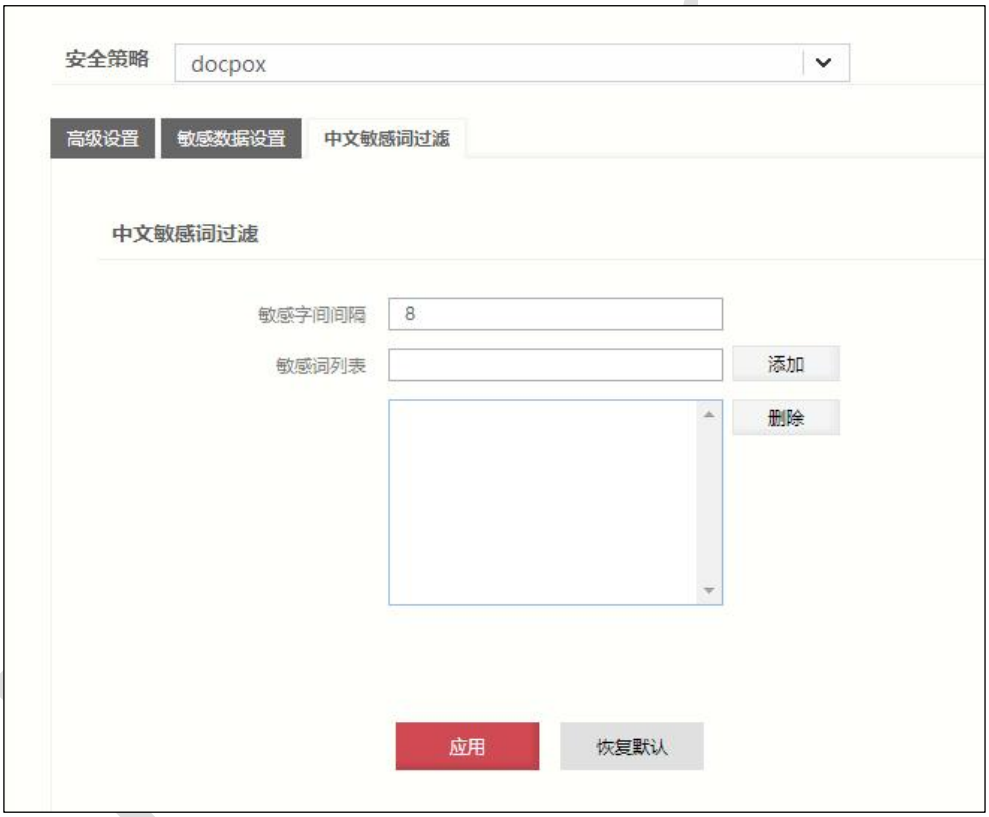
TopsecOS# **waf security-policy modify name** *sec01* **protect-level** high

5.2.15.3 中文敏感词过滤

TopWAF 支持中文敏感词过滤技术，通过对用户提交信息进行过滤，有效的解决了用户提交政治敏感、违反法规相关的言论信息，从而保障网站的内容健康呈现。

WEBUI 方式

步骤1 选择 **Web 防护** > **安全策略** > **高级设置**，激活“中文敏感词过滤”页签，如下图所示。



步骤2 从“安全策略”下拉列表中选择需要配置的安全策略。

步骤3 配置中文敏感词过滤策略。

在配置中文敏感词过滤策略时，各项参数的具体说明如下表所示。

参数	说明
敏感字间间隔	设置敏感字的间隔，可以按照间隔大小匹配敏感字的过滤策略。
敏感词列表	设置中文敏感词。在右侧的文本框中输入敏感词后，点击右侧的【添加】按钮，将输入的敏感词添加到列表中。

步骤4 点击【应用】按钮完成配置；点击【恢复默认】按钮恢复出厂配置。

CLI 方式

waf sensitive-keywords add-keyword security-policy <*mstring*> **word** <*mstring*>

命令描述：

添加中文敏感词过滤策略。

参数说明：

参数	说明
security-policy <*mstring*>	必选项，指定待修改模糊匹配策略的安全策略，字符串类型。关于安全策略的配置具体请参见 5.2.1 安全策略。 注意：不能以“\\”结尾或不包含“<script>”字符串。
word <*mstring*>	必选项，设置中文敏感词，字符串类型。 注意：不能以“\\”结尾或不包含“<script>”字符串。

5.3 服务器策略

服务器策略功能指定了 TopWAF 保护的服务器对象、安全策略以及部署模式等。一般情况下，TopWAF 部署于防火墙和 Web 服务器之间，对 Web 服务器的出入流量进行检测。TopWAF 为了适应不同网络场景的需求，支持多种部署模式。TopWAF 支持的部署模式包括：Web 保护、服务器负载均衡、离线检测及反向代理。

- Web 保护模式

在 Web 保护模式下，TopWAF 用于在线保护单个服务器或者服务器组。TopWAF 的接口可以工作在路由模式，也可以工作在交换模式、虚拟线模式。其中，虚拟线模式是最为便捷的部署方式，TopWAF“完全透明”地接入网络，无需调整用户的拓扑，无需关心 vlan 和聚合接口的配置，推荐使用此种部署方式。

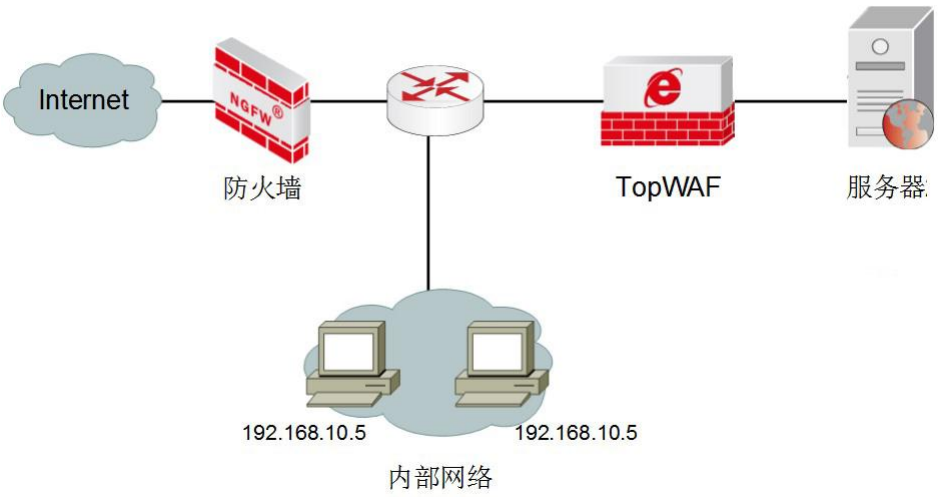


图 5-3 Web 保护模式组网示意图

- 服务器负载均衡模式

对于一些由多台 Web 服务器组成的网站系统，TopWAF 设备可以采用服务器负载均衡模式部署，把流量按照用户配置的调度算法分发给各个物理服务器。这样在确保 Web 应用安全的前提下，实现服务器负载均衡。

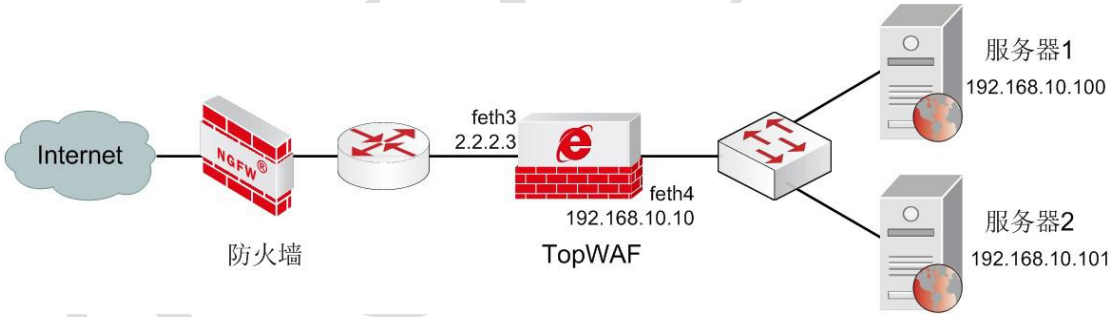


图 5-4 负载均衡模式组网示意图

- 离线检测模式

TopWAF 工作在离线检测模式时，设备只对 HTTP（S）流量进行监控和报警，不进行阻断。如下图所示，接口 feth3 工作在嗅探模式，只接收报文，并不转发。该模式需要使用交换机的端口镜像功能，也就是将交换机端口上的双向 HTTP（S）流量镜像一份给 TopWAF。

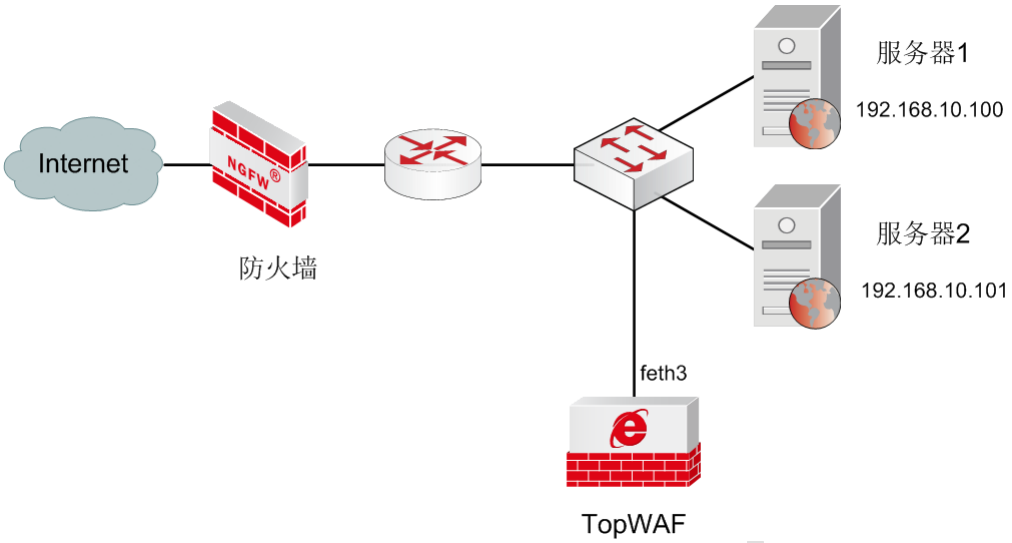


图 5-5 离线检测模式组网示意图

- 反向代理模式

TopWAF 工作于反向代理模式时，对于客户端而言 TopWAF 就像是原始服务器，并且客户端不需要进行任何特别的设置。客户端向 TopWAF 发送普通请求，TopWAF 判断向何处（原始服务器）转交请求，并将获得的内容返回给客户端。

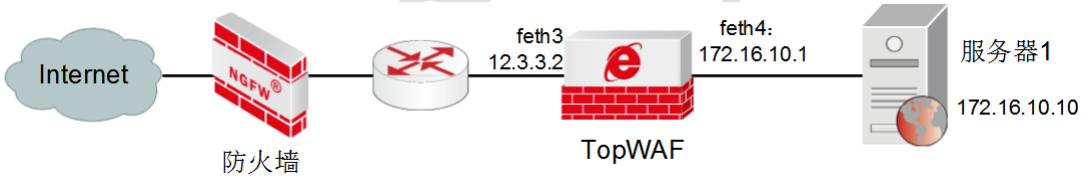


图 5-6 反向代理模式示意图

WEBUI 方式

步骤1 选择 **Web 防护** > **服务器策略**。

步骤2 点击『添加』，弹出“添加服务器策略”窗口，如下图所示。

步骤3 配置服务器策略参数。

在配置服务器策略时，各项参数的具体说明如下表所示。

参数		说明
名称		设置服务器策略名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
是否启用		设置是否启用该服务器策略。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
流量日志		设置是否启用流量日志功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。开启流量日志功能后，可查看流量日志统计结果，具体请参见 4.2.1 日志查看。
部署	部署模式	设置服务器的部署模式。 1）Web 保护：当服务器部署在桥接模式或者路由模式时，保护单个服务器或者服务器组。 2）服务器负载均衡：当服务器部署负载均衡模式时，被保护的服务器可以负载均衡，根据调度模式响应客户端的请求。 3）离线检测：TopWAF 旁路检测被保护的服务器。离线检测模式的服务器策略只处理嗅探接口接收的数据，并不发送任何阻断报文，因此，TopWAF 至少指定一个接口为嗅探模式，离线保护模式的服务器策略正常生效。 4）反向代理：客户端向 TopWAF 发送普通请求，TopWAF 判断向何处（原始服务器）转交请求，并将获得的内容返回给客户端。
	单个服务器	当“部署模式”设置为 Web 保护或离线检测时，设置被保护的单个服务器。服务器策略对单个服务器生效，在界面中输入服务器的 IP 地址或域名及端口号。
	服务器组	选择服务器组，关于服务器组的设置具体请参见 5.1.3 服务器组。
	虚拟服务器	当“部署模式”设置为“服务器负载均衡”或“反向代理”时，设置服务器组为用户提供的虚拟服务器地址及端口。 此时服务器组的成员对用户不可见，仅可通过虚拟服务器地址及端口访问服务器资源。
	调度模式	当“部署模式”设置为“服务器负载均衡”或“反向代理”时，设置服务器组成员的调度模式。 1）轮叫调度：根据服务器组成员均衡，表示响应请求报文时进行轮询，依次使用从第一个到最后一个可用的成员服务器。该模式适用于所有服务器处理性能均相同的情况。 轮叫调度算法假设所有服务器处理性能均相同，不管服务器的当前连接数和响应速度。不适用于服务器组中处理性能不一的情况，而且当请求服务时间变化比较大时，轮叫调度算法容易导致服务器间的负载不平衡。 2）加权轮叫：与轮叫模式类似，服务器组在按照次序以循环方式响应请求报文基础上，根据每个服务器的权重来响应请求报文。该模式适用于服务器的处理性能不相同的情况。关于服务器的权重设置具体请参见 5.1.3 服务器组。

参数		说明
		3）源地址散列：根据请求的源 IP 地址进行哈希运算找出对应的服务器，若该服务器是可用的且未超载，将请求发送到该服务器，否则返回空。 4)最小连接:将新的连接请求分配到当前连接数最小的服务器。最小连接调度是一种动态调度算法，通过服务器当前所活跃的连接数来估算服务器的负载情况。
	虚拟主机组	选择被保护的主机组，用于对接收的数据进行过滤，只保护主机组中列出的服务器。主机组的设置具体请参见 5.1.2 虚拟主机组。
	运行模式	选择当检测服务器安全策略生效时的动作。 1）检测但不阻断：继续进行检测，检测到攻击或者异常访问时，不阻断对服务器的访问。 2）关闭检测：关闭检测功能。 3）检测并阻断：继续进行检测，检测到攻击或者异常访问时，阻断当前对服务器的请求。
策略	安全策略	选择服务器的安全策略，关于安全策略的配置具体请参见 5.2.1 安全策略。
	告警策略	选择服务器的告警策略，关于告警策略的配置具体请参见 5.6 告警策略。
	IP 黑白名单	选择服务器策略中 IP 黑白名单，关于 IP 黑白名单的设置具体请参见 5.1.1IP 黑白名单。
	错误页面	选择服务器策略中错误页面，在触发服务器策略时，将返回错误页面的信息，关于错误页面的设置具体请参见 5.1.7 错误页面。
	智能模式	设置是否启用智能模式功能。默认为“  ”，表示已关闭，点击该按钮将显示“  ”，表示已开启。智能模式表示当一个客户端发起请求访问后，服务器如果成功响应，并且未触发 TopWAF 的安全防护策略，之后另外一个客户端发起同样的请求后，TopWAF 将不对服务器的响应报文的进行安全过滤，提高服务器响应速度。 说明： 开启智能模式前需要先开启“处理服务器响应”功能，否则智能模式不生效。
	自学习	设置是否启用自学习功能。默认为“”，表示已关闭，点击该按钮将显示“  ”，表示已开启。关于自学习的配置具体请参见 5.2.12 自学习。
	处理服务器响应	设置是否对服务器返回客户端的响应报文进行安全监测。默认为“  ”，表示已开启，点击该按钮将显示“  ”，表示已关闭。
	URI 大小写敏感性	设置是否启用 URI 地址大小写敏感性功能，开启该功能将区分 URI 地址中的大小写。默认为“  ”，表示已关闭，点击该

参数		说明
		按钮将显示“”，表示已开启。
	参数分隔符	选择 URI 地址的参数分隔符，可选项：&和；。
	Cookie 版本	选择 Cookie 分隔符的版本。 version0：由 Netscape 公司制定的，几乎所有的浏览器都支持。Cookie 的内容中不能包括：空格，方括号，圆括号，等于号（=），逗号，双引号，斜杠，问号，@符号，冒号，分号。 version1：根据 RFC2109 文档制定的。放宽了很多限制。version0 中所限制的字符都可以使用。
	真实客户端 IP 头	指定存放客户端真实 IP 地址的字段。当客户端通过代理访问服务器的时候，请求头中会有个字段存放真实客户端 IP 地址，通常使用的是“X-Forworded-For”。
SSL	是否启用	设置是否启用 SSL 功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
	证书	选择 TopWAF 中的证书，关于证书的导入具体请参见 5.1.8 证书。
DDoS 防御	是否启用	设置是否启用 DDoS 防御功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
	防护对象	选择 DDoS 防御对象。关于 DDoS 防御的配置具体请参见 6.3DDOS 防御。

步骤4 参数配置完成后，点击【确定】按钮，完成服务器策略的配置。

CLI 方式

waf server-policy add name <*mstring*> **security-policy** <*string*> **deploy-mode** <bridge|route|nat|sniffer|rproxy > **{address** <*mstring*> **port** <*string*>|**server-group** <*mstring*>|**virtual-address** <*mstring*> **virtual-port** <*num*>**}** [**alarm-policy** <*mstring*>] [**argument-separator** < and|comma >] [**autolearn** <on|off>] [**case-sensitive** <on|off>] [**certfile** <*mstring*>] [**cookie-version** <0|1>] [**ddos-enable** <on|off>] [**enable** <on|off>] [**vhost-group** <*mstring*>] [**ip-group** <*mstring*>] [**mode** <disable|enable|detection>] [**process-response** <on|off>] [**schedule** <rr|wrr|lc|src_hash>] [**smartmode** <on|off>] [**ssl** <on|off>] [**traffic-log** <on|off>] [**ddos-zone** <*mstring*>] [**error-page** <*mstring*>] [**realip-header** <*mstring*>]

命令描述：

添加服务器策略。

可使用 **waf server-policy delete name** <*mstring*>命令删除服务器策略。

可使用 **waf server-policy modify name** <*mstring*> **security-policy** <*string*> **deploy-mode** <bridge|route|nat|sniffer|rproxy > **{address** <*mstring*> **port** <*string*>|**server-group** <*mstring*>|**virtual-address** <*mstring*> **virtual-port** <*num*>**}** [**alarm-policy** <*mstring*>] [**argument-separator** <and|comma>] [**autolearn** <on|off>] [**case-sensitive** <on|off>] [**certfile** <*mstring*>] [**cookie-version** <0|1>] [**ddos-enable** <on|off>] [**enable** <on|off>] [**vhost-group** <*mstring*>] [**ip-group** <*mstring*>] [**mode** <disable|enable|detection>] [**process-response** <on|off>] [**schedule** <rr|wrr|lc|src_hash>] [**smartmode** <on|off>] [**ssl** <on|off>] [**traffic-log** <on|off>] [**ddos-zone** <*mstring*>] [**error-page** <*mstring*>] [**realip-header** <*mstring*>]命令修改服务器策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置服务器策略名称，字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。
security-policy <*string*>	必选项，设置安全策略。字符串类型，为已定义的安全策略。关于安全策略的配置具体请参见 5.2.1 安全策略。
deploy-mode bridge|route|nat|sniffer|rproxy	必选项，设置部署模式。桥模式|路由模式|服务器负载均衡模式|离线检测模式|反向代理。
address <*mstring*>	可选项，设置单个服务器地址。字符串类型，表示服务器地址。当 **deploy-mode** 设置为 bridge、route、sniffer 或者 rproxy 时，可设置该参数。 注意：不能以“\\”结尾或不包含“<script>”字符串。
port <*string*>	可选项，设置服务器端口号，取值范围：1-65535。当 **deploy-mode** 设置为 bridge、route、sniffer 时，可设置该参数。可设置多个端口，最多支持六个端口。
server-group <*mstring*>	可选项，设置服务器组。字符串类型，为已定义的服务器组对象。 注意：不能以“\\”结尾或不包含“<script>”字符串。
virtual-address <*mstring*>	可选项，设置虚拟服务器地址。字符串类型，表示虚拟服务器地址。当 **deploy-mode** 设置为 nat 时，可设置该参数。
virtual-port <*num*>	可选项，设置虚拟端口。数值类型，取值范围：1-65535。当 deploy-mode 设置为 nat 时，可设置该参数。
alarm-policy <*mstring*>	可选项，设置告警策略名称。字符串类型，为已定义的告警策略名称。

参数	说明
argument-separator <and|comma>	可选项，设置 URI 地址参数分隔符。&|;
autolearn <on|off>	可选项，设置是否启用自学习功能。开启|关闭
case-sensitive <on|off>	可选项，设置是否启用大小写敏感性。开启|关闭
certfile <*mstring*>	可选项，设置服务器证书。字符串类型，为已定义的证书对象。
cookie-version <0|1>	可选项，设置 Cookie 版本。Netscape 版本|新的 RFC 规范版本，默认值：0。
ddos-enable <on|off>	可选项，设置是否启用 DDOS 防护。开启|关闭，默认值：关闭。
enable <on|off>	可选项，设置是否开启服务器策略。开启|关闭，默认值：开启。
vhost-group <*mstring*>	可选项，设置主机组。字符串类型，为已定义的主机组对象。
ip-group <*mstring*>	可选项，设置 IP 黑白名单名称。字符串类型，为已定义的 IP 黑白名单对象。
mode <disable|enable|detection>	可选项，设置服务运行模式。关闭检测|检测不阻断|检测并阻断
process-response <on|off>	可选项，设置是否处理服务器响应。开启|关闭，默认值：开启。
schedule <rr|wrr|lc|src_hash>	可选项，设置调度模式。轮叫模式|加权轮叫|最小连接|源地址散列
smartmode <on|off>	可选项，设置是否开启智能模式。开启|关闭，默认值：关闭。
ssl <on|off>	可选项，设置是否为 HTTPS 类型服务器。是|否，默认值：否。
traffic-log <on|off>	可选项，设置是否开启到此服务器策略的流量日志。开启|关闭，默认值：关闭。
ddos-zone <*mstring*>	可选项，设置 DDOS 安全策略。字符串类型，为已定义的 DDOS 安全策略。
error-page <*mstring*>	可选项，设置错误页面。字符串类型，为已定义的错误页面名称。
realip-header <*mstring*>	可选项，设置原始客户端 IP 头。字符串类型，指定存放客户端真实 IP 地址的字段，通常使用的是“X-Forworded-For”。

命令示例：

添加名称为 test 的服务器策略，引用 sec01 安全策略，设置服务器服务器部署模式为路由模式，服务器地址为 192.168.3.3，服务器端口为 80。

TopsecOS# **waf server-policy add name** *test* **security-policy** *sec01* **deploy-mode** *route* **address** *192.168.3.3* **port** *80*

waf server-policy show [**name** <*mstring*>]

命令描述：

查看服务器策略配置信息。

参数说明：

参数	说明
name <*mstring*>	可选项，设置服务器策略名称。字符串类型，支持数字、字母、中文和特殊字符“_-*.”。 注意：不能以“\\”结尾或不包含“<script>”字符串。

命令示例：

查看 test 服务器策略的配置信息。

TopsecOS# **waf server-policy show name** *test*

ID: 8032

Server Name: test

Enable: on

Running Mode: enable

Deploy Mode: bridge

Address: 192.168.104.28

Port: 80

Host Group:

Alarm Policy:

```
IP Group:
Security Policy:          test
Autolearn:                on
Traffic-Log Enable:       on
Smart mode:               off
Response Process:         on
Argument separator:       and
Cookie Version:           0
Case Sensitive:           off
SSL enable:               off
Certfile:
DDos enable:              on
DDos zone name:           33333
Error Page                default
```

waf server-policy clean<cr>

命令描述：

清除服务器策略配置信息。

5.4 自学习报告

TopWAF 可对服务器与客户端交互的 HTTP 流量进行分析，学习参数信息和 cookie 信息。针对不同的 URL 路径，学习请求方法，学习 Web 网站参数的长度、类型、隐藏域和只读属性信息；学习 Cookie 的路径、域名、只读属性和安全属性等信息，并以报告的形式显示。本节介绍如何对自学习报告执行查看、修改和删除等操作。

WEBUI 方式

TopWAF 可进行自学习之前，管理员首先需执行如下操作：

- 设置自学习策略，关于自学习策略的配置具体请参见 5.2.12 自学习。
- 开启服务器策略的自学习开关，关于服务器策略自学习开关的开启具体请参见 5.3 服务器策略。

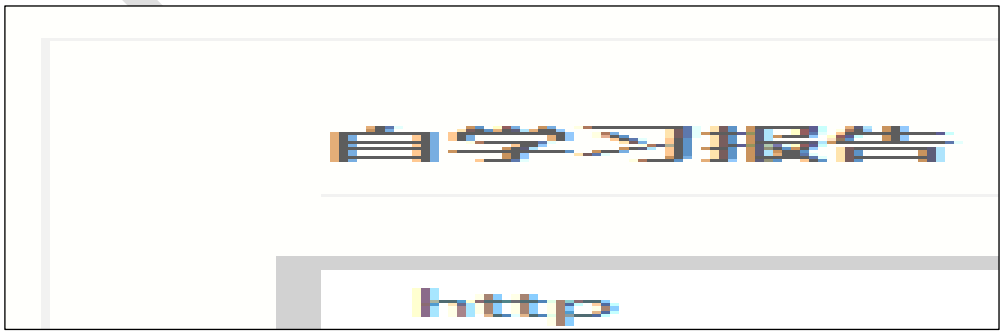
步骤1 选择 **Web 防护** > **自学习报告**。

步骤2 在“服务器策略”下拉列表中选择服务器策略名称，显示“学习到的页面”。

步骤3 查看学习结果。

1）查看参数学习结果。点击“自学习报告”导航栏相应的节点，显示参数学习结果界面，如下图所示。

2）查看 Cookie 学习结果。激活“Cookie”页签，显示学习到的 Cookie 信息，如下图所示。



步骤4 修改学习结果。选中待修改的学习结果，点击『编辑』可修改学习到的参数信息。

步骤5 删除学习结果。选中待删除的参数项，点击『删除』可删除 TopWAF 自学习到的参数信息。

步骤6 重新学习。点击【重新学习】按钮，TopWAF 自学习到的所有参数信息清空，重新学习。

5.5 邮件策略

邮件策略可以被告警策略和报表策略引用，当告警策略或报表策略被触发时，系统通过配置的邮件策略将告警或报表信息发送给指定的邮件收件人。关于告警策略的配置具体请参见 5.6 告警策略，关于报表的策略的配置具体请参见 5.7 报表策略。

TopWAF 最多支持添加 128 条邮件策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **邮件策略**。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。

在配置邮件策略时，各项参数的具体说明如下表所示。

参数	说明
邮件策略名称	设置邮件策略名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
邮件服务器地址	设置邮件服务器地址。支持 IPv4 地址、IPv6 地址和 URL 域名形式。
邮件服务器端口	设置邮件服务器端口号，取值范围：1-65535；默认值：25。
安全认证方式	设置邮件认证的安全认证方式。要求客户端和服务器双方的加密机制一致。

参数	说明
	说明： 1）明文密码：密码采用明文报文发送。 2）starttls 认证：将纯文本连接升级为加密连接（TLS 或 SSL）的方式，而不是另外使用一个端口作加密通信。 3）启用 SSL：使用 SSL 加密连发发送邮件。
邮件认证开关	设置是否开启邮件认证功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。 说明： “安全认证方式”为“明文密码”时，邮件认证开关才可以关闭。
邮件认证用户名	启动“邮件认证开关”后才能设置该参数值。用于发送报警信息的电子邮件用户名。
邮件认证密码	启动“邮件认证开关”后才能设置该参数值。设置发件人帐户对应的密码。
发件人地址	设置邮件发件人地址，例如 abc@topsec.com.cn。TopWAF 只支持设置一个发件人地址。
收件人地址	设置邮件收件人地址，例如 abc@topsec.com.cn，TopWAF 支持设置多个收件人地址，多个收件人地址之间用逗号“,”分隔。

步骤3 参数配置完成后，点击【确定】按钮，完成邮件策略的配置。

步骤4 勾选邮件策略，点击『测试』，测试邮件策略是否生效。如果配置正确，将弹出窗口提示“测试成功”，邮件策略指定的收件人将会接收到测试邮件。

CLI 方式

waf mail-policy add name <*mstring*> **address** <*mstring*> **port** <*num*> **from** <*mstring*> **to** <*mstring*> [**auth** <on|off>] [**auth-username** <*mstring*>] [**auth-passwd** <*astring*>] [**security** <plain|starttls|ssl>]

命令描述：

添加邮件策略。

可使用 **waf mail-policy delete** 命令删除邮件策略。

可使用 **waf mail-policy modify** 命令修改邮件策略。

参数说明：

参数	说明
name <m*string*>	必选项，设置邮件策略名称。

参数	说明
	字符串类型。不以“\\”结尾、或不包含“<script>”的字符串。长度范围：1-31 字符。
address <m*string*>	必选项，设置邮件服务器的地址。 字符串类型，支持 IPv4 地址、IPv6 地址和 URL 域名形式，长度范围：1-45 字符。
port <*num*>	可选项，设置邮件服务器的端口号。 实数类型，取值范围：0-65535；默认值：25。
from <m*string*>	必选项，设置邮件发件人地址。 字符串类型，例如：topsec@topsec.com.cn，长度范围：1-63 字符。
to <m*string*>	必选项，设置邮件收件人地址。 字符串类型，例如：topsec@topsec.com.cn，长度范围：1-511 字符。
auth <on|off>	可选项，设置是否开启邮件认证开关。 开启|关闭。
auth-username <*mstring*>	可选项，设置“auth”为 on 后，需设置发件人帐户对应的用户名。 字符串类型，不以“\\”结尾、或不包含“<script>”的字符串。长度范围：1-63 字符。
auth-passwd <*astring*>	可选项，设置“auth”为 on 后，需设置发件人帐户对应的用户密码。 字符串类型，可包含任意特殊字符，长度范围：1-127 字符。
security <plain|starttls|ssl>	可选项，设置邮件认证的安全认证方式。 明文认证|采用 STARTTLS 认证|采用 SSL 认证，默认值：明文认证。 说明： 该参数设置为“starttls”或“ssl”时，命令 **auth** <on|off> 邮件认证开关必须设置为“on”。

命令示例：

添加名称为 mail-policy 的邮件策略，邮件服务器的地址为 192.168.6.9，端口号为 25，发件人地址为 zhangsan@topsec.com.cn，收件人地址为 lisi@topsec.com.cn。

TopsecOS# **waf mail-policy add name** *mail-policy* **address** *192.168.6.9* **port** *25* **from** *zhangsan@topsec.com.cn* **to** *lisi@topsec.com.cn*

waf mail-policy test name <*mstring*>

命令描述：

测试邮件策略是否配置正确。

参数说明：

参数	说明
name <*mstring*>	必选项，设置邮件策略名称。 字符串类型，不以“\\”结尾、或不包含“<script>”的字符串。

命令示例：

TopsecOS# **waf mail-policy test name** *mail-policy*

测试完成后，策略中收件人地址将收到标题为“Test mail”，邮件正文为“This is a test mail sent by Topwaf, please don't reply this.”的测试邮件。

waf mail-policy show [**name** <*mstring*>]

命令描述：

查看邮件策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置邮件策略名称。 字符串类型，不以“\\”结尾、或不包含“<script>”的字符串。

命令示例：

查看 mail-policy 邮件策略的配置信息。

TopsecOS# **waf mail-policy show name** *mail-policy*

Mail policy Name : mail-policy

Address : 192.168.6.9

Port : 25

Security type : plain

From : zhangsan@topsec.com.cn

To : lisi@topsec.com.cn

Authorization : off

Username :

Password :

5.6 告警策略

TopWAF 的告警功能给管理员提供了一个自动化的攻击监管平台，可帮助管理员监控站点的安全状态。管理员无需登录 TopWAF 设备，通过手机、PC 查看邮箱接收的告警信息，便可掌控 TopWAF 所保护站点遭受攻击的情况。

TopWAF 告警模块会周期性统计 TopWAF 检测到的各种攻击信息，并能够根据告警策略，将被保护站点遭受的攻击生成告警信息，在告警策略指定的时间（每小时、每日或每周）定期将告警信息通过邮件发送给指定收件人。

- ✧ 告警策略只有被服务器策略引用后，才会生成告警信息。此外，告警策略只有被邮件策略引用后，告警信息才能发送给指定收件人。关于服务器策略的配置具体请参见 5.3 服务器策略。关于邮件策略的配置具体请参见 5.5 邮件策略。
- ✧ TopWAF 最多支持添加 128 条告警策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **告警策略**。

步骤2 添加告警策略。

1）点击『添加』，弹出“添加”窗口，如下图所示。

在配置告警策略时，各项参数的具体说明如下表所示。

参数	说明
名称	设置告警策略名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
攻击类型	设置告警的攻击类型。 全选：选择所有的攻击类型。 反选：选择除了已经勾选的攻击类型外的攻击类型。 勾选攻击类型：跨站脚本攻击（XSS）、跨站请求伪造攻击（CSRF）、SQL 注入攻击（SQLI）、系统命令注入攻击（OSI）、远程文件包含攻击（RFI）、WebShell 检测、目录遍历攻击（DIRT）、信息泄露攻击（Info Leak）、用户自定义规则、robots 抓取、恶意扫描、异常、违规（violation）、策略限制、Cookie 挟持、盗链、LDAP 注入防护、XPath 注入防护、SSI 注入防护、Web 服务器漏洞防护、访问控制、其它。
定时发送计划时间表	设置定时发送告警信息的时间。 每小时：通过设置“间隔小时数”参数，指定每隔几小时发送告警邮件。

参数	说明
	每日：通过设置“定时发送时间”参数，指定每日的指定时间发送告警信息。 每周：通过设置“星期集合”和“定时发送时间”参数，设置在指定的星期及时间发送告警信息。
间隔小时数	当“定时发送计划时间表”设置为“每小时”时，设置告警信息周期发送告警信息的时间间隔，在一个定时发送周期内，如果设备产生告警信息，将发送告警邮件到指定的收件人。单位：小时；取值范围：1-24；默认值：2。
星期集合	当“定时发送计划时间表”设置为“每周”时，设置在每周的指定星期发送告警信息，可选择多项。
定时发送时间	当“定时发送计划时间表”设置为“每日”或者“每周”时，设置发送告警信息的具体时间。
告警等级过滤	设置发送的告警信息需满足的安全等级条件，只发送安全等级高于设置的等级的告警信息。可选项：低级、中级、高级。
报警类型	可选项：邮件、手机。选择“邮件”，TopWAF 以发送邮件的方式进行报警；选择“手机”，TopWAF 通过发送短信的方式进行报警。 说明： 1）选择以邮件方式报警时，需配置 TopWAF 与邮件服务器的连接信息，具体请参见 5.5 邮件策略； 2）选择以手机方式报警时，需配置短信服务，具体请参见 设置短信服务。
邮件策略名	选择通过邮件发送告警信息的邮件策略，关于邮件策略的配置具体请参见 5.5 邮件策略。
邮件标题	设置告警邮件的标题，默认值：TopWAF 告警信息报告。
接收信息手机号	设置接收报警信息的手机号码。

2）参数配置完成后，点击【确定】按钮，完成告警策略的配置。

步骤3 设置短信服务（设置以短信方式告警的告警策略时，该步骤必选）。

1）点击『短信告警』，设置 WAF 与短信服务端的认证信息，如下图所示。

在设置短信服务时，各项参数的具体说明如下表所示。

参数		说明
发送短信方式		设置将 WAF 的报警信息转变成手机短信的服务器类型。可选项：短信网关协议类型、数据库类型。
短信网关协议类型	协议型号	可选项：中国移动 V2、中国移动 V3、中国联通、中国电信。
	服务器地址	设置短信网关的 IP 地址。
	端口	设置短信网关端口号。取值范围：1-65535。
	账户名	设置短信网关的登录账户名。
	账号密码	设置短信网关登录账户对应的密码。
	SP 接入号	设置移动、电信或联通运营商的短信接入号。
	业务代码	设置移动、电信或联通运营商的短信业务代码。
	超时时间	设置连接超时时间。单位：秒；取值范围：5-30。
数据库类型	数据库类型	可选项。Mysql、SqlServer
	服务器地址	设置数据库服务器的 IP 地址。
	端口	设置数据库服务器使用的端口。
	数据库名	设置数据库名。
	账户名	设置数据库的登录账户名。

参数		说明
	账号密码	设置数据库登录账号对应的密码。
	数据库字符编码	设置 TopWAF 所连接的数据库服务器的编码方式。 可选项：utf-8、gbk。
	超时时间	设置连接超时时间。单位：秒；取值范围：5-30。
	SQL 插入语句模板	SQL 插入语句需要根据实际的数据库编写，然后将手机号码和短信内容字段的值替换成变量$PHONE 和 $CONTENT 即可。 SQL 插入语句填写说明： 1)在自定义插入语句模板的 values 中必须使用**$PHONE** 和**$CONTENT** 两个变量代替手机号码字段的值和短信内容字段的值，这个两个变量在真正的插入语句中会替换成用户的手机号和网关产生的短信验证码内容。其它必须的字段名和其对应的默认值由用户填写。 2）自定义 SQL 插入语句模板的实例：假设用户配置的数据库表名为 sms_send，插入语句中必须的字段有 SM_ID、SRC_ID、MOBILES、CONTENT、SEND_TIME，分别表示发送序号（默认值为 0），源 ID（默认值为 1），手机号码，发送内容，发送时间（默认为空，立即发送）。则自定义的模板语句如下： insert into sms_send(SM_ID, SRC_ID, **MOBILES**, **CONTENT**, SEND_TIME) values('0', '1', '**$PHONE**', '**$CONTENT**', '')。

✧ 在设置短信服务时，配置的认证参数需与实际的短信网关或数据库服务器保持一致。

2）点击【应用】按钮，完成短信服务的配置。

3）在“接收信息手机”参数文本框中输入手机号码，点击【测试】按钮，该手机会接收到测试短信。

CLI 方式

waf alarm-policy add name <*mstring*> **[alarm-type**<mail|sms>**]** [**mail-policy** <*mstring*>| **telnum**< *mstring*>**] [events** <*mstring*>] [**level** <low|medium|high>] [**subject** <*mstring*>] [**schedule** < hourly|daily|weekly>] [**interval** <*num*>] [**attime** <*time*>] [**weekdays** <*mstring*>]

命令描述：

添加告警策略。

可使用 **waf alarm-policy delete** 命令删除告警策略。

可使用 **waf alarm-policy modify** 命令修改告警策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置告警策略名称。 字符串类型，不以“\\”结尾、或不包含“<script>”的字符串。
alarm-type<mail|sms>	设置报警方式。 邮件报警|短信报警
mail-policy <*mstring*>	**alarm-type** 设置为邮件报警方式时，该参数必选，设置引用的邮件策略名称。关于邮件策略的配置具体请参见 5.5 邮件策略。
telnum< *mstring*>	**alarm-type** 设置为手机报警方式时，该参数必选。设置接收报警消息的手机号码。
events <*mstring*>	可选项，设置告警的攻击类型。 字符串类型，可选项包括：xss、scanner、sqli、osi 等。可使用 **waf enumeration alarm-events** <cr>命令查看 TopWAF 告警策略支持的所有事件类型。
level <low|medium|high>	可选项，设置告警级别。 低|中|高，默认值：中。
subject <*mstring*>	可选项，设置邮件的标题。 字符串类型，不以“\\”结尾、或不包含“<script>”的字符串。默认值：“TopWAF 攻击告警报告”。
schedule <hourly|daily|weekly>	可选项，设置定期发送告警计划。 每小时发送|每日发送|每周发送，默认为每小时发送。
interval <*num*>	当 **schedule** 参数设置为 hourly 时，该参数可选。设置告警信息周期发送告警信息的时间间隔，在一个定时发送周期内，如果设备产生告警信息，将发送告警邮件到指定的收件人。 实数类型，单位：小时；取值范围：1-24；默认值：2。
attime <*time*>	当 **schedule** 参数设置为 daily 或 weekly 时，该参数可选，设置 schedule 为发送报警信息的具体时间。 字符串类型，形式为：“小时：分钟：秒”，如 08:12:30。
weekdays <*mstring*>	当 **schedule** 参数设置为 weekly 时，该参数可选。设置每周哪些星期发送报警信息。 可选项包括：mon、tue、wed、thu、fri、sat、sun，可同时设置多个，多个星期中间用逗号“,”分隔。如“mon,tue”，表示星期一和星期二。

命令示例：

添加名称为 alarm-policy 的告警策略，每周的周日和周一的 23:12:12 定时发送告警信息。

TopsecOS# **waf alarm-policy add name** *alarm-report* **schedule** *weekly* **weekdays** *mon,sun* **attime** *23:12:12*

waf alarm-policy show [**name** <*mstring*>]

命令描述：

查看告警策略配置信息。

参数说明：

参数	说明
name <*mstring*>	可选项，设置告警策略名称。 字符串类型，不以“\\”结尾、或不包含“<script>”的字符串。

命令示例：

查看 alarm-report 告警策略的配置信息。

TopsecOS # **waf alarm-policy show name** *alarm-report*

Alarm Name : alarm-report

Interval : 2

Schdule : weekly

Weekdays : mon,sun

Events : xss,csrf,sqli

Fix Send Time: 23:12:12

Level : medium

Send type : mail

Subject : TopWAF 攻击告警报告

Mail Policy :

waf enumeration alarm-events <cr>

命令描述：

查看邮件策略支持的告警事件类型。

命令示例：

TopsecOS# **waf enumeration alarm-events**

type:xss	Description: 跨站脚本攻击
type:scanner	Description: 漏洞扫描攻击
type:sqli	Description: SQL 注入攻击
type:osi	Description: 操作系统命令注入攻击
type:rfi	Description: 远程文件包含攻击
type:dir	Description: 路径遍历攻击
type:leak	Description: 信息泄露攻击
type:ldap	Description: LDAP 注入攻击
type:other	Description: 其他攻击
type:xpath	Description: XPath 注入攻击
type:ssi	Description: SSI 注入攻击
type:server	Description: Web 服务器漏洞攻击
type:webshell	Description: Webshell 检测
type:user	Description: 用户自定义规则命中
type:anomal	Description: 协议异常
type:violation	Description: 协议违规
type:policy	Description: 用户策略限制
type:robots	Description: Robots 防护
type:csrf	Description: 跨站请求伪造攻击
type:cookie	Description: Cookie 篡改攻击
type:stealing	Description: URL 盗窃攻击
type:acl	Description: ACL URL 命中

waf alarm-policy clean <cr>

命令描述：

清除告警策略配置信息。

sms supersms modify type <ismg> **ismg_type** <cmppv2|cmppv3|sgip|smgp> **ip** <*mstring*> **port** <*port*> **username** <*mstring*> **userpasswd** <*mstring*> **[sp_id** <*mstring*>**] [service_id** <*mstring*> **] [enterprise_id** <*mstring*>**] [timeout** <*num*>**]**

命令描述：

设置 TopWAF 通过连接短信网关进行短信报警的认证信息。

参数说明：

参数	说明
type <ismg>	必选项，设置短信服务器的类型为短信网关。
ismg_type <cmppv2|cmppv3|sgip|smgp>	必选项，设置短信网关协议类型。 中国移动 V2|中国移动 V3|中国联通|中国电信。
ip <*mstring*>	必选项，设置短信网关的 IP 地址。 字符串类型，格式为 IP 地址类型。
port <*port*>	必选项，设置短信网关的端口号。 协议端口类型，取值范围：0-65535。
username <*mstring*>	必选项，设置短信网关的登录账号名。 字符串类型。不以'\\'结尾、或不包含"<script>"的字符串。
userpasswd <*mstring*>	必选项，设置短信网关登录账号对应的密码。 字符串类型。不以'\\'结尾、或不包含"<script>"的字符串。
sp_id <*mstring*>	可选项，设置 SP 接入号。 字符串类型。不以'\\'结尾、或不包含"<script>"的字符串。
service_id <*mstring*>	可选项，设置业务代码。 字符串类型。不以'\\'结尾、或不包含"<script>"的字符串。
enterprise_id <*mstring*>	可选项，设置企业代码。 字符串类型。不以'\\'结尾、或不包含"<script>"的字符串。

参数	说明
timeout <*num*>	可选项，设置连接超时时间。 实数类型。单位：秒；取值范围：5-30。

sms supersms modify type <db> **db_type** <mssql|mysql> **ip** <*mstring*> **port**<*port*> **db_name** <*mstring*> **username** <*mstring*> **userpasswd** <*mstring*> **[charset** <gbk|utf-8>**] [timeout** <*num*>**]**

命令描述：

设置 TopWAF 通过连接数据库服务器进行短信报警的认证信息。

参数说明：

参数	说明
type <db>	必选项，设置短信服务器的类型为数据库。
db_type <mssql|mysql>	必选项，设置数据库的类型，包括：Mysql、SqlServer。
ip <*mstring*>	必选项，设置数据库所运行主机的 IP 地址。 字符串类型的 IP 地址。
port<*port*>	必选项，设置数据库使用的端口号。 协议端口类型，取值范围：0-65535。
db_name <*mstring*>	必选项，设置数据库名称。 字符串类型。不以'\\'结尾、或不包含"<script>"的字符串。
username <*mstring*>	必选项，设置数据库登录账号。 字符串类型。不以'\\'结尾、或不包含"<script>"的字符串。
userpasswd <*mstring*>	必选项，设置数据库登录账号对应的登录密码。 字符串类型。不以'\\'结尾、或不包含"<script>"的字符串。
charset <gbk|utf-8>	可选项，设置数据库的编码方式，包括 gbk、utf-8。
timeout <*num*>	可选项，设置连接超时时间。 实数类型。单位：秒；取值范围：5-30。

sms supersms test phone <*mstring*>

命令描述：

测试短信网关或数据库是否成功连接。

参数说明：

参数	说明
phone <*mstring*>	必选项，输入接收测试短信的手机号码。

sms supersms show <cr>

命令描述：

显示短信配置信息。

sms supersms show-module <cr>

命令描述：

显示短信模板配置信息。

sms supersms clean <cr>

命令描述：

清除所有的短信配置信息。

5.7 报表策略

TopWAF 支持日报、周报、月报，支持中文、英文两种语言，通过引用邮件策略，可以将生成的 PDF 格式报表发送到指定邮箱，邮件策略的配置具体请参见 5.5 邮件策略。

TopWAF 最多支持添加 128 条报表策略。

WEBUI 方式

步骤4 选择 **Web 防护** > **报表策略**。

步骤5 点击『添加』，弹出“添加”窗口，如下图所示。

在配置报表策略时，各项参数的具体说明如下表所示。

参数	说明
名称	设置报表策略名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
定时发送计划时间表	设置定时发送告警信息的时间。 无：仅在有告警产生时发送告警邮件。 每日：通过设置“定时发送时间”参数，指定每日的指定时间发送报表信息。 每周：通过设置“星期集合”和“定时发送时间”参数，设置在指定的星期及时间发送报表信息。

参数	说明
	每月：通过设置“日期集合”和“定时发送时间”参数，设置在指定的日期及时间发送报表信息。
报表语言	设置报表的语言，可选项：中文、英语。
邮件标题	设置告警邮件的标题，默认值：TopWAF 报表。
邮件内容	设置告警邮件的内容，默认值：TopWAF 报表信息。
邮件策略名	选择通过邮件发送告警信息的报表策略，关于邮件策略的配置具体请参见 5.5 邮件策略。

步骤6 参数配置完成后，点击【确定】按钮，完成报表策略的配置。

CLI 方式

waf report-policy add name <*mstring*> [**mail-policy** <*mstring*>] [**schedule** <none|daily|weekly|monthly>] [**weekdays** <*mstring*>] [**monthdays**<*mstring*>] [**attime** <*time*>] [**formats** <pdf>] [**title** <*mstring*>] [**body** <*mstring*>] [**language** <english|chinese>]

命令描述：

添加报表策略。

可使用 **waf report-policy delete** 命令删除报表策略。

可使用 **waf report-policy modify** 命令修改报表策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置报表策略名称。 字符串类型，支持数字、字母、中文和特殊字符“_-*.”，不以“\\”结尾且不包含“<script>”字符串。
mail-policy <*mstring*>	可选项，设置引用的邮件策略名称。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。
schedule<none|daily|weekly|monthly>	可选项，设置定期发送告警计划（无|每日发送|每周发送|每月），默认为无，表示不定期发送告警信息。
weekdays <*mstring*>	可选项，设置 **schedule** 为每周发送时，设置该参数，设置每周定时发送时间。

参数	说明
	字符串类型，不以“\\”结尾且不包含“<script>”字符串。支持多输入形式，多个输入用逗号分隔，如“mon,tue”，表示星期一和星期二。
monthdays<*mstring*>	可选项，设置 **schedule** 为每月发送时，设置该参数，设置每月定时发送日期。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。支持多输入形式，多个输入用逗号分隔，如“1,22”，表示每月的 1 日和 22 日。
attime <*time*>	可选项，设置 **schedule** 为每日发送、每周发送或每月发送时，设置该参数，设置每日定时发送时间。 时间类型，表示每日定时发送时间，格式为：“hour:minute:second”，如 08:12:30。
formats <pdf>	可选项，设置报表文件的格式。 只能设置报表文件的格式为 pdf。
title <*mstring*>	可选项，设置邮件的标题。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-127。
body <*mstring*>	可选项，设置邮件内容。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-2047。
language <english|chinese>	可选项，设置报表使用的语言。英语|中文。

命令示例：

添加名称为 report 的报表策略，每周的周日和周一 12:00:00 定时发送报表。

TopsecOS# **waf report-policy add name** *report* **schedule** weekly **weekdays** mon,sun **attime** *12:00:00*

waf report-policy show [**name** <*mstring*>]

命令描述：

查看报表策略配置信息。

命令示例：

查看 report 报表策略的配置信息。

TopsecOS # **waf report-policy show name** *report*

Report Name	report
Time	08:00:00
Schedule	monthly
Weekday	
Mondthday	1
Formats	pdf
Report language	chinese
Title	TopWAF 报表
Body	TopWAF 报表信息。
Mail policy name	

waf report-policy clean <cr>

命令描述：

清除报表策略配置信息。

5.8 漏洞扫描

漏洞扫描用来检测被保护站点存在的安全漏洞，以及安全漏洞的风险等级。管理员可以依据漏洞扫描形成的扫描报告，修复站点的安全漏洞，增强站点的安全性。管理员还可以把扫描报告导入 TopWAF 自动生成对应的防护规则，具体请参见 5.2.14.2 漏洞扫描报告生成防护策略。

WEBUI 方式

步骤5 选择 **Web 防护** > **漏洞扫描**，激活“漏洞扫描”页签。

步骤6 点击『添加』，弹出“添加”窗口，如下图所示。

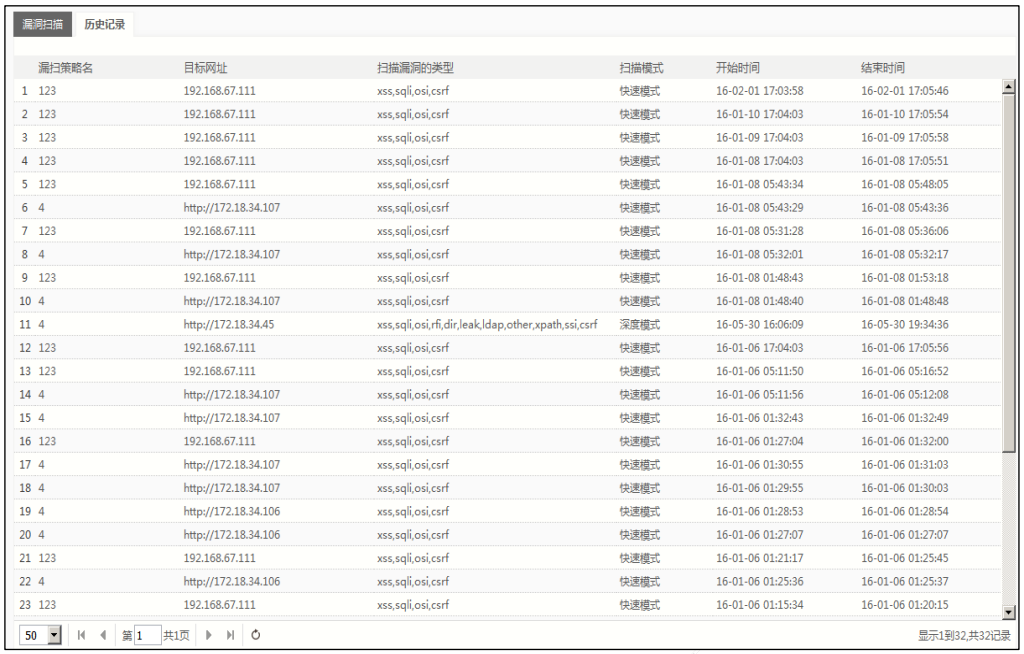
在配置漏洞扫描时，各项参数的具体说明如下表所示。

参数	说明
名称	设置漏洞扫描名称，字符形式，支持数字、字母、中文和特殊字符“_-*.”。
目标网址	设置漏洞扫描的 URL 地址。
扫描漏洞的类型	设置漏洞扫描的类型。 全选：选择所有的攻击类型。 反选：选择除已勾选的攻击类型外的攻击类型。 关于攻击类型的配置具体请参见 5.2.6 防护策略。
扫描的模式	选择漏洞扫描方式。 快速模式：快速扫描只扫描规则库中较为常见的漏洞，扫描耗时短。 深度模式：深度扫描对服务器进行全面扫描，扫描规则库中支持的漏洞扫描类型，扫描耗时长。

参数	说明
报告的文档类型	设置输出的报告文档类型，可选项：html、pdf、txt 和 xml。
扫描周期	设置漏洞扫描策略生效时间。 无：不进行周期性扫描，需要用户配置完成后，在漏洞扫描任务所在行，点击状态操作按钮，启动漏洞扫描。 每日：通过设置“定时扫描开启时间”参数，指定每日的指定时间扫描漏洞。 每周：通过设置“星期集合”和“定时扫描开启时间”参数，设置在指定的星期及时间扫描漏洞。 每月：通过设置“日期集合”和“定时扫描开启时间”参数，设置在指定的日期及时间扫描漏洞。
启用认证	设置是否开启邮件认证功能。默认为“”，表示已关闭，点击该按钮将显示“”，表示已开启。
用户名	启动“启用认证”后才能设置该参数值。用于发送报警信息的电子邮件用户名，必须是 SMTP 服务器的合法帐户。
密码	启动“启用认证”后才能设置该参数值。 设置发件人帐户对应的密码。
邮件策略名	选择通过邮件发送告警信息的漏洞扫描，关于漏洞扫描的配置具体请参见 5.5 邮件策略。
邮件标题	设置告警邮件的标题，默认值：TopWAF 漏洞扫描报告。
邮件内容	设置告警邮件的内容，默认值：TopWAF 漏洞扫描结果。由漏洞扫描进程发送。

步骤7 参数配置完成后，点击【确定】按钮完成漏洞扫描策略的添加。对于已经成功添加的策略，管理员可以进行编辑、下载和删除操作。

步骤8 在本页面激活“历史记录”页签，可查看漏洞扫描的历史记录，如下图所示。



CLI 方式

waf vulnerability-scan-policy add name <*mstring*> **url** <*mstring*> [**scantype** <*mstring*>] [**mode** <fast|deep>] [**formats** <*mstring*>] [**schedule** <none|daily|weekly|monthly>] [**attime** <*time*>] [**weekdays** < *mstring*>] [**mondays** < *mstring*>] [**auth** <on|off>] [**auth-username** < *mstring*>] [**auth-passwd** < *mstring*>] [**mail-policy** < *mstring*>] [**subject** <*mstring*>] [**body** <*mstring*>] [**auth-domain** <*mstring*>]

命令描述：

添加漏洞扫描策略。

可使用 **waf vulnerability-scan-policy delete** 命令删除漏洞扫描策略。

可使用 **waf vulnerability-scan-policy modify** 命令修改漏洞扫描策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置漏洞扫描策略名称。 字符串类型，支持数字、字母、中文和特殊字符“_-*.”，不以“\\”结尾且不包含“<script>”字符串。
url <*mstring*>	必选项，设置扫描的网站地址。 字符串类型，支持 IP 地址和 URL 域名形式，不以“\\”

参数	说明
	结尾且不包含“<script>”字符串。
scantype <*mstring*>	可选项，设置扫描漏洞的类型。 字符串类型，可选项：xss、csrf、sqli、osi、rfi、dir、leak、ldap、xpath、ssi、other、。支持多个输入形式，多个输入间用逗号分隔，例如“xss,csrf”。可使用可使用 **waf enumeration scantypes** <cr>命令查看 TopWAF 支持的告警策略支持的事件类型。
mode <fast|deep>	可选项，设置扫描模式。快速扫描|深度扫描，默认值：快速扫描。
formats <*mstring*>	可选项，设置报表文件的格式。 字符串类型，可选项：html、pdf、txt 和 xml。
schedule <none|daily|weekly|monthly>	可选项，设置定期扫描计划。无|每日发送|每周发送|每月发送，默认为无，表示不进行定扫描。
attime <*time*>	可选项，设置 **schedule** 为每日发送、每周发送或每月发送时，设置该参数，设置每日定时发送时间。 时间类型，格式为：“hour:minute:second”，如 08:12:30。
weekdays <*mstring*>	可选项，设置 **schedule** 为每周发送时，设置该参数，设置每周定时发送时间。 字符串类型，表示星期，可选项：mon、tue、wed、thu、fri、sat、sun，分别表示星期一、星期二、星期三、星期四、星期五、星期六、星期日。支持多输入形式，多个输入用逗号分隔，如“mon,tue”，表示星期一和星期二。
mondays < *mstring*>	可选项，设置 schedule 为每月发送时，设置该参数，设置每月定时发送时间。 字符串类型，取值范围：1-31，支持多输入形式，多个输入用逗号分隔，如“1,22”，表示每月的 1 日和 22 日。
auth <on|off>	可选项，设置是否开启邮件认证开关。 开启|关闭，默认值：关闭。
auth-username<*mstring*>	可选项，设置“auth”为 on 后，可设置发件人帐户对应的用户名。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-63。
auth-passwd <*mstring*>	可选项，设置“auth”为 on 后，可设置发件人帐户对应的用户密码。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-127。
mail-policy <*mstring*>	可选项，设置引用的邮件策略名称。 字符串类型，不以“\\”结尾且不包含“<script>”字

参数	说明
	符串。
subject <*mstring*>]	可选项，设置邮件的标题。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。长度范围：1-127；单位：字符；默认值：“TopWAF 攻击告警报告”。
body <*mstring*>	可选项，设置邮件内容。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-2047。
auth-domain <*mstring*>	必须项，设置认证 domain。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。单位：字符；长度范围：1-255。

命令示例：

添加一条名称为“v-report”的漏洞扫描策略，指定漏洞扫描指定的服务器地址为 192.168.3.3，每周的周日和周一的 23:12:12 定时扫描。

TopsecOS# **waf vulnerability-scan-policy add name** *v-report* **url** 192.168.3.3 **schedule** weekly **weekdays** *mon,sun* **attime** *23:12:12*

waf vulnerability-scan-policy show [**name** <*mstring*>]

命令描述：

查看漏洞扫描策略配置信息。

命令示例：

查看 v-policy 漏洞扫描策略的配置信息。

TopsecOS# **waf vulnerability-scan-policy show name** *v-policy*

profile Name: v-policy

Url: 2.3.3.3

Leaktype: xss,csrf,sqli,osi

Authenticate: off

Mode: fast

```
Schedule:          weekly
Formats:           pdf,xml
Attime:            23:12:12
Weekdays:          mon,sun
Monthdays:
Subject:           TopWAF 漏洞扫描报告
Body:              TopWAF 漏洞扫描结果。由漏洞扫描进程发送。
Username:
Password:
Auth domain:
Mailpolicy:
```

waf enumeration scantypes <cr>

命令描述：

查看漏洞扫描支持的漏扫类型。

命令示例：

```
TopsecOS# waf enumeration scantypes
type:xss          Description:  跨站脚本攻击
type:sqli         Description:  SQL 注入攻击
type:osi          Description:  操作系统命令注入攻击
type:rfi          Description:  远程文件包含攻击
type:dir          Description:  路径遍历攻击
type:leak         Description:  信息泄露攻击
type:ldap         Description:  LDAP 注入攻击
type:other        Description:  其他攻击
type:xpath        Description:  XPath 注入攻击
type:ssi          Description:  SSI 注入攻击
type:csrf         Description:  跨站请求伪造攻击
```

waf vulnerability-scan-policy clean <cr>

命令描述：

清除漏洞扫描策略配置信息。

waf vulnerability-scan-policy start name <*mstring*>

命令描述：

启动漏洞扫描策略。

waf vulnerability-scan-policy stop name <*mstring*>

命令描述：

停止漏洞扫描策略。

waf vulnerability-scan-policy history <cr>

命令描述：

查看漏洞扫描历史记录。

5.9 网页防篡改

网页防篡改防止攻击者恶意修改被保护站点网页、脚本、图片、数据库等任何类型的文件。解决了网站被恶意修改的问题，维护政府和企业形象，保障互联网业务的正常运营。

TopWAF 将被保护网站的文件备份在系统存储区中，提取了被保护文件的指纹并存入了指纹库，TopWAF 的防篡改模块定期和 Web 服务器通讯，轮询受保护文件的指纹，如果指纹发生变化，则根据管理员的配置采取报警或自动恢复机制。有效的做到了篡改预防以及篡改后的修复。

TopWAF 最多支持添加 16 条受保护网站防篡改策略。

WEBUI 方式

步骤1 选择 **Web 防护** > **网页防篡改** > **全网站防篡改**。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。

在配置受保护网站防篡改策略时，各项参数的具体说明如下表所示。

参数	说明
名称	设置网页防篡改策略名称，字符形式，支持数字、字母和特殊字符“_-*.”。
是否开启	设置是否开网页防篡改功能。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
网站的 IP 地址	设置网页防篡改策略保护的网站 IP 地址。
FTP 端口	设置 FTP 端口号，默认值：21。

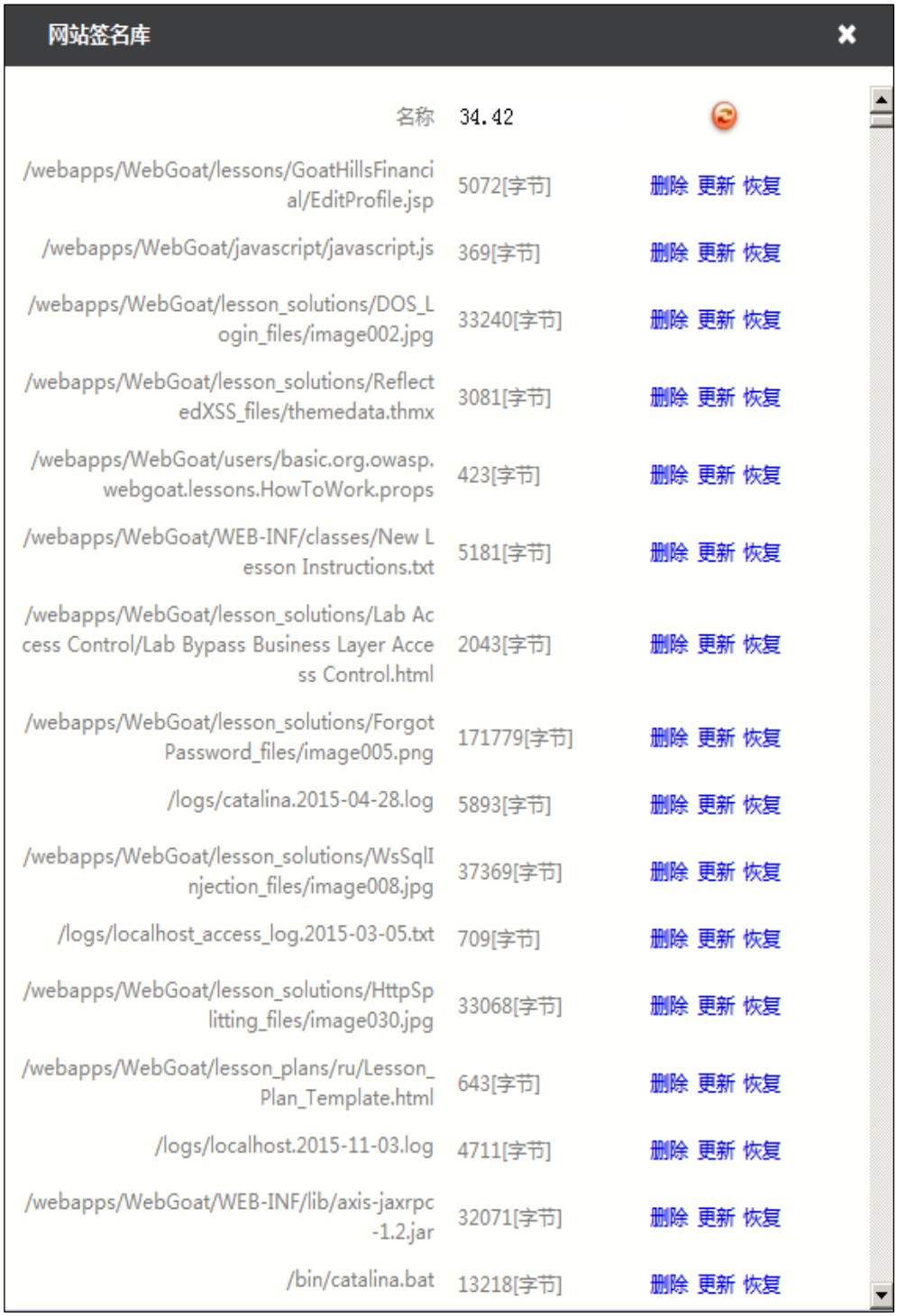
参数	说明
FTP 用户	设置 FTP 用户名称。
FTP 密码	设置 FTP 用户密码。
网站所在目录	设置网站所在 FTP 的文件路径。
FTP 测试	配置完“网站的 IP 地址”、“网站所在目录”、“FTP 用户”和“FTP 密码”后，可点击【FTP 测试】按钮，测试网站路径是否可达。如果网站路径可达将弹出“ftp 测试成功”的提示窗口，点击【确定】按钮关闭该窗口；如果网站路径不可达，将弹出“ftp 测试连接失败，请检查输入的 IP 地址或者端口是否有误”的错误提示信息。
动作	设置检测到网页已被篡改时的动作。可选项：报警和自动恢复。 报警：产生告警日志信息，但是不恢复被篡改的界面，关于告警日志的查看，具体请参见 4.2.1 日志查看。 自动恢复：将被篡改的网页恢复为篡改前的网页。
保护目录深度	设置从网站所在目录防护的目录层级数。取值范围：1-5；默认值：5。
保护单文件最大值	设置被保护的网站路径下，文件的大小的最大值，单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节。 说明： 单位不区分大小写。
不保护的文件类型	设置不被保护的文件类型，字符串类型，扩展名形式，如 PDF 文档的扩展名为“pdf”。
网站根目录轮询时间	设置对网站根目录进行网页防篡改功能检查的时间周期，单位：秒；默认值：10。
网站其它目录轮询时间	设置对网站除根目录外的路径进行网页防篡改功能检查的时间周期，单位：秒；默认值：600。

步骤3 参数配置完成后，点击【确定】按钮，完成受保护网站防篡改策略的配置。

✧ 为防止设备重启后，因网站签名库与策略不匹配导致网站页面被恢复为错误内容，编辑后请保存配置。

步骤4 选中受保护网站防篡改策略，点击『查看状态』，在弹出的“查看状态”窗口中，可查看防护策略的工作状态。

步骤5 选中受保护网站防篡改策略，点击『网站签名库』，在弹出的“网站签名库”窗口中，查看网站特征指纹库状态，如下图所示。



CLI 方式

waf anti-tamper web add name <*nstring*> [**enable** <on|off>] **ip** <*nstring*> [**ftpport** <*num*>] [**ftpuser** <*mstring*>] [**ftppass** <*mstring*>] [**dir** <*string*>] [**depth** <*num*>] [**maxsize** < *string*>] [**notype** < *mstring*>] [**rootchktime** <*num*>] [**otherchktime** <*num*>] [**action** <alert|resume>]

命令描述：

添加网页防篡改策略。

可使用 **waf anti-tamper web delete** 命令删除网页防篡改策略。

可使用 **waf anti-tamper web modify** 命令修改网页防篡改策略。

参数说明：

参数	说明
name <*nstring*>	必选项，设置网页防篡改策略名称。 字符串类型，支持数字、字母和特殊字符“_-*.”，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
enable <on|off>	设置是否开启网页防篡改功能。 开启|关闭，默认值：开启。
ip <*nstring*>	必选项，设置网页防篡改策略保护的网站 IP 地址。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
ftpport <*num*>	可选项，设置 FTP 端口号，实数类型。
ftpuser <*mstring*>	可选项，设置 FTP 用户名。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。
ftppass <*mstring*>	可选项，设置 FTP 用户密码。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。
dir <*string*>	可选项，设置网站所在 FTP 的路径。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。
depth <*num*>	可选项，设置从网站所在目录防护的目录层级数。 实数类型，取值范围：1-5；默认值：5。
maxsize <*string*>	可选项，设置被保护的网站路径下，文件的大小的最大值。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。单位：字节、K、M、G，其中 K 表示千字节，M 表示兆字节，G 表示吉字节；默认值：4M。 说明： 单位不区分大小写。
notype <*mstring*>	可选项，设置不被保护的文件类型。 字符串类型，扩展名形式，如 PDF 文档的扩展名为“pdf”，不以“\\”结尾且不包含“<script>”字符串。
rootchktime <*num*>	可选项，设置对网站根目录进行网页防篡改功能检查的时间周期。 实数类型，单位：秒；默认值：600。

参数	说明
otherchktime <*num*>	可选项，设置对网站除根目录外的路径进行网页防篡改功能检查的时间周期。 实数类型，单位：秒；默认值：600。
action <alert|resume>	可选项，设置检测到网页已被篡改时的动作。 alert：报警，产生告警日志信息，但是不恢复被篡改的界面，关于告警日志的查看，具体请参见 4.2.1 日志查看。 resume：自动恢复，将被篡改的网页恢复为篡改前的网页。

命令示例：

添加名称为 test 的网页防篡改策略，指定网站的地址为 192.168.3.3。

TopsecOS# **waf anti-tamper web add name** *test* **ip** *192.168.3.3*

waf anti-tamper web show [**name** <*nstring*>]

命令描述：

查看网页防篡改策略配置信息。

命令示例：

TopsecOS# **waf anti-tamper web show**

ID:8350 name:test ip:192.168.3.3 ftpport:21 ftpuser:anonymous ftppass: dir:/ depth:5 maxsize:4m notype: rootchktime:10 otherchktime:600 enable:on action:alert

waf anti-tamper web status name <*nstring*>

命令描述：

查看网页防篡改策略状态信息。

命令示例：

TopsecOS# **waf anti-tamper web status name** *123*

offline monitoring...

waf anti-tamper web clean<cr>

命令描述：

清除网页防篡改策略配置信息。

waf anti-tamper disk status <cr>

命令描述：

查看网页防篡改功能可使用空间。

命令示例：

TopsecOS# **waf anti-tamper disk status**

134217727 (k) left.

waf anti-tamper file resume name <*nstring*> **file** <*mstring*>

命令描述：

恢复指定路径上被篡改的网页。

参数说明：

参数	说明
name <*nstring*>	必选项，指定恢复网页所使用的防篡改策略的名称。 字符串类型，支持数字、字母和特殊字符“_-*.”，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
file <*mstring*>	必选项，设置网站文件名称。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 名称包括网站文件目录，例如“/root/added”，表示 root 路径下的 added 文件。

命令示例：

TopsecOS# **waf anti-tamper file resume name** *test* **file** /site

waf anti-tamper network status name <*nstring*>

命令描述：

查看网站的工作状态。

命令示例：

TopsecOS# **waf anti-tamper network status name** *test*

Network connection: occurred exception, please check your network

Logining or other operation of the server: occurred exception, please check your username ,password, or configuration

File resume: ok

Web dbsign: ok

enable: on

resume times: 0

file counts: 41

file total size: 18413542 Byte

waf anti-tamper signdb update name <*nstring*> **[file** <*mstring*>]

命令描述：

更新网站特征指纹库。

参数说明：

参数	说明
name <*nstring*>	可选项，设置网页防篡改策略名称。 字符串类型，支持数字、字母和特殊字符“_-*.”，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
file <*mstring*>	必选项，设置网站文件名称。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。名称包括网站文件目录，例如“/root/added”，表示 root 路径下的 added 文件。

命令示例：

TopsecOS# **waf anti-tamper signdb update name** *test* **file** /test/123

waf anti-tamper signdb delete name <*nstring*> **file** <*mstring*>

命令描述：

删除网站特征指纹库。

参数说明：

参数	说明
name <*nstring*>	必选项，指定要删除的网页防篡改策略的名称。 字符串类型，支持数字、字母和特殊字符“_-*.”，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
file <*mstring*>	必选项，设置网站文件名称。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。名称包括网站文件目录，例如“/root/added”，表示 root 路径下的 added 文件。

命令示例：

TopsecOS# **waf anti-tamper signdb delete name** *test* **file** /test/123

waf anti-tamper signdb show name <*nstring*>

命令描述：

查看网站特征指纹库。

命令示例：

TopsecOS# **waf anti-tamper signdb show name** *test*

/root/test/ljjkk 16

/root/added 11

/test.pdf 7

/touch 13

/tamper_file 36

/fdsa/add2_other 8

/deleted_file 85

/fdsa/added2_file_other 8

/add_filed 4

/root/kk 12

6 网络层防护

TopWAF 的网络层防护是保护 Web 服务器免受来自网络层的攻击，并且保证客户端的正常访问请求。主要内容包括：

- 资源对象：主要介绍如何添加 TopWAF 的对象资源，用于在配置访问控制时进行引用。
- 访问控制：主要介绍如何配置 TopWAF 的访问控制策略。
- DDOS 防御：主要介绍如何配置 DDoS 防护策略，检测数据流量中的 HTTP 报文和 HTTPS 报文，及时发现并阻断威胁攻击，需要在服务器策略中引用才能生效。
- 防火墙联动：主要介绍如何配置 TopWAF 与防火墙进行联动，并查看防火墙联动状态。

6.1 资源对象

对象，是具备某些公共特征的一些实例的集合，是访问控制策略的重要组成部分。某一对象资源可以被其他对象所引用，合理地构建和管理对象资源能够大大简化管理员对 TopWAF 的管理工作，当某个对象发生变化时，管理员只需要修改对象本身即可，而无需逐一地修改所有引用该资源的策略。

在 TopWAF 中，管理员可以定义的资源对象的类型包括：

- 区域：通过与接口绑定，定义区域的访问权限。
- 地址：包括主机对象、地址范围对象、子网对象和地址组。
- 服务：包括 TopWAF 预定义的服务对象和管理员自定义的服务对象。

6.1.1 区域

区域，设置接口所属的安全域，是一个或多个接口的集合，以供访问控制模块调用。TopWAF 通过区域划分网络、标识报文的传输路径，当报文在不同的区域之间进行传输时，触发安全策略的检查。

TopWAF 支持区域对象的设置，管理员可以根据实际情况，将网络划分为不同的安全区域，并根据其不同的安全需求，定义相应的规则进行区域边界防护。可通过本机服务功能设置用户是否具有该服务的访问权限，关于本机服务的配置具体请参见 8.1.3 本机服务。

WEBUI 方式

步骤1 选择 **网络层防护** > **资源对象** > **区域**。

步骤2 点击『添加』，弹出“添加”窗口。如下图所示。

在设置区域对象时，各项参数的具体说明如下表所示。

参数	说明
区域名称	必选项，设置区域对象名称。
描述	设置必要的说明信息。最多可输入 125 个字节。
区域	必选项，点击『添加』选择与该区域绑定的接口，可同时选择一个或多个接口。接口的设置请参见 7.1 接口。

步骤3 点击【确定】按钮完成区域对象的添加。

CLI 方式

define area add name <*nstring*> **interface** <*mstring*> [**comment** <*wstring*>]

命令描述：

添加一个区域对象。

参数说明：

参数	说明
name <*nstring*>	必选项，设置区域对象名称。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。
interface <*mstring*>	必选项，指定接口。 字符串类型。
comment <*wstring*>	可选项，设置对区域对象的具体说明。 字符串类型。不包含"<>\\"中任意字符。

命令示例：

添加一个与接口 feth0 绑定的区域 area_feth0。

TopsecOS# **define area add name** *area_feth0* **interface** *feth0* **comment** *comment_conten*

define area delete name <*nstring*>

命令描述：

删除一个区域对象。如果该区域被规则引用，则无法删除。

参数说明：

参数	说明
name <*nstring*>	必选项，指定要删除的区域对象名称。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。

命令示例：

TopsecOS# **define area delete name** *area_feth 0*

define area show [**name** <*nstring*>]

命令描述：

显示 TopWAF 系统中的区域对象。

参数说明：

参数	说明
name <*nstring*>	可选项，指定要显示的区域对象名称。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。

命令示例：

TopsecOS# **define area show**

ID 10065 define area add name area_feth0 interface 'feth0 ' refered 5

ID 10066 define area add name 23 interface 'feth0 ' comment ' ' refered 2

ID 10067 define area add name 3453525 interface 'feth3 ' comment ' ' refered 0

6.1.2 地址

地址对象是 IPv4 地址或 IPv6 地址的集合，地址组是地址的集合。在 TopWAF 系统中，地址对象是 TopWAF 访问控制规则模块配置的重要组成元素，它包含一个或若干个 IPv4 或 IPv6 地址，只需定义一次即可被引用。

按照网络地址的表达方式，可以将四种类型的地址加入到地址对象中：

主机地址：可以唯一标识网络中的主机。

- 范围地址：若干个主机 IP 的集合，这些 IP 地址是连续的。

- 子网地址：若干个主机 IP 的集合，它与范围地址的区别在于：不是通过起始 IP 和终止 IP 来指定地址范围，而是通过 IP 地址和网络掩码来共同确定。如子网地址“192.168.1.0/24”，表示 IP 范围为“192.168.1.1-192.168.1.255”。

✧ 地址对象的成员不能同时包含 IPv4 地址和 IPv6 地址。

WEBUI 方式

步骤1 选择 **网络层防护** > **资源对象** > **地址**，激活“地址”页签。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。

在添加地址对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置地址对象的名称。
主机	必选项，地址类型选择“主机”，点击『添加』在文本框中输入该主机对象的 IP 地址。 说明： 主机地址支持 IPv4 和 IPv6 版本，其中 IPv6 格式为：

参数	说明
	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。
范围	必选项，地址类型选择“范围”，点击『添加』在文本框中输入地址范围的起始 IP 地址和终止 IP 地址。 说明： 地址范围的起始 IP 和终止 IP 地址支持 IPv4 和 IPv6 版本，其中 IPv6 格式为：xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。
子网	必选项，地址类型选择“子网”，点击『添加』在文本框中输入子网对象的 IP 地址和子网掩码地址。 说明： 子网地址支持 IPv4 和 IPv6 版本，其中 IPv6 格式为：xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。

步骤3 点击【确定】按钮完成地址对象的添加。

CLI 方式

define host add name <*nstring*> **ipaddr** <*mstring*>

命令描述：

添加一个主机地址对象。

参数说明：

参数	说明
name <*nstring*>	必选项，设置要添加的主机地址对象的名称。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。
ipaddr <*mstring*>	可选项，设置主机对象的 IP 地址。 字符串类型，表示 IP 地址，格式为：192.168.1.6，可以为一个或多个 IP 地址，多个时用单引号括起来，之间用空格分隔’192.168.83.1 192.168.1.6’。不以'\\'结尾或不包含"<script>"字符串。

命令示例：

添加一个主机 host1，并设定其 IP 地址为 192.168.1.8。

TopsecOS# **define host add name** *host1* **ipaddr** *192.168.1.8*

define host show [**name** <*nstring*>]

命令描述：

查看所有主机地址对象。

参数说明：

参数	说明
name <*nstring*>	必选项，设置要添加的主机对象的名称。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。

命令示例：

TopsecOS# **define host show**

ID 10063 define host add name 123 ipaddr '1.1.1.1' refered 1

ID 10064 define host add name add ipaddr '127.0.0.1' refered 0

ID 10185 define host add name host1 ipaddr '127.0.0.1' refered 0

define host delete [id <*num*>**] [name** <*nstring*>**]**

命令描述：

删除一个主机对象。如果该对象被规则引用，则无法删除。

参数说明：

参数	说明
id <*num*>	可选项，指定要删除的主机对象对应的 ID 号。 实数类型。
name <*nstring*>	可选项，指定要删除的主机对象的名称。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。

使用说明：

在删除主机对象时，既可根据主机对象的名称来删除，又可以通过主机地址对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除未被策略引用的主机地址对象。

命令示例：

删除主机对象 host1。

TopsecOS# **define host delete name** *host1*

define range add name <*nstring*> **ip1** <*mstring*> **ip2** <*mstring*>

命令描述：

添加一个地址范围对象。

参数说明：

参数	说明
name <*nstring*>	必选项，设置地址范围对象的名称。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。
ip1 <*mstring*>	必选项，设置地址范围的起始 IP 地址。 字符串类型，表示 IP 地址，格式为 x.x.x.x 或 x:x:x:x:x:x:x:x，比如 192.168.1.254 或 2014::3。不以'\\'结尾或不包含"<script>"字符串。
ip2 <*mstring*>	必选项，设置地址范围的结束 IP 地址。 字符串类型，表示 IP 地址，格式为 x.x.x.x 或 x:x:x:x:x:x:x:x，比如 192.168.1.254 或 2014::3。不以'\\'结尾或不包含"<script>"字符串。

使用说明：

ip1 的参数值应不大于 ip2 的参数值，否则就会出现错误提示。

命令示例：

添加地址范围对象 range1，其地址范围为：172.16.1.10-172.16.1.80。

TopsecOS# **define range add name** *range1* **ip1** *172.16.1.10* **ip2** *172.16.1.80*

define range modify name <*nstring*> [**ip1** <*mstring*>] [**ip2** <*mstring*>]

命令描述：

修改一个地址范围资源对象。

参数说明：

参数	说明
name <*nstring*>	必选项。指定待修改的地址范围对象。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。
ip1 <*mstring*>	可选项。设置地址范围的起始 IPv4 或 IPv6 地址。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。
ip2 <*mstring*>	可选项。设置地址范围的结束 IPv4 或 IPv6 地址。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。

命令示例：

修改 range1 对象的 IPv4 地址范围为：172.16.1.10-172.16.1.90。

TopsecOS# **define range modify name** *range1* **ip1** *172.16.1.10* **ip2** *172.16.1.90*

define range delete [name <*nstring*>**] [id** <*num*>**]**

命令描述：

根据名称或 ID 号删除未被引用的地址范围资源对象。

参数说明：

参数	说明
name <*nstring*>	可选项，设置待删除的地址范围资源对象名称。 字符串类型，不包含"!@#$%^&+=|?\"\\'><`~ "中任意字符以及空格。
id <*num*>	可选项，设置待删除的地址范围资源对象的 ID 号。 实数类型。

使用说明：

在删除地址范围对象时，既可根据地址范围对象的名称来删除，又可以通过地址范围对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

命令示例：

删除地址范围对象 range1。

TopsecOS# **define range delete name** *range1*

define range show [name <*nstring*>**]**

命令描述：

显示地址范围资源对象。

参数说明：

参数	说明
name <*nstring*>	可选项，按名字显示某个地址范围资源对象。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

命令示例：

TopsecOS# **define range show**

ID 8011 define range add name r1 ip1 172.16.1.10 ip2 172.16.1.80 refered 0

ID 8012 define range add name r2 ip1 1111::2 ip2 2222::2 refered 0

TopsecOS# **define range show name** *r2*

ID 8012 define range add name r2 ip1 1111::2 ip2 2222::2 refered 0

define range clean <cr>

命令描述：

清空地址范围资源对象。

命令示例：

TopsecOS# **define range clean**

define subnet add name <*nstring*> **ipaddr** <*nstring*> **[mask** <*nstring*>**]**

命令描述：

添加一个子网地址对象。

参数说明：

参数	说明
name <*nstring*>	必选项。设置待添加的子网地址对象名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
ipaddr <*nstring*>	必选项。设置子网 IPv4 或 IPv6 地址。 字符串类型。不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。IPv4 子网地址格式为 x.x.x.x/x，例如 192.168.0.1/24。IPv6 中子网用前缀表示，格式为 xxxx::xxxx/x，例如 2014::1/64。
mask <*nstring*>	可选项，设置子网掩码，用来判断任意两个 IP 地址是否属于同一子网络。 字符串类型，表示 IPv4 子网掩码，例如 255.255.255.0。如果采用 IPv6 地址，不需输入该参数。不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

命令示例：

添加子网对象 subnet1，其子网地址为：192.168.10.1，掩码为：255.255.255.0。

TopsecOS# **define subnet add name** *subnet1* **ipaddr** *192.168.10.1* **mask** *255.255.255.0*

define subnet delete [**name** <*nstring*>] [**id** <*num*>]

命令描述：

根据名称或 ID 号删除未被引用的子网地址对象。

参数说明：

参数	说明
name <*nstring*>	可选项，设置待删除的子网地址对象名称。 字符串类型，不包含“!@#$%^&+=|?\"\\\'> <`~”中的任一字符。
id <*num*>	可选项，设置待删除的子网对象对应的 ID 号。 实数类型。

使用说明：

在删除子网对象时，既可根据子网对象的名称来删除，又可以通过子网对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

命令示例：

删除子网对象 subnet1。

TopsecOS# **define subnet delete name** *subnet1*

define subnet show [**name** <*nstring*>]

命令描述：

显示所有的子网资源对象。

参数说明：

参数	说明
name <*nstring*>	可选项，设置待显示的子网地址对象名称。 字符串类型，不包含“!@#$%^&+=|?\"\\\'> <`~”中的任一字符。

命令示例：

TopsecOS# **define subnet show**

ID 8008 define subnet add name subnet1 ipaddr 192.168.20.0/24 refered 0

ID 8009 define subnet add name subnet2 ipaddr 2200::1/64 refered 0

ID 8010 define subnet add name subnet3 ipaddr 192.168.0.1/24 refered 0

TopsecOS# **define subnet show name** *subnet2*

ID 8009 define subnet add name subnet2 ipaddr 2200::1/64 refered 0

define subnet clean <cr>

命令描述：

清空所有未被引用的子网资源对象。

6.1.2.1 地址组

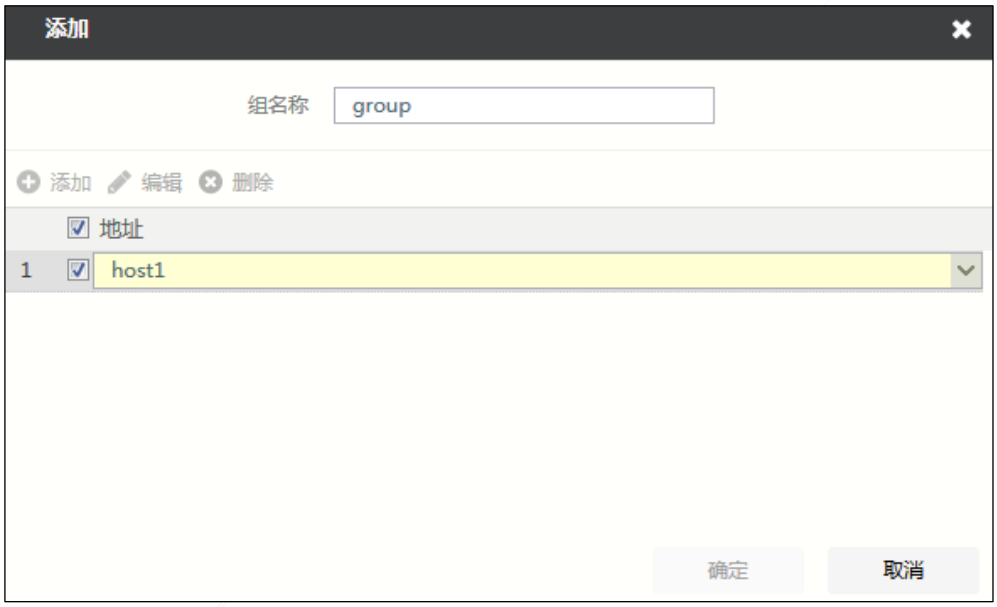
当地址对象包含的成员越来越多时，如果一个访问控制策略需要引用多个地址对象，则管理员配置策略时会比较复杂。因此，TopWAF 支持地址组功能，地址组是一个集合，成员可以是主机地址对象、范围地址对象、子网地址对象和已经定义好的地址对象。与地址对象相比，地址组增强了资源对象管理的层次性，提高了地址管理的灵活度。

✧ 地址组的成员可以是 IPv4 地址、IPv6 地址，也可以同时将 IPv4 地址和 IPv6 地址加入地址组。

WEBUI 方式

步骤1 选择 **网络层防护** > **资源对象** > **地址**，激活“地址组”页签。

步骤2 点击『添加』，弹出“添加”窗口。如下图所示。



在添加地址组对象时，各项参数的具体说明如下表所示。

参数	说明
组名称	必选项，设置地址组对象名称。
地址组成员	必选项，选择地址对象，可同时选择一个或多个地址对象。

步骤3 点击【确定】按钮完成地址组对象的添加。

CLI 方式

define group_address add name <*nstring*> [**member** <*mstring*>]

命令描述：

添加一个地址组对象。

参数说明：

参数	说明
name <*nstring*>	必选项，设置地址组对象的名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
member <*mstring*>	可选项，设置地址组对象中的成员。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。表示地址对象，可以是已经定义的主机对象、子网对象或地址范围对象。

使用说明：

在定义地址组之前，可以先定义地址对象。

命令示例：

添加地址组对象 groupaddr1，其成员为已定义的主机对象 host1。

TopsecOS# **define host add name** *host1* **ipaddr** *192.168.16.3*

TopsecOS# **define group_address add name** *groupaddr1* **member** *host1*

define group_address show <cr>

命令描述：

查看所有地址组对象。

命令示例：

TopsecOS# **define group_address show**

ID 10181 define group_address add name ad12　refered 0

ID 10183 define group_address add name ad34　refered 0

define group_address delete [**id** <*num*>] [**name** <*nstring*>]

命令描述：

删除一个地址组对象。如果该对象被规则引用，则无法删除。

参数说明：

参数	说明
id <*num*>	可选项，指定要删除的地址组对象对应的 ID 号。 实数类型。
name <*nstring*>	可选项，指定要删除的地址组的名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

使用说明：

在删除地址组对象时，既可根据地址组对象的名称来删除，又可以通过地址组对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除所有**未被引用的**地址组对象。

命令示例：

删除地址组 groupaddr1。

TopsecOS# **define group_addrees delete name** *groupaddr1*

define group_address clean <cr>

命令描述：

删除所有未被引用的地址组对象。

命令示例：

TopsecOS# **define group_address clean**

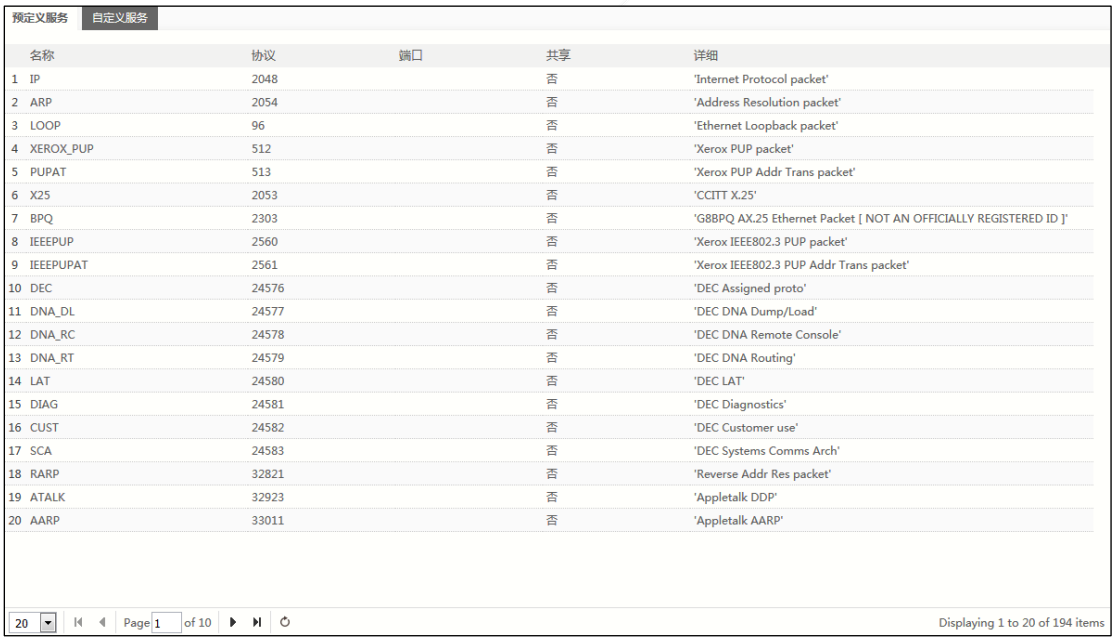
6.1.3 服务

服务对象是 TopWAF 访问控制模块配置的重要组成元素，便于 TopWAF 管理员根据不同的服务指定策略规则。服务对象由协议类型和协议端口号组成，分为以下两类：

- 预定义服务：系统预定义的一些常用服务。
- 自定义服务：根据自身业务的需要自定义的服务和端口号。

6.1.3.1 预定义服务

为方便对用户网络中不同服务的访问控制，系统预先定义了 194 条常见服务供用户在设置访问控制规则时使用。对于这些预定义的服务，用户不可以进行修改和删除，只能通过选择 **网络层防护 > 资源对象 > 服务**，激活“预定义服务”页签来进行查看。如下图所示。



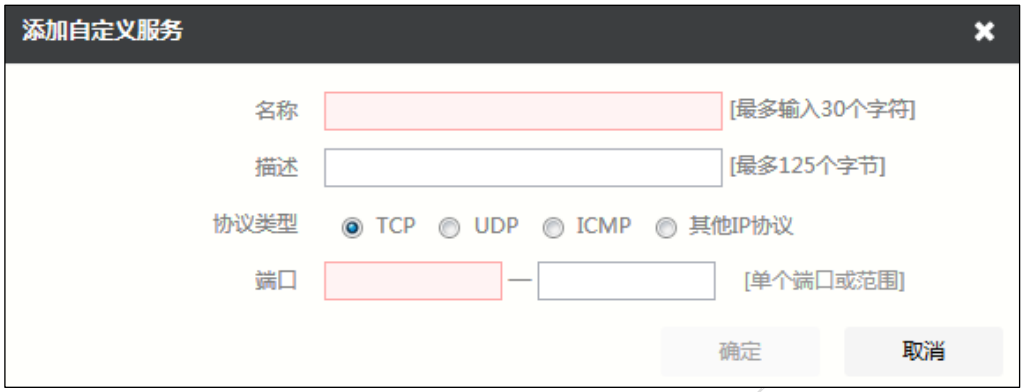
6.1.3.2 自定义服务

为实现对网络中某种服务进行访问控制，但在系统没有预先定义该服务，用户可以根据需要自行定义服务，然后设置 ACL 规则对自定义服务进行控制。

WEBUI 方式

步骤1 选择 **网络层防护** > **资源对象** > **服务**，激活“自定义服务”页签。

步骤2 点击『添加』，弹出“添加自定义服务”窗口。如下图所示。



在设置自定义服务对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置自定义服务对象名，用于在 NGFW 中唯一标识自定义服务对象。名称中不能包含如下特殊字符：%、\、’、 <、>、’、&、“。最多输入 30 个字符。
描述	输入自定义服务对象的描述信息。最多输入 125 个字节。
协议类型	必选项，表示自定义服务使用的协议类型，可选项：TCP、UDP、ICMP 和其他 IP 协议。
端口	当“类型”选择 TCP、UDP、其他 IP 协议时显示该选项。用于输入自定义服务对象占用的单个端口或端口范围，前后两个文本框分别表示起始和终止端口号（端口取值范围：0-65535）。如果是单个端口则只填写起始端口。 说明： 当协议类型为 ICMP 时，需要配置类型值和代码值。类型值取值范围：0-18。 当协议类型为“其他 IP 协议”时，还需要设置协议号。

步骤3 点击【确定】按钮完成服务对象的添加。

CLI 方式

define service add name <*nstring*> **protocol** <*num*> [**port1** <*num*>] [**port2** <*num*>] [**comment** <*wstring*>]

命令描述：

添加一个服务对象。

参数说明：

参数	说明
name <*nstring*>	必选项，设置服务对象名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
protocol <*num*>	必选项，设置 3 层或 4 层协议号。 实数类型。表示协议码。
port1 <*num*>	可选项，设置服务的起始端口，只有一个端口时只须设置起始端口，不用设置结束端口。如果为 ICMP 协议，则表示类型范围。取值范围：0-18。 实数类型，表示起始端口号或 ICMP 协议类型。
port2 <*num*>	可选项，设置服务的结束端口。 实数类型。
comment <*wstring*>	可选项，设置备注内容。 字符串类型。不包含"<>\\"中任意字符。

使用说明：

服务分为系统提供的预定义服务和用户自定义服务，对于预定义服务用户无法进行添加、删除、修改等操作。

命令示例：

添加服务对象 http8080，设置协议号为 6、端口号为 8080。

TopsecOS# **define service add name** *http8080* **protocol** *6* **port1** *8080*

define service modify name <*nstring*> [**protocol** <*num*>] [**port1** <*num*>] [**port2** <*num*>] [**comment** <*wstring*>]

命令描述：

修改一个自定义服务对象。

参数说明：

参数	说明
name <*nstring*>	必选项，设置服务对象名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
protocol <*num*>	可选项，重新设置 3 层或 4 层协议号。 实数类型，表示协议码。
port1 <*num*>	可选项，修改服务的起始端口，只有一个端口时只须设置起始端口，不用设置结束端口。如果为 ICMP 协议，则表示类型范围。取值范围：0-18。 实数类型，表示起始端口号或 ICMP 协议类型。
port2 <*num*>	可选项，修改服务的结束端口。 实数类型。
comment <*wstring*>	可选项，修改备注内容。 字符串类型。不包含"<>\\"中任意字符。

命令示例：

将服务对象 http8080 的端口号改为 8000。

TopsecOS# **define service add name** *http8080* **protocol** *6* **port1** *8080*

TopsecOS# **define service modify name** *http8080* **port1** *8000*

define service delete [id <*num*>] [**name** <*nstring*>]

命令描述：

删除一个自定义服务对象。

参数说明：

参数	说明
id <*num*>	可选项，指定要删除的服务对象对应的 ID 号。 实数类型。
name <*nstring*>	可选项，指定要删除的服务对象的名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

使用说明：

在删除服务对象时，既可根据服务对象的名称来删除，又可以通过服务对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除未被策略引用的服务对象。

命令示例：

删除服务对象 http8000。

TopsecOS# **define service delete name** *http8000*

define service clean <cr>

命令描述：

清空所有未被引用的自定义服务对象。

define service show [**name** <*nstring*>] [**type** <custom|default>]

命令描述：

查看所有服务对象信息。

参数说明：

参数	说明
name <*nstring*>	可选项，按名称显示某个服务对象的信息。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
type <custom|default>	可选项，按类型查看服务对象信息。 自定义服务对象|预定义服务对象。

命令示例：

TopsecOS# **define service show**

ID 8001 define service add name http8080 protocol 6 port1 8080 refered 0

6.2 访问控制

实现包过滤的核心技术是使用访问控制列表（Access Control Lists，简称 ACL）。ACL 包含一组指令列表，这些指令列表表明哪些数据包可以接收、哪些数据包需要拒绝。指令列表是由多条访问控制规则组成的。

访问控制规则，是一组管理员自定义的策略，这些规则可以描述满足哪些条件的报文可以通过 TopWAF，以及满足哪些条件的报文将被 TopWAF 禁止。

6.2.1 原理简介

包过滤的处理过程是先获取 TopWAF 接收到的数据包的报文头信息，然后和访问控制规则进行比较，根据比较的结果对数据包进行转发或者丢弃。

在访问策略中，策略源定义了报文的来源，策略源可以是地址（主机、范围、子网）、区域。当报文的源地址属于策略源的范围，则被认为满足策略源约束条件。策略目的定义了报文的目的地址范围，可以包括一个或多个主机、子网、或范围，也可以包括多个区域（或 VLAN）。策略服务定义了报文采用的网络协议或特定端口号。访问控制定义了 TopWAF 对满足策略的报文所采取的处理方式，包括允许（该报文被允许通过）和禁止（丢弃该包）。一个报文和某一条访问策略匹配指的是：报文的源地址包含于策略源定义、报文目的地址包含于策略目的，以及报文端口包含于策略服务等。只有当一个报文完全符合策略中所规定的所有条件时，这条策略才适用于该报文。

6.2.2 配置访问控制规则

TopWAF 通过访问控制规则的设置对设备各个接口之间的数据转发进行控制。一般情况下，访问控制规则分为两部分：过滤条件和动作，过滤条件由安全域间流量的源安全域/源地址、

目的安全域/目的地址、服务类型等构成；动作包括允许和禁止。策略规则都有其独有的 ID 号，策略规则 ID 会在定义规则时自动生成。TopWAF 的所有策略规则有特定的排列顺序，管理员也可以按照自己的需求设置策略规则的排列位置。策略规则的排列位置可以是绝对位置，即处在首位或者处在末位，也可以是相对位置，即位于某个 ID 之前或之后。在流量进入系统时，系统会将流量与访问控制列表中的策略进行匹配，并对流量按照匹配到的策略的动作进行处理。同时，对于定义的策略规则，TopWAF 提供了对规则的分组管理功能，不同组之间的前后顺序和组内规则的排列顺序共同决定访问控制规则的匹配顺序。

6.2.2.1 配置访问控制策略

WEBUI 方式

在配置访问控制策略之前，需要先配置资源（可选）。关于资源对象的配置具体请参见 0TopWAF 的网络层防护是保护 Web 服务器免受来自网络层的攻击，并且保证客户端的正常访问请求。主要内容包括：

- 资源对象：主要介绍如何添加 TopWAF 的对象资源，用于在配置访问控制时进行引用。
- 访问控制：主要介绍如何配置 TopWAF 的访问控制策略。
- DDOS 防御：主要介绍如何配置 DDoS 防护策略，检测数据流量中的 HTTP 报文和 HTTPS 报文，及时发现并阻断威胁攻击，需要在服务器策略中引用才能生效。
- 防火墙联动：主要介绍如何配置 TopWAF 与防火墙进行联动，并查看防火墙联动状态。

资源对象。

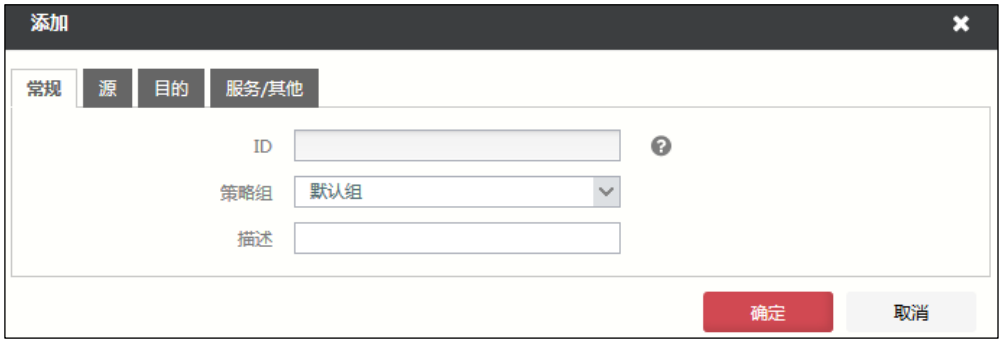
步骤1 选择 **网络层防护** > **访问控制**，进入访问控制界面，如下图所示。

界面显示已添加访问控制策略和策略组的基本内容，如策略 ID、地址、区域、服务等。

策略列表中状态栏显示“✔”表示该策略已启用，选中该策略，点击上方的『禁用』可禁用该策略；反之，策略列表中状态栏显示“✘”表示该策略被禁用，选中该策略，点击上方的『启用』可启用该策略。

步骤2 添加访问控制策略。

1）点击『添加』，选择“策略”，弹出“添加”窗口。如下图所示。



在设置访问控制规则时，各项参数的具体说明如下表所示。

参数	说明
ID	系统自动生成，无需设置。
策略组	设置访问控制规则所属的规则组。
描述	设置对该访问控制规则的必要描述信息。
源	选择对象，设定发起连接的源应当匹配的条件。可以实现基于哪些条件对报文进行访问控制。如果不指定，表示任何源地址均匹配该规则。可设定的选项包括： 1）区域：选择区域资源限定报文的来源区域。 2）地址：选择已定义的地址资源对象，限定报文的源 IP 地址。 说明： 1）多个选项设定的条件之间是“与”的关系，数据包的源地址在匹配规则的时候必须都要匹配上选择的选项，规则才能生效； 2）每一选项均可选择多个对象，多个对象之间是“或”的关系。只要满足其中一个对象即可； 3）当没有设置地址对象时，默认表示任意地址；
目的	选择对象，设定发起连接的目的应当匹配的条件。可以实现基于哪些条件对报文进行访问控制。当设定多项时，必须同时满足各个条件才匹配该规则。如果不指定，表示任何源地址均匹配该规则。可设定的选项包括： 1）区域：选择区域资源限定报文的目的区域。 2）地址：选择已定义的地址资源对象，限定报文的目的 IP 地址。 说明： 1）多个选项设定的条件之间是“与”的关系，数据包的目的地址在匹配规则的时候必须都要匹配上选择的选项，规则才能生效；

参数	说明
	2）每一选项均可选择多个对象，多个对象之间是“或”的关系。只要满足其中一个对象即可； 3）当没有设置地址对象时，默认表示任意地址。
服务	选择服务对象，对数据报文的协议和目的端口号进行限定。如果没有选择任何服务，则系统默认为不对协议和端口号进行限定。
动作	设置对于匹配规则的数据报文采取的操作。可选项：允许、禁止。当选择“允许”时，表示对于匹配规则的数据报文，允许通过设备。
状态	设置是否启动该访问控制规则。可选项：启用、禁用。
访问控制日志	当数据报文匹配该访问控制规则后，设置是否记录日志。可选项：不记录、记录。
最大活动会话数	设置 TopWAF 上的最大会话个数。

✧ 数据包在匹配访问控制规则时必须匹配上选择的所有选项，规则才能生效。

2）点击【确定】按钮完成该条访问控制策略的添加。

步骤3 点击『查询』，弹出“搜索”窗口，设置资源对象参数和源/目的 IP 地址，点击【确定】按钮即可将匹配的访问控制策略显示在访问控制列表中。

步骤4 选择一个策略，点击移动图标“”，弹出“移动”窗口，设置将当前策略移动到已存在策略之前或之后。

步骤5 对于已添加的策略，点击上方的『编辑』、『删除』、『清空』可执行相应操作。

CLI 方式

firewall policy add action <accept|deny> [**srcarea** <*mstring*>] [**dstarea** <*mstring*>] [**src** <*mstring*>] [**dst** <*mstring*>] [**service** <*mstring*>] [**log** <on|off>] [**enable** <yes|no>] [**group_name** <*mstring*>] [**max_active_session** <*string*>] [**orig_dst** <*mstring*>] [**traffic-statistic** <on|off>] [**comment** <*wstring*>] [**slog** <on|off>]

命令描述：

添加一条访问控制规则。

参数说明：

参数	说明
action <accept|deny>	必选项，设定访问权限，即允许或禁止匹配该规则的报文通过 TopWAF。 允许|禁止。
srcarea <*mstring*>	可选项，设定源区域。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。必须为已定义的区域资源名，可以有一个或多个，需用单引号' '括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
dstarea <*mstring*>	可选项，设定目标区域。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。为已定义的区域资源名，可以有一个或多个，需用单引号' '括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
src <*mstring*>	可选项，源地址对象。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。为已定义的地址对象名，可以用主机、子网或地址范围。也可以输入多个，格式为'aa ll'，用单引号，中间用空格分隔。
dst <*mstring*>	可选项，目的地址对象。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。为已定义的地址对象名，可以用主机、子网或地址范围。也可以输入多个，格式为'aa ll'，用单引号，中间用空格分隔。
service <*mstring*>	可选项，设定服务资源。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。必须是系统缺省服务或自定义服务的名称，可以输入多个，格式为'IP ICMP'，用单引号，中间用空格分隔。名称的大小写必须与系统定义相一致，如'IP'。
log <on|off>	可选项，设置当数据报文匹配规则时，是否在日志中记录还是进行报警提示，默认不做记录。 记录日志|不记录日志。
enable <yes|no>	可选项，设置是否启用这条规则，默认启用该规则。 启用|不启用。
group_name <*mstring*>	可选项，设置访问控制规则组。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。
max_active_session <*string*>	可选项，设置 TopWAF 上的用户的最大会话个数。 字符串类型，不包含" &\"\\'%<>" 中任意字符以及空格。
orig_dst < *mstring* >	可选项，设置地址转换前的目标地址对象。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。必须是系统已经定义的地址对象名。
traffic-statistic <on|off>	可选项，设置策略统计开关，默认为关。 开|关。
comment < *wstring* >	可选项，设置访问控制规则描述。 字符串类型，长度必须小于 126 位。不包含"<>\\"中任意字符。

参数	说明
slog <on|off>	可选项，设置是否记录设备的会话日志。 记录|不记录。

命令示例：

添加一条拒绝 area_feth0 源区域数据包访问的访问控制策略，并记录日志。

TopsecOS# **define area add name** *area_feth0* **interface** *feth0* **comment** *comment_content*

TopsecOS# **firewall policy add action** *deny* **srcarea** *area_feth0* **log** *on* **enable** *yes*

firewall policy modify action <accept|deny> **id** <*num*> [**srcarea** <*mstring*>] [**dstarea** <*mstring*>] [**src** <*mstring*>] [**dst** <*mstring*>] [**service** <*mstring*>] [**log** <on|off>] [**enable** <yes|no>] [**group_name** <*mstring*>] [**max_active_session** <*string*>] [**orig_dst** <*mstring*>] [**traffic-statistic** <on|off>] [**comment** <*wstring*>] [**slog** <on|off>]

命令描述

修改访问控制规则。

参数说明：

参数	说明
action <accept|deny>	必选项，指定访问权限，即允许或禁止匹配该规则的报文通过 TopWAF。 允许|禁止。
id <*num*>	必选项，指定要修改的访问控制规则 ID。 实数类型。
srcarea <*mstring*>	可选项，指定要修改的源区域。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。必须为已定义的区域资源名，可以有一个或多个，需用单引号'‘括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
dstarea <*mstring*>	可选项，指定要修改的目标区域。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。为已

参数	说明
	定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
src <*mstring*>	可选项，指定要修改的源地址对象。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。为已定义的地址对象名，可以用主机、子网或地址范围。也可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
dst <*mstring*>	可选项，指定要修改的目的地址对象。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。为已定义的地址对象名，可以用主机、子网或地址范围。也可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
service <*mstring*>	可选项，指定要修改的服务对象。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。必须是系统缺省服务或自定义服务的名称，可以输入多个，格式为’IP ICMP’，用单引号，中间用空格分隔。名称的大小写必须与系统定义相一致，如’IP’。
log <on|off>	可选项，修改当数据报文匹配规则时，是否在日志中记录，默认不做记录。 记录日志|不记录日志。
enable <yes|no>	可选项，是否启用这条规则，默认启用该规则。 启用|不启用。
group_name <*mstring*>	可选项，指定要修改的策略组名。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。
max_active_session <*string*>	可选项，最大活动会话数。 字符串类型，不包含" &\"\\'%<>" 中任意字符以及空格。
orig_dst < *mstring* >	可选项，指定地址转换前的目标地址对象。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。必须是系统已经定义的地址对象名。
traffic-statistic <on|off>	可选项，策略统计开关，默认为关。 开|关。
comment < *wstring* >	可选项，修改规则描述。 字符串类型，长度必须小于 126 位。不包含"<>\\"中任意字符。
slog <on|off>	可选项，修改是否记录设备的会话日志。 记录|不记录。

命令示例：

允许匹配 IP 号为 11156 的访问控制策略的源区域 area_feth0 的数据报文通过，并记录日志。

TopsecOS# **define area add name** *area_feth0* **access** *on* **interface** *feth0* **comment** *comment_content*

TopsecOS# **firewall policy modify id** *11156* **action** *accept* **srcarea** *area_feth0* **log** *on* **enable** *yes*

firewall policy delete [**id** <*num*>*]*

命令描述：

删除一条访问控制规则。

参数说明：

参数	说明
id <*num*>	必选项，指定访问控制规则 ID。 实数类型，必须是已定义的规则 ID 值。

命令示例：

TopsecOS# **firewall policy delete id** *8503*

firewall policy move <*num*> [**before** <*num*>| **after** <*num*>]

命令描述：

移动一条访问控制规则的位置。

参数说明：

参数	说明
move <*num*>	必选项，移动一条访问控制规则的位置。 实数类型，表示待移动的规则的 ID 号。
before <*num*>	可选项，设置将规则移动到指定规则之前。 实数类型，表示参照物规则的 ID 号。
after <*num*>	可选项，设置将规则移动到指定规则之后。

参数	说明
	实数类型，表示参照物规则的 ID 号。

命令示例：

移动一条访问控制规则 8503 到规则 8490 之前。

TopsecOS# **firewall policy move** *8503* **before** *8490*

firewall policy show [**src** <*mstring*>] [**srcarea** <*mstring*>] [**srcip** <*mstring*>] [**dst** <*mstring*>] [**dstarea** <*mstring*>] [**dstip** <*mstring*>] [**group-name** <*string*>] [**name** <*mstring*>] [**orig_dst** <*mstring*>]

命令描述：

查看访问控制规则。

参数说明：

参数	说明
src <*mstring*>	可选项，指定源地址对象类型。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。表示已定义的地址对象名。可以输入多个，格式为'aa ll'，用单引号，中间用空格分隔。
srcarea <*mstring*>	可选项，指定源区域。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。必须为已定义的区域资源名，可以有一个或多个，需用单引号' '括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
srcip <*mstring*>	可选项，指定源 IP。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。
dst <*mstring*>	可选项，指定目的地址对象类型。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。表示已定义的地址对象名，可以输入多个，格式为'aa ll'，用单引号，中间用空格分隔。
dstarea <*mstring*>	可选项，指定目标区域。 字符串类型，字符串类型，不以'\\'结尾或不包含"<script>"字符串。表示已定义的区域资源名，可以有一个或多个，需用单引号' '括起来，多个区域名之间用空格分隔即可，

	例如'area_feth0 area_feth1'。
dstip <*mstring*>	可选项，指定目的 IP。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。
group-name <*string*>	可选项，指定策略组。不指定时表示默认组。 字符串类型，不包含" &\"\\'%<>" 中任意字符以及空格。
name <*mstring*>	可选项，指定访问控制规则的名称，未引用任何对象时为“none”。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。
orig_dst <*mstring*>	可选项，指定地址转换前的目的地址对象名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。

命令示例：

查看所有访问控制规则。

TopsecOS# **firewall policy show**

ID 11151 firewall policy add action accept slog on group_name '3' app 'fuwu' enable

ID 11156 firewall policy add action accept log on srcarea 'area_feth0' enable

查看源区域为 area_feth0 的访问控制规则。

TopsecOS# **firewall policy show srcarea** *area_feth0*

ID 11156 firewall policy add action accept log on srcarea 'area_feth0' enable

firewall policy clean <cr>

命令描述：

清空所有访问控制规则。

命令示例：

TopsecOS# **firewall policy clean**

firewall policy total [**status** <enable|disable>]

命令描述：

根据策略状态统计访问控制规则的数量。

参数说明：

参数	说明
status <enable|disable>	可选项，设置访问控制策略状态。 启用|未启用。

命令示例：

TopsecOS# **firewall policy total**

total:2

firewall policy dump <on|off>

命令描述：

设置访问控制策略的显示开关。

参数说明：

参数	说明
dump <on|off>	必选项，设置访问控制策略的显示开关。 打开|关闭。

命令示例：

TopsecOS# **firewall policy dump** on

6.2.2.2 配置访问控制策略组

WEBUI 方式

步骤1 选择 **网络层防护** > **访问控制**，进入访问控制界面。

步骤2 点击『添加』，选择“策略组”，弹出“添加策略组”窗口，设置访问控制策略组名称后，点击【确定】按钮完成策略组的添加。

步骤3 选择访问控制策略组，点击插入图标“”，弹出“插入策略组”窗口，设置策略组名称，然后点击【确定】按钮完成访问控制策略组的添加；点击移动图标“”，弹出“移动”窗口，设置将当前策略组移动到已存在策略组之前或之后。

CLI 方式

firewall group_policy add name <*nstring*> [**before** <*nstring*>]

命令描述：

添加一条访问控制规则组。

参数说明：

参数	说明
name <*nstring*>	必选项，设置规则组名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
before <*nstring*>	可选项，设置在某规则组之前插入一条规则组。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

命令示例：

在 ACL 规则组 8108 前插入规则组 subnat83 中。

TopsecOS# **firewall group_policy add name** *subnat83* **before** *8108*

firewall group_policy clean <cr>

命令描述：

清空访问控制规则组。

命令示例：

TopsecOS# **firewall group_policy clean**

firewall group_policy delete [**id** <*num*>| **name** < *nstring* >]

命令描述：

根据 ID 或名称删除某访问控制规则组。

参数说明：

参数	说明
id <*num*>	可选项，指定规则组 ID 号。 实数类型。
name <*nstring*>	可选项，设置规则组名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

命令示例：

删除规则组 subnat83。

TopsecOS# **firewall group_policy delete name** *subnat83*

firewall group_policy rename oldname <*nstring*> **newname** <*nstring*>

命令描述：

重命名访问控制规则组。

参数说明：

参数	说明
oldname <*nstring*>	必选项，设置规则组旧的名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
newname <*nstring*>	必选项，设置规则组新的名称。 字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

firewall group_policy show <cr>

命令描述：

查看访问控制规则组。

命令示例：

TopsecOS# **firewall group_policy show**

ID 10070 firewall group_policy add name 33

ID 10071 firewall group_policy add name dfg

ID 10072 firewall group_policy add name df

ID 10073 firewall group_policy add name 234

ID 10186 firewall group_policy add name dre

firewall group_policy move <*string*>[**before** <*string*>| **after** <*string*>]

命令描述：

移动访问控制规则组。

参数说明：

参数	说明
move <*string*>	必选项，移动访问控制规则组。 字符串类型，不包含" &\"\\'%<>" 中任意字符以及空格。
before <*string*>	必选项，移动到指定的规则组之前。 字符串类型，不包含" &\"\\'%<>" 中任意字符以及空格。
after <*string*>	必选项，移动到指定规则组之后。 字符串类型，不包含" &\"\\'%<>" 中任意字符以及空格。

命令示例：

将名为“test10”的规则组移动到名为“test2”的规则组之前。

TopsecOS# **firewall group_policy move** *test10* **before** *test2*

6.3 DDOS 防御

网络中存在多种防不胜防的攻击，侵入或破坏网络上的服务器、盗取服务器的敏感数据、破坏服务器对外提供的服务，或者直接破坏网络基础设施导致网络服务异常甚至中断。作为网络安全设备，必须具备攻击防护功能来检测各种类型的网络攻击，从而采取相应的措施保护内部网络免受恶意攻击，以保证内部网络及系统正常运行。

Flood 攻击是指攻击者向目标发送大量的虚假请求，被攻击者不断应答这些无用信息，而合法的用户却无法得到相应的服务，即发生拒绝服务。

DoS（Denial of Service，即拒绝服务）攻击，其目的是使计算机或网络无法提供正常的服务。常见的 DoS 攻击是单包攻击，包括扫描类攻击、畸形报文类攻击和特殊报文类攻击。

- 扫描类攻击主要包括 IP 地址扫描和端口扫描，IP 地址扫描是指攻击者发送目的地址不断变化的 IP 报文（TCP、UDP、ICMP）来发现网络上存在的主机和网络，从而准确地发现潜在的攻击目标。端口扫描是指通过扫描 TCP 和 UDP 的端口，检测被攻击对象的操作系统和潜在服务。攻击者通过扫描窥探就能大致了解目标主机提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。
- 畸形报文攻击是指攻击者向目标主机发送有缺陷的 IP 报文，使得目标主机在处理这样的 IP 报文时发生错误，或者造成系统崩溃，影响目标主机的正常运行，主要的畸形报文攻击有 Ping of Death、Teardrop 等。
- 特殊报文攻击是指攻击者利用一些合法的报文对网络进行侦察，这些报文都是合法的应用类型，只是正常网络很少用到。主要的特殊报文攻击有超大 ICMP 报文控制、Tracert 和时间戳选项 IP 报文控制等。

DDoS（Distributed Denial of Service，即分布式拒绝服务）攻击，是在 DoS 攻击基础上产生的一种攻击，通过可利用的僵尸主机（攻击者入侵过或者可间接利用的主机）向目标对象发送大量请求，造成目标对象的网络带宽拥塞、资源耗尽而不能提供正常的服务。随着商业利益的驱使，DDoS 攻击已经成为互联网面临的重要安全威胁。

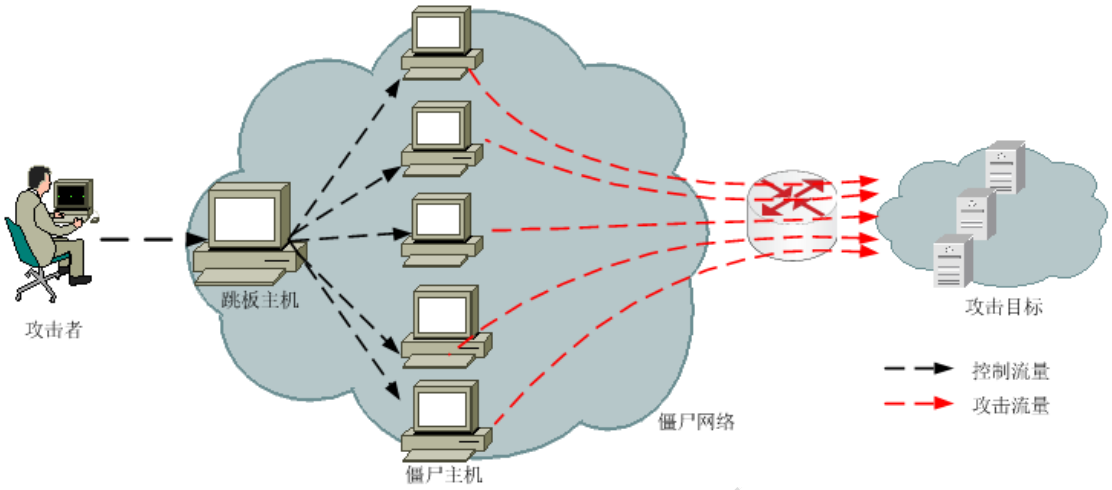


图 4-1 DDoS 攻击示意图

如上图所示，攻击者通过各种手段取得网络上大量在线主机的控制权限，这些被控制的主机称为僵尸主机，攻击者和僵尸主机构成的网络称为僵尸网络。当被攻击目标确定后，攻击者控制僵尸主机向目标发送大量的攻击报文，导致被攻击目标的网络链路拥塞、系统资源耗尽。

常见的应用层 DDoS 攻击有 HTTP Flood、HTTPS Flood 等，其根本目的都是使目标主机、服务器或网络无法及时接收并处理合法用户的请求。具体的表现方式有以下几种：

1）制造大量无用数据，造成通往目的主机的网络拥塞，使目的主机无法正常和外界通信；

2）利用目的主机提供服务或传输协议上处理重复连接的缺陷，反复高频地发出攻击性的重复服务请求，使得目的主机无法及时处理其他正常的请求；

3）利用目的主机所提供服务程序或传输协议的本身实现缺陷，反复发送畸形的攻击数据引发系统错误的分配大量系统资源，使目的主机处于挂起状态甚至死机。

针对当前应用层不断泛滥、防范难度很强的 DDoS 攻击，TopWAF 提供了 DDoS 防御模块，能够有效检测并抵御 HTTP、HTTPS 类型的 DDoS 攻击行为及传统的单包攻击，高效地完成对 DDOS 攻击的过滤和防护，从而确保服务器可以正常提供服务。

DDoS 模块首先对到达目标服务器的流量进行统计，然后与设置的威胁检查条件做对比，如果超过设置的阈值，将根据设置的防御动作进行 DDoS 防御。

威胁检查条件与触发的 CC 防御动作关系如下表所示。

威胁检查条件	触发的 CC 攻击防御动作
HTTP Flood 攻击检测	HTTP Flood 源限速 HTTP Flood 源认证 HTTP Flood 目的限速
HTTP 新建连接 Flood 攻击检测	HTTP 源新建连接速率检查 HTTP 目的新建连接速率检查
HTTP 并发连接 Flood 攻击	HTTP 源并发连接数检查 HTTP 目的并发连接数检查 HTTP 慢速攻击
HTTP URI CC 攻击检测	HTTP URI 访问占比检查
HTTPS Flood 攻击检测	HTTPS Flood 源限速 HTTPS Flood 源认证 HTTPS Flood 目的限速
HTTPS 新建连接 Flood 攻击检测	HTTPS 源新建连接速率检查 HTTPS SSL DOS 防范 HTTPS 目的新建连接速率检查
HTTPS 并发连接 Flood 攻击	HTTPS 源并发连接数检查 HTTPS SSL DOS 防范 HTTPS 目的并发连接数检查

6.3.1 全局配置

为使 TopWAF 以最佳性能保护内网服务器，管理员需结合实际网络环境配置“全局配置”，包括安全级别、统计采用比、重传超时时间、攻击开始抖动时间、攻击结束抖动时间、动态白名单超时时间、动态黑名单超时时间、动态源节点超时时间、动态保护节点超时时间参数。

WEBUI 方式

步骤1 选择 **网络层防护** > **DDOS 防御** > **全局配置**，如下图所示。

在全局参数时，各项参数的具体说明如下表所示。

参数	说明
安全级别	配置匹配某防护策略的攻击流量所属的危险级别，可选项：高、中、低。
统计采样比	配置 TopWAF 自动对匹配某防护策略的流量进行采样的采样比，单位：$1/2^n$；n 取值范围：0-15。即如果 n 取值为 10，TopWAF 每检测到 1024 个匹配该防护策略的数据包，抓取其中的一个数据包作为统计分析该流量的依据。
重传超时时间	配置系统重传计时器超时时间。单位：秒；取值范围：3-20。 说明： 重传超时是 TCP 协议保证数据可靠性的重要机制，发送方发送一个数据包后开启计时器，在重传超时时间内没有收到确认报文，则重新再次发送数据包。
攻击开始抖动时间	设置 TopWAF 确认攻击开始的抖动时间，避免流量抖动而导致 TopWAF 将其误判为攻击开始。单位：秒；取值范围：1-86400；默认值：3。 说明： 该参数设置为 N，连续 N 秒内流量都超过设定的阈值，TopWAF 才判定为攻击开始。
攻击结束抖动时间	设置 TopWAF 确认攻击结束的抖动时间，避免流量抖动而导致

参数	说明
	TopWAF 将其误判为攻击结束。单位：秒；取值范围：1-86400；默认值：300。 说明： 该参数设置为 N，连续 N 秒内流量都不超过设定的阈值，TopWAF 才判定为攻击结束。
动态黑名单超时时间	配置动态黑名单的超时时间，单位：分钟；取值范围：1-1440。 说明： 经过动态黑名单超时时间后，如果黑名单对应的主机没有发起通往 TopWAF 防护区域的连接，则该黑名单自动从 TopWAF 黑名单中删除。
动态白名单超时时间	配置动态白名单的超时时间，单位：分钟；取值范围：1-1440。 说明： 经过动态白名单超时时间后，白名单自动从 TopWAF 白名单中删除。
动态源节点超时时间	配置 TopWAF 记录的源 IP 地址的老化时间，超过该老化时间后，仍没有该源 IP 地址对应的流量去往防护区，系统则会将该记录的源 IP 地址删除。单位：秒；取值范围：10-86400。 说明： 1）如果配置了基于源行为分析的防护策略，TopWAF 会产生源节点，在发生异常事件后记录源 IP 地址。 2）如果源节点在动态黑名单中，动态源节点不超时。
动态保护节点超时时间	配置 TopWAF 记录的目的 IP 地址的老化时间，超过该老化时间后，仍没有该目的 IP 地址对应的流量去往防护区，系统则会将该记录的目的 IP 地址删除。单位：秒；取值范围：10-86400。 说明： 如果通往 TopWAF 防护区的流量成功匹配防护策略，TopWAF 即会记录目标 IP 地址。

步骤2 参数设置完成后，点击【应用】按钮提交系统。

CLI 方式

ddos global set security_level <low|medium|high>

命令描述：

设置匹配某防护策略的流量的安全级别。

参数说明：

参数	说明
security_level <low|medium|high>	必选项，设置安全级别。 低|中|高。

命令示例：

设置安全级别为低。

TopsecOS# **ddos global set security_level** low

ddos global set stat ratio <*num*>

命令描述：

设置设备自动对匹配某防护策略的流量进行采样的统计标准。

参数说明：

参数	说明
ratio <*num*>	必选项，设置抽样因子。 实数类型。单位：$1/2^n$；n 取值范围：0-15。

命令示例：

设置抽样因子为 7。

TopsecOS# **ddos global set stat ratio** *7*

ddos global set retransmit timeout <*num*>

命令描述：

设置系统重传计时器超时时间。

参数说明：

参数	说明
retransmit timeout <*num*>	必选项，设置系统重传计时器的超时时间。 实数类型。单位：秒；取值范围：3-20；默认值：5。

命令示例：

TopsecOS# **ddos global set retransmit timeout** *5*

ddos global set source timeout <*num*>

命令描述：

设置动态源节点超时时间。

参数说明：

参数	说明
source timeout <*num*>	动态源节点超时时间。 实数类型。位：秒；取值范围：10-86400；默认值：300。

命令示例：

TopsecOS# **ddos global set source timeout** *300*

ddos global set server timeout <*num*>

命令描述：

设置动态保护节点超时时间。

参数说明：

参数	说明
server timeout<*num*>	设置动态保护节点超时时间。 实数类型。单位：秒；取值范围：10-86400；默认值：60。

命令示例：

TopsecOS# **ddos global set server timeout** *60*

ddos global set confirmtime start-time <*num*> **end-time** <*num*>

命令描述：

设置攻击开始及结束抖动时间。

参数说明：

参数	说明
confirmtime start-time <*num*>	设置攻击开始确认时间。 实数类型。单位：秒；取值范围：1-86400；默认值：3。
end-time <*num*>	设置攻击结束确认时间。 实数类型。单位：秒；取值范围：1-86400；默认值：300。

命令示例：

TopsecOS# **ddos global set confirmtime start-time** *3***end-time** *300*

ddos global set blacklist timeout <*num*>

命令描述：

设置动态黑名单超时时间。

参数说明：

参数	说明
blacklist timeout <*num*>	动态黑名单超时时间。 实数类型。单位：分钟；取值范围：1-1440；默认值：5。

命令示例：

TopsecOS# **ddos global set blacklist timeout** *5*

ddos global set whitelist timeout <*num*>

命令描述：

设置动态白名单超时时间。

参数说明：

参数	说明
whitelist timeout <*num*>	动态白名单超时时间。 实数类型。单位：分钟；取值范围：1-1440；默认值：5。

命令示例：

TopsecOS# **ddos global set whitelist timeout** *5*

ddos global clean <cr>

命令描述;

清除 DDoS 防御的全局配置信息。

ddos global show [confirmtime|time|virtualline]

命令描述:

查看 DDoS 防御的全局配置信息。

参数说明：

参数	说明
confirmtime|time|virtualline	DDoS 攻击的确认时间|系统时间|虚拟线组

命令示例：

查看 DDoS 防御的所有全局配置信息。

TopsecOS# **ddos global show**

ddos global set default-group off

ddos global set stat ethernet

ddos global set stat ratio 7

ddos global set retransmit timeout 5

ddos global set whitelist timeout 5

ddos global set blacklist timeout 5

ddos global set source timeout 300

ddos global set server timeout 60

ddos global set security_level low

ddos global set related-auth off

ddos global set filter on

ddos global set cdn-check off

ddos global set deployscene offline

ddos global set devtype clean

ddos global set netflowswitch off

ddos global set confirmtime start-time 3 end-time 300

查看 DDoS 攻击的确认时间。

TopsecOS# **ddos global show confirmtime**

ddos global set confirmtime start-time 3 end-time 300

查看全局时间。

TopsecOS# **ddos global show time**

+08 2015-06-16 15:55:31

查看虚拟线组配置信息。

TopsecOS# **ddos global show virtualline**

12853 feth10=flowmonitor feth11=flowmonitor

6.3.2 防护配置

TopWAF 可对被保护的服务器提供 DDoS 攻击防护功能。DDoS 防御基于防护对象实现。配置防护对象时，需配置防护对象的基本信息、防护属性以及基线学习。其中基线学习配置包括周期性学习真实用户流量模型的时间以及基线参考容忍度。

防护对象配置完成后，需被服务器策略引用方可生效，关于服务器策略的定义请参见 5.3 服务器策略。

- 防御动作支持检测清洗和强制防御。当设置为检测清洗时，先检测服务器是否受到异常或者攻击，当检测到可疑流量（如流量超过策略配置的阈值）后，TopWAF 对流向服务

器的流量进行清洗处理；当设置为强制防御时，不管是否设定了检测条件或者发生了攻击事件，都会进入清洗流程，按照清洗的规则进行清洗。

- 基线学习是由防护对象对真实网络中的用户流量进行分析和统计，完成用户流量模型的自学习，并自动形成流量模型。其中，“用户流量”是按照预设采样率进行报文抓取且经过检测的流量。学习到的基线是管理员在防护对象绑定的防护策略中配置过的检测 Flood 对象的真实网络阈值，因此在对用户流量进行学习之前，管理员需要在防护策略中配置 Flood 阈值，并设置比较高的数值，避免引起攻击误报。基线学习结果中的 Flood 检测阈值为学习周期内的最大值。

防护策略是基于不同应用层协议的攻击防护策略，可以有效检测并抵御常见的 HTTP Flood 攻击和 HTTPS Flood 攻击。当服务器策略引用某个防护对象时（关于服务器策略的定义请参见 5.3 服务器策略），如果防护对象绑定了防护策略，则 TopWAF 会根据该防护对象下的具体策略对目标服务器进行防护。

WEBUI 方式

步骤1 选择 **网络层防护** > **DDOS 防御** > **防护配置**，进入防护对象界面。

步骤2 防护配置。

1）点击『添加』，弹出“添加”窗口，如下图所示。

2）配置防护对象。

在设置防护对象信息时，各项参数的具体说明如下表所示。

参数	说明
防护对象名称	必选项，设置防护服务器的名称。名称长度不超过 32 个字节。
防护动作	设置 TopWAF 针对通往保护对象的流量采取的防护措施。可选项：检测清洗、强制防御。 1）检测清洗：所有防范都在检测到异常或者攻击之后进行。旁路部署时，当检测到可疑流量（如流量超过策略配置的阈值）后，将进行清洗处理； 2）强制防御：不管是否设定了检测条件或者发生了攻击事件，都会进入清洗流程，按照设备自身的规则进行清洗。
基线学习开关	“基线”是由防护服务器对真实的客户端流量进行分析和统计，完成客户端流量模型的自学习，并自动形成的一种流量准则。其中，“客户端流量”是按照预设采样率进行抓取的进入设备的流量，并且该流量进行过检测。 设置是否开启基线学习功能。若不开启，则表示防护服务器不进行真实客户端流量模型的学习。
学习结果立即生效	如果开启了防护对象的“基线学习”功能，设置是否开启学习结果的立即生效功能。开启后，系统将学习结果立即下发到防护策略中。如果不开启，则将学习结果存入服务器数据库中。默认关闭。 说明： 学习结果以表格的形式显示在规定时间内的学习结果，主要参数包括：检测项、学习到的阈值、阈值单位、当前配置、参考数值、学习结果产生时间等。关于学习结果的查看具体请参见 查看基线学习结果。
是否周期性学习	基线学习开关开启后，设置是否进行周期性学习。 说明： 默认情况下，防护对象的基线学习不循环，学习结果不下发。
学习周期	如果开启了防护对象对客户端流量的“周期性学习”功能，设置学习周期数值。单位：min；取值范围：1-65535；默认值：1。
基线参考容忍度	“容忍度”是指应用学习结果时，自动下发到防护策略中时相对于学习结果的比例参数。由于防护对象学习的是真实的客户端流量，若直接将学习结果下发到防护策略中，如果网络中瞬间流量过大容易导致误触发防护策略，故需要设置容忍度。 单位：%；取值范围：1-500；默认值：50。 说明： 基线学习结果下发的阈值=学习结果*（1+容忍度）。

3）配置防护策略。激活“防护策略”页签。

- HTTP 威胁检查

激活“HTTP 威胁检查”页签，如下图所示。

在设置 HTTP 威胁检查时，各项参数的具体说明如下表所示。

参数	说明
HTTP Flood 攻击检测	设置 HTTP Flood 攻击检测功能是否开启，并设置其阈值。 包传送速率取值范围：1-1200000；默认值：2000；单位：pps。
HTTP 新建连接 Flood 攻击检测	设置 Flood 攻击的新建连接功能是否开启，并设置其阈值。 新建连接 Flood 攻击指的是攻击者发起新连接的速率很快，短时间内发出大量的新连接，达到占用服务器的连接，使服务器资源耗尽的目的。 新建连接速率取值范围：1-1200000；默认值：1000；单位：cps。 说明： 配置新建连接检测后，如果 HTTP 的新建连接速率超过阈值会上报异常，说明发现了新建连接 Flood 攻击。
HTTP 并发连接 Flood 攻击	设置 Flood 攻击的并发连接功能是否开启，并设置其阈值。 并发连接 Flood 攻击指的是此时此刻服务器上没有断开的连接的总数，若数值很大则表明发生了并发连接攻击。 并发连接数取值范围：1-1200000；默认值：1000；单位：conns。 说明： 配置并发连接检测后，如果 HTTP 的并发连接速率超过阈值会上报异常，说明发现了并发连接 Flood 攻击。
HTTP URI 监控	设置 HTTP URI 监控功能是否开启，并设置参数。CC 攻击是模拟多个用户不停的访问 Web 服务器上那些需要大量数

参数	说明
	据操作（即需要 CPU 长时间处理）的页面，进而导致 Web 服务器 CPU 长时间高负荷运转直至宕机，以达到攻击目的。 URI 访问次数单位：times；取值范围：1-1200000；默认值：2000。 检测周期单位：s；取值范围：1-65535；默认值：4。
URI 监控列表	URI 对象定义了为了预防 CC 攻击而需要大量数据操作的页面，管理员可以通过定义 CC 攻击规则以保护特定服务器上的 URI 对象。配置该功能后，设备针对一些耗资源和性能的 URI 来进行监控，包括对源和目的这两方面进行监控。首先是对目的进行监控，如果一个服务器在一个周期内被访问的所有监控 URI 的总次数 m 大于设定的阈值，则启动对源的监控。启动对源的监控后，如果一个源在一个周期内（与服务器的周期一样）访问监控的 URI 的总次数 k 占比（k/m）大于设定的阈值，则认为该源含有攻击行为，设备将该源加入黑名单。 启用 HTTP URI 监控功能后，点击界面下方的『添加』，添加指定的 URI 操作。 1）域名（或者 URI）域名格式为 rfc 格式。 2）匹配状态：模糊匹配、完全匹配。默认值：模糊匹配。 说明： 1）rfc 格式的域名规范：域名字符串必须包含在以下字符中：26 个英文字母、阿拉伯数字 0-9、英文中的连词号“-”。必须以字母开始，字母或数字结束；标签（两个“.”之间的部分）长度不能超过 63；整个域名长度不能超过 255。比如搜狐视频的域名为：video.sohu.com.cn。 2）匹配状态中的 URI 参数：“/abc/index.asp”可匹配“/abc/index.asp?id=333”；URI 设置为 index.asp，则认为是/index.asp，若想匹配各个目录的 index.asp，则 URI 需设置为“/index.asp”。

- HTTP 慢速攻击

激活“HTTP 慢速攻击”页签，如下图所示。

在设置 HTTP 慢速攻击时，各项参数的具体说明如下表所示。

参数	说明
HTTP Slow-header 防范	设置 HTTP Slow-header 防范功能是否开启，并设置最大传输时间和最大异常连接数。在正常的 HTTP 请求中，客户端发送完成 HTTP Header 字段之后，会追加发送一个 CRLF 标志，表明 HTTP 请求已经结束。在 Slow-header 攻击中，攻击者在发送 HTTP 请求时，长时间缓慢地发送垃圾数据，始终不发送最后一个 CRLF 标志位，造成 Web 服务组件长时间等待，进而造成服务资源被大量占用，引起拒绝服务。 1）最大传输时间：针对源 IP 检测的发送一个 header 的最大时长。单位：s；取值范围：1-65535；默认值：8。超过最大传输时间时，执行动作：源异常会话监控。 2）最大异常连接数：“连接”指的是正在传输不完整的 header 的连接。单位：conns（连接数）；取值范围：1-65535；默认值：10。 3）执行动作：加黑名单。 说明： 1）当源传输一个 header 的时长超过最大传输时间时，该连接被标记为异常连接。当源的异常连接数超过最大异常连接数时，该源 IP 加入动态黑名单。 2）需要先开启 HTTP 威胁检查的 HTTP 并发连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HHT Slow-header 防范功能才能生效。关于 HTTP 并发连接 FLOOD 攻击检测的设置具体请参见 HTTP 威胁检查。
HTTP Slow-post 防范	在 HTTP 请求中，HTTP 协议的 Content-length 字段表明需要上传的数据量的大小，Web 服务组件根据该字段大小来判断数据传输是否完成。在 Slow-post 攻击中，攻击者利用该特性，首先设定一个比较大的 Content-length 字段，然后以极低的速度发送

参数	说明
	数据包，并保持这个连接不被断开，从而长期占用服务器资源，进而影响其他客户端的请求，造成拒绝服务攻击。 设置进行 Slow-post 防范的最大传输时间、最小传输速率和最大异常连接数。 1）最大传输时间：针对源 IP 的实体传输时间阈值，单位：s；取值范围：1-65535；默认值：8。执行动作：slow-post 防范。 2）最小传输速率：针对源 IP 的实体发送速率阈值，单位：Bps；取值范围：1-65535；默认值：1。执行动作：异常会话监控。 3）最大异常连接数：针对目的 IP 的并发连接数阈值。“连接”指的是正在传输不完整的实体的连接。单位：conns（连接数）；取值范围：1-65535；默认值：10。 4）执行动作：加黑名单。 说明： 1）当源传输一个实体的时长超过最大传输时间，并且传输速度小于最小传输速率，则该连接被标记为异常连接，当源的异常连接数超过最大异常连接数，则源 IP 加入动态黑名单。 2）需要先开启 HTTP 威胁检查的 HTTP 并发连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTP Slow-post 防范功能才能生效。关于 HTTP 并发连接 FLOOD 攻击检测的设置具体请参见 HTTP 威胁检查。

➢ HTTP CC 攻击

激活“HTTP CC 攻击”页签，如下图所示。

在设置 HTTP CC 攻击时，各项参数的具体说明如下表所示。

参数	说明
HTTP Flood 源限速	设置源 HTTP Flood 的最大报文速率和执行动作。如果源的 HTTP 速率超过最大速率，则会对该源进行限速。 最大速率单位：pps；取值范围：1-4294967295；默认值：20000。 执行动作可选项：丢弃、加黑名单；默认值：丢弃。 说明： 需要先开启 HTTP 威胁检查的 HTTP Flood 攻击检测功能，达到设置的包传送速率上限，HTTP Flood 源限速功能才能生效。关于 HTTP Flood 攻击检测的设置具体请参见 HTTP 威胁检查。
HTTP 源新建连接速率检查	设置 HTTP 源新建连接的最大速率和执行动作。 新建连接速率单位：cps；取值范围：0-6000；默认值：60。 执行动作可选项：丢弃、加黑名单；默认值：丢弃。 说明： 需要先开启 HTTP 威胁检查的 HTTP 新建连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTP 源新建连接速率检查功能才能生效。关于 HTTP 新建连接 FLOOD 攻击检测的设置具体请参见 HTTP 威胁检查。
HTTP 源并发连接数检查	设置 HTTP 源并发连接的最大个数和执行动作。 并发连接数单位：conns；取值范围：0-20000；默认值：200。 执行动作可选项：丢弃、加黑名单；默认值：丢弃。 说明： 需要先开启 HTTP 威胁检查的 HTTP 并发连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTP 源并发连接数检查功能才能生效。关于 HTTP 并发连接 FLOOD 攻击检测的设置具体请参见 HTTP 威胁检查。
HTTP Flood 源认证	设置进行 HTTP Flood 源认证的认证模式和最大失败次数。 重定向：HTTP 协议的一种机制，通常是服务器告知客户端所访问的资源 URL 发生了变化，并跳转到新的地址页面； 验证码：要求用户输入验证码进行验证的一种方式。 最大失败次数：即最大源认证尝试次数，单位：times；默认值：0，表示失败次数不限。 执行动作可选项：重定向、验证码；默认值：重定向。 说明： 1）如果源认证失败次数达到最大源认证尝试次数，则该源 IP 加入动态黑名单中； 2）当最大失败次数为 0 时，表示验证失败次数检查功能不开启，为防止误将代理加入黑名单，需确认在没有代理或只有透明代理的情况下启动该功能； 3）开启验证码认证模式时，系统会默认先用重定向模式进行防范，若防御效果不佳才会启动验证码模式。 说明：

参数	说明
	需要先开启 HTTP 威胁检查的 HTTP Flood 攻击检测功能，达到设置的包传送速率上限，HTTP Flood 源认证功能才能生效。关于 HTTP Flood 攻击检测的设置具体请参见 HTTP 威胁检查。
HTTP Flood 目的限速	设置目的 HTTP Flood 的最大报文速率和执行动作。 如果目的的 HTTP 的流量超过最大速率，则对该目的 IP 的流量进行限速。 最大速率单位：pps；取值范围：0-4294967295；默认值：20000。 执行动作为丢弃。 说明： 需要先开启 HTTP 威胁检查的 HTTP Flood 攻击检测功能，达到设置的包传送速率上限，HTTP Flood 目的限速功能才能生效。关于 HTTP Flood 攻击检测的设置具体请参见 HTTP 威胁检查。
HTTP 目的新建连接速率检查	设置 HTTP 目的新建连接的最大速率和执行动作。 最大速率单位：cps；取值范围：0-400000；默认值：2000。 执行动作：丢弃。 说明： 需要先开启 HTTP 威胁检查的 HTTP 新建连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTP Flood 目的新建连接速率检查功能才能生效。关于 HTTP 新建连接 FLOOD 攻击检测的设置具体请参见 HTTP 威胁检查。
HTTP 目的并发连接数检查	设置 HTTP 目的并发连接的最大个数和执行动作。 并发连接数单位：conns；取值范围：0-1200000；默认值：8000。 执行动作：丢弃。 说明： 需要先开启 HTTP 威胁检查的 HTTP 并发连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTP 目的并发连接数检查功能才能生效。关于 HTTP 并发连接 FLOOD 攻击检测的设置具体请参见 HTTP 威胁检查。
HTTP URI 访问占比检查	设置 HTTP URI 访问占比检查。 每个客户端访问 URI 监控列表中指定 URI 比例上限，单位：%；取值范围：1-100；默认值：30。关于 URI 监控列表的设置具体请参见 HTTP 威胁检查。 执行动作：加黑名单。 说明： 需要先开启 HTTP 威胁检查的 HTTP URI CC 攻击检测功能，达到设置的 URI 访问次数上限，HTTP URI 访问占比功能才能生效。关于 HTTP URI CC 攻击检测的设置具体请参见 HTTP 威胁检查。

➢ HTTPS 威胁检查

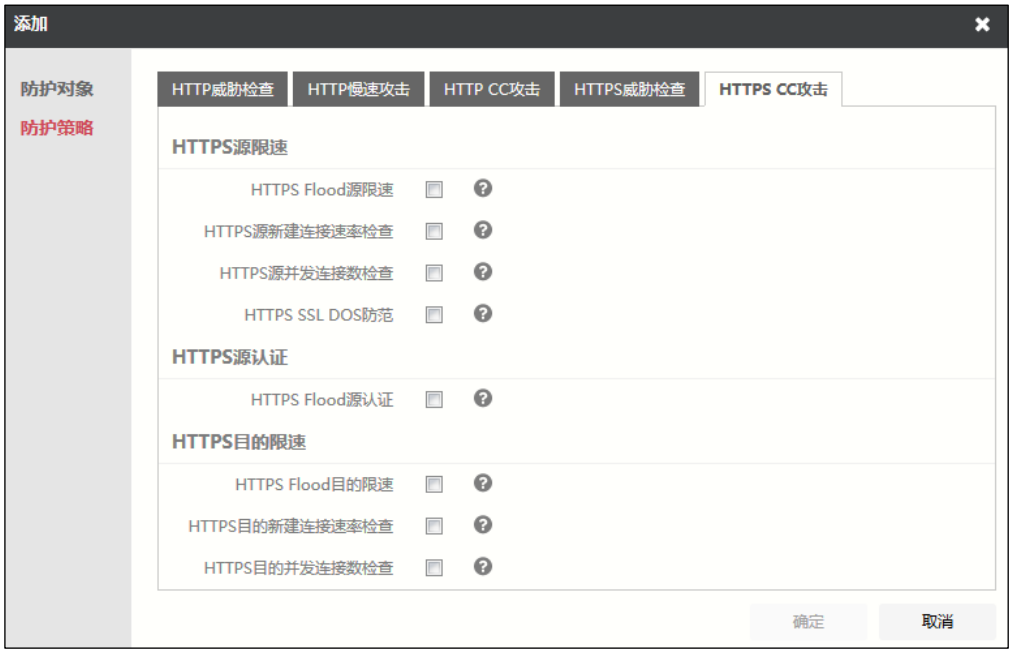
激活“HTTPS 威胁检查”页签，如下图所示。

在设置 HTTPS 威胁检查时，各项参数的具体说明如下表所示。

参数	说明
HTTPS Flood 攻击检测	设置进行 HTTPS Flood 攻击检测的阈值。 包传送速率单位：pps；取值范围：1-1200000；默认值：2000。
HTTPS 新建连接 Flood 攻击检测	设置 Flood 攻击的新建连接数。配置新建连接检测后，如果到目的服务器的源发起的 HTTPS 新建连接速率超过阈值会上报异常，说明发现了新建连接 Flood 攻击。 新建连接速率单位：cps；取值范围：1-1200000；默认值：1000。
HTTPS 并发连接 Flood 攻击检测	设置 Flood 攻击的并发连接数。配置并发连接检测后，如果目的服务器的 HTTPS 的并发连接速率超过阈值会上报异常，说明发现了并发连接 Flood 攻击。 并发连接数单位：conns；取值范围：1-1200000；默认值：1000。

➢ HTTPS CC 攻击

激活“HTTPS CC 攻击”页签，如下图所示。



在设置 HTTPS CC 攻击时，各项参数的具体说明如下表所示。

参数	说明
HTTPS Flood 源限速	设置源 HTTPS Flood 的最大报文速率和执行动作。 最大速率单位：pps；取值范围：1-4294967295；默认值：20000。 执行动作可选项：丢弃、加黑名单；默认值：丢弃。 说明： 需要先开启 HTTPS 威胁检查的 HTTPS Flood 攻击检测功能，达到设置的包传送速率上限，HTTPS Flood 源限速功能才能生效。关于 HTTPS Flood 攻击检测的设置具体请参见 HTTPS 威胁检查。
HTTPS 源新建连接速率检查	设置 HTTPS 源新建连接的最大速率和执行动作。 最大速率单位：cps；取值范围：0-6000；默认值：60。 执行动作可选项：丢弃、加黑名单；默认值：丢弃。 说明： 需要先开启 HTTPS 威胁检查的 HTTPS 新建连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTPS 源新建连接速率检查功能才能生效。关于 HTTPS 新建连接 FLOOD 攻击检测的设置具体请参见 HTTPS 威胁检查。
HTTPS 源并发连接数检查	设置 HTTPS 源并发连接的最大个数和执行动作。 并发连接最大个数单位：conns；取值范围：0-20000；默认值：200。 执行动作可选项：丢弃、加黑名单；默认值：丢弃。 说明： 需要先开启 HTTPS 威胁检查的 HTTPS 并发连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTPS 源

参数	说明
	并发连接数检查功能才能生效。关于 HTTPS 并发连接 FLOOD 攻击检测的设置具体请参见 HTTPS 威胁检查。
HTTP SSL DOS 防范	ssl-dos 攻击，即 SSL 重协商攻击，利用反复的和服务器进行 SSL 的密钥重协商，达到消耗服务器性能的目的。 设置 ssl-dos 攻击防范的周期、最大重协商次数和最大异常连接数。 1）周期单位：s；取值范围：1-65535；默认值：2。 2）最大重协商次数单位：times；取值范围：1-65535；默认值：4。 3）最大异常连接数单位：conns；取值范围 1-65535；默认值：10。 4）执行动作：加黑名单。 说明： 1）当检测到新建连接或并发连接 Flood 攻击时，如果配置了 ssl-dos 攻击防御，则会启动该功能。当源在一个周期内的重协商次数超过最大重协商次数，则该连接被标记为异常连接；当源的异常连接数超过最大异常连接数，则源 IP 加入动态黑名单。 2)需要先开启 HTTPS 威胁检查的 HTTPS 新建连接 FLOOD 攻击检测或者 HTTPS 并发连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTPS 源并发连接数检查功能才能生效。关于 HTTPS 并发连接 FLOOD 攻击检测的设置具体请参见 HTTPS 威胁检查。
HTTPS Flood 源认证	设置进行 HTTPS Flood 源认证的最大失败次数。 最大失败次数单位：times；取值范围：0-65535；默认值：0。执行动作：加黑名单。 说明： 需要先开启 HTTPS 威胁检查的 HTTPS Flood 攻击检测功能，达到设置的包传送速率上限，HTTPS Flood 源认证功能才能生效。关于 HTTPS Flood 攻击检测的设置具体请参见 HTTPS 威胁检查。
HTTPS Flood 目的限速	设置目的 HTTPS Flood 的最大报文速率和执行动作。 最大速率单位：pps；取值范围：1-4294967295；默认值：20000。 执行动作为丢弃。 说明： 需要先开启 HTTPS 威胁检查的 HTTPS Flood 攻击检测功能，达到设置的包传送速率上限，HTTPS Flood 目的限速功能才能生效。关于 HTTPS Flood 攻击检测的设置具体请参见 HTTPS 威胁检查。
HTTPS 目的新建连接速率检查	设置 HTTPS 目的新建连接的最大速率和执行动作。 最大速率单位：cps；取值范围：0-400000；默认值：2000。

参数	说明
	执行动作：丢弃。 说明： 需要先开启 HTTPS 威胁检查的 HTTPS 新建连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTPS Flood 目的新建连接速率检查功能才能生效。关于 HTTPS 新建连接 FLOOD 攻击检测的设置具体请参见 HTTPS 威胁检查。
HTTPS 目的并发连接数检查	设置 HTTPS 目的并发连接的最大个数和执行动作。 并发连接最大个数单位：conns；取值范围：1-1200000；默认值：8000。 执行动作：丢弃。 说明： 需要先开启 HTTPS 威胁检查的 HTTPS 并发连接 FLOOD 攻击检测功能，达到设置的新建连接速率上限，HTTPS 目的并发连接数检查功能才能生效。关于 HTTPS 并发连接 FLOOD 攻击检测的设置具体请参见 HTTPS 威胁检查。

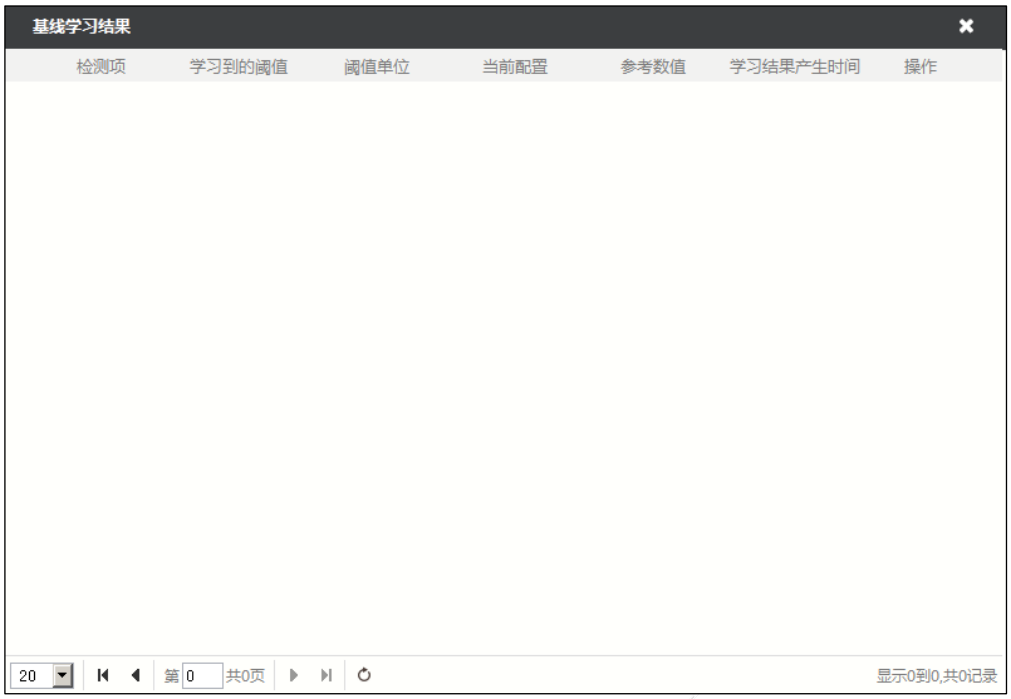
4）配置完成后，点击【确定】按钮即可。

步骤3 查看基线学习结果。

TopWAF 开启了防护对象的基线学习、学习结果立即生效、周期性学习等功能后，即可将学习结果进行收集，结合容忍度比例进行调节，并下发到防护策略中，同时学习结果还以表格的形式供管理员进行查看。

1）选择 **网络层防护** > **DDOS 防御** > **防护配置**。

2）在防护对象的基本信息中开启“基线学习”并生成学习结果后，在防护对象列表中选择防护对象，点击“基线学习状态”下的『学习结束』，弹出“基线学习结果”窗口，查看防护对象对用户流量进行学习的结果信息。



3）点击『应用』，系统将相应学习结果下发到防护对象的防护策略中，覆盖原有策略参数。

CLI 方式

ddos blacklist del ip <*mstring*> [**zone** <*mstring*>]

命令描述：

删除 DDoS 防御策略的黑名单。

参数说明：

参数	说明
ip <*mstring*>	必选项，设置黑名单 IP 地址。 字符串形式，不以'\\'结尾或不包含"<script>"字符串。支持 IPv4 和 IPv6 格式。IPv4 地址格式为 A.B.C.D。IPv6 地址格式为 X:X:X:X:X:X:X:X/(0-128)，其中 X 为一个 4 位十六进制整数。
zone <*mstring*>	可选项，设置防护区域名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。

ddos blacklist set unblock ip <*mstring*> [**zone** <*mstring*>]

命令描述：

设置 DDoS 防御策略的黑名单。

参数说明：

参数	说明
unblock ip <*mstring*>	必选项，设置黑名单 IP 地址。 字符串形式，不以'\\'结尾或不包含"<script>"字符串。支持 IPv4 和 IPv6 格式。IPv4 地址格式为 A.B.C.D。IPv6 地址格式为 X:X:X:X:X:X:X:X/(0-128)，其中 X 为一个 4 位十六进制整数。
zone <*mstring*>	可选项，设置防护区域名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。

ddos blacklist show [**zone** <*string*>]

命令描述：

查看 DDoS 防御中的黑名单。

参数说明：

参数	说明
zone <*string*>	可选项，设置防护区域名称。 字符串类型，不包含" &\"'\\'%<>"中任意字符以及空格。

命令示例：

TopsecOS# **ddos blacklist show**

TopWAF source list: source_num=0

ddos config clean <cr>

命令描述：

清除 DDoS 防御的所有配置信息。

ddos learntime modify time <*num*>

命令描述：

设置 DDoS 自学习的周期。

参数说明：

参数	说明
modify time <*num*>	必选项，自学习的周期。 实数类型，取值范围：1-65535；单位：分钟。

ddos learntime show <*cr*>

命令描述：

查看 DDoS 自学习周期配置信息。

命令示例：

TopsecOS# **ddos learntime show**

ddos learn time 5(minutes)

ddos log set < **atk_log**| **flow_log** > **writedb** <enable|disable>

命令描述：

设置 DDoS 攻击日志和流量日志功能开启或者关闭。

参数说明：

参数	说明
atk_log| **flow_log**	必选项，设置日志类型。
writedb <enable|disable>	设置是否写入数据库。 开启|关闭。

命令示例：

TopsecOS# **ddos log set flow_log writedb** enable

ddos log add interval <*num*>

命令描述：

设置 DDoS 日志发送时间间隔。

可使用 **ddos log del interval** <*number*>命令删除日志发送时间间隔配置，恢复为默认值。

参数说明：

参数	说明
interval <*num*>	必选项，DDoS 日志发送时间间隔。 实数类型，取值范围：1-10；单位：分钟；默认值：1

命令示例：

TopsecOS# **ddos log add interval** 5

ddos log show interval <cr>

命令描述：

查看 DDoS 日志发送时间间隔。

命令示例：

TopsecOS# **ddos log show interval**

ddos log add interval 1

ddos log show safe parameter<cr>

命令描述：

查看 DDoS 日志导出文件列表。

ddos show [spec-information|stat|zone]

命令描述：

查看 DDoS 防御功能的配置信息。

参数说明：

参数	说明
spec-information|stat|zone	规格信息|丢弃统计信息|防护区域名称，如果不设置表示查看 DDoS 防御功能的所有配置信息。

命令示例：

查看 DDoS 规格信息。

```
TopsecOS# ddos show spec-information

ddos device spec:

device type : clean

zone number : 128

group number : 1024

ip segment : 1000

sever node : 32

source node : 128

whilte-black list : 1024


ADS_ATOMOBJ_IP :on

ADS_ATOMOBJ_TCP :on

ADS_ATOMOBJ_UDP :off

ADS_ATOMOBJ_ICMP :off

ADS_ATOMOBJ_HTTP :on
```

ADS_ATOMOBJ_HTTPS :on

ADS_ATOMOBJ_SIP :off

ADS_ATOMOBJ_NTP :off

ADS_ATOMOBJ_DNS :off

ADS_ATOMOBJ_FILTER :off

ADS_ATOMOBJ_FLOW :off

ZONE_DEFAULT_DEFINITION :off

ADS_OTHER_MODULE_DEBUG :off

ADS_OTHER_MODULE_BGP :off

ADS_OTHER_MODULE_MPLS :off

查看 DDoS 防御功能所有配置信息。

TopsecOS# **ddos show**

ddos log add interval 1

ddos global set deployscene offline

ddos global set default-group off

ddos global set stat ethernet

ddos global set stat ratio 7

ddos global set retransmit timeout 5

ddos global set whitelist timeout 5

ddos global set blacklist timeout 5

ddos global set source timeout 300

ddos global set server timeout 60

ddos global set security_level low

ddos global set related-auth off

ddos global set filter on

ddos global set cdn-check off

ddos global set devtype clean

ddos global set confirmtime start-time 12 end-time 34

ddos global add dns retrans-interval after 2 before 5

ddos templet add name 123

ddos zone add name 123

ddos zone add name 123 templet 123

ddos zone add name 123 baseline-learn accept on

查看 DDoS 防御功能丢弃报文的统计信息。

TopsecOS# **ddos show stat**

ads entry =234989

total recv =0

total drop =0

total pass =0

查看 DDoS 防御区域名称。

TopsecOS# **ddos show zone**

ddos zone add name 100

ddos zone add name 11

ddos zone add name aa

ddos zone add name aaa

ddos zone add name anti-ddos

ddos zone add name 123

ddos source show [**configuration**|**grp_id** <*num*>]

命令描述：

查看 DDoS 攻击源信息。

参数说明：

参数	说明
configuration	查看黑白名单超时配置信息。
grp_id <*num*>	查看保护组信息。 实数类型。

命令示例：

查看 DDoS 的黑白名单超时配置信息。

TopsecOS# **ddos source show configuration**

ddos global set whitelist timeout 5

ddos global set blacklist timeout 5

查看 DDoS 的查看保护组信息。

TopsecOS# **ddos source show grp_id** *1*

TopWAF source list: source_num=0

ddos templet add name <*mstring*> **service** <http> **atk-detect** <flood> [**alert-rate** <*num*>]

命令描述：

配置 HTTP 洪泛攻击防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-detect** <flood>命令删除洪泛攻击防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-detect <flood>	设置 DDoS 攻击检测类型。 配置洪泛类型的攻击检测。
alert-rate <*num*>	设置 HTTP Flood 攻击检测的阈值。流量速率阈值单位：pps；取值范围：1-1200000；默认值：2000。 实数类型。

ddos templet add name <*mstring*> **service** <http> **atk-detect** <monitored-uri> **index** <*num*> **uri** < *mstring* > [**match-mode** <blur-match|full-match>]

命令描述：

配置 HTTP 监控 URI 的匹配规则。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-detect** <monitored-uri> **{index** <*num*>|**all**}命令删除 HTTP 监控 URI 的匹配规则。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-detect <monitored-uri>	设置 DDoS 攻击检测类型。 配置 HTTP 监控 URI 的匹配规则

参数	说明
index <*num*>	设置匹配规则的索引号。 实数类型。取值范围：1-10。
uri <*mstring*>	设置域名或 URI。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。长度：1-255。
match-mode <blur-match|full-match>	设置匹配模式。 模糊匹配|完全匹配。

ddos templet add name <*mstring*> **service** <http> **atk-detect** <new-conn-flood> [**alert-rate** <*num*>]

命令描述：

配置 HTTP 新建连接洪泛攻击防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-detect** <new-conn-flood>命令删除新建连接洪泛攻击防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-detect <new-conn-flood>	设置 DDoS 攻击检测类型。 配置新建连接洪泛攻击的攻击检测。
alert-rate <*num*>	可选项，设置 Flood 攻击的新建连接阈值。流量速率阈值单位：cps；取值范围：1-1200000；默认值：1000。 实数类型。

ddos templet add name <*mstring*> **service** <http> **atk-detect** <uri-cc> [**cycle** <*num*>] [**dst-alert-number** <*num*>]

命令描述：

配置 HTTP URI CC 攻击防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-detect** <uri-cc>命令删除 URI CC 攻击防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-detect <uri-cc>	设置 DDoS 攻击检测类型。 配置 URI CC 攻击的攻击检测。
cycle <*num*>	可选项，设置监控时间间隔。 实数类型，单位：s；取值范围：1-65535；默认值：4。
dst-alert-number <*num*>	可选项，设置服务器端指定 URI 报文数的阈值。 实数类型，单位：p；取值范围：1-1200000；默认值：2000。

ddos templet add name <*mstring*> **service** <http> **atk-detect** <concur-conn-flood> [**alert-number** <*num*>]

命令描述：

配置 HTTP 并发连接攻击防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-detect** <concur-conn-flood>命令删除 HTTP 并发连接攻击防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-detect <concur-conn-flood>	设置 DDoS 攻击检测类型。 配置并发连接洪泛攻击的攻击检测。

参数	说明
alert-number <*num*>	可选项，设置基于 HTTP 协议的并发连接数。 实数类型。单位：conns；取值范围：1-1200000；默认值：1000。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <src-concur-conn-check>

alert-num <*num*> **action** <blacklist|drop>

命令描述：

配置 HTTP Flood 源 IP 限速防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <src-concur-conn-check>命令删除 HTTP Flood 源 IP 限速防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <src-concur-conn-check>	设置 DDoS 攻击防御方式。 配置源 IP 限速的攻击防御策略。
alert-num <*num*>	设置最大异常连接数。 实数类型。取值范围：0-20000；默认值：200。
action <blacklist|drop>	设置执行动作。 加入黑名单|丢弃。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <src-new-conn-check> **alert-rate** <*num*> **action** <blacklist|drop>

命令描述：

配置 HTTP Flood 源新建连接速率防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <src-new-conn-check>命令删除 HTTP Flood 源新建连接速率防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <src-new-conn-check>	设置 DDoS 攻击防御方式。 配置源新建连接速率的攻击防御策略。
alert-rate <*num*>	设置最大新建连接数。 实数类型。取值范围：0-6000；默认值：60。
action <blacklist|drop>	设置执行动作。 加入黑名单|丢弃。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <src-rate-check> **alert-rate** <*num*> **action** <blacklist|drop>

命令描述：

配置 HTTP Flood 源并发连接速率防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <src-rate-check>命令删除 HTTP Flood 源并发连接速率防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <src-rate-check>	设置 DDoS 攻击防御方式。 配置源并发连接速率的攻击防御策略。
alert-rate <*num*>	设置最大并发连接数。 实数类型。取值范围：0-6000；默认值：60。

参数	说明
action <blacklist|drop>	设置执行动作。 加入黑名单|丢弃。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <src-auth> **mode** <redirect|verify-code> **max-failed-times** <*num*>

命令描述：

配置 HTTP Flood 源认证防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <src-auth>命令删除 HTTP Flood 源认证防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <src-auth>	设置 DDoS 攻击防御方式。 配置源认证的攻击防御策略。
mode <redirect|verify-code>	设置源认证的认证模式。 重定向|验证码，默认值：重定向
max-failed-times <*num*>	设置源认证的最大失败次数。 实数类型。取值范围：0-65535；默认值：0。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <dst-concur-conn-check> **alert-num** <*num*> **action** <drop>

命令描述：

配置 HTTP Flood 目的 IP 限速防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <dst-concur-conn-check>命令删除 HTTP Flood 目的 IP 限速防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <dst-concur-conn-check>	设置 DDoS 攻击防御方式。 配置目的 IP 限速的攻击防御策略。
alert-num <*num*>	设置最大并发连接数。 实数类型。取值范围：0- 4294967295；默认值：20000；单位：pps。
action <drop>	设置执行动作。 丢弃。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <dst-new-conn-check> **alert-rate** <*num*> **action** <drop>

命令描述：

配置 HTTP Flood 目的新建连接速率防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <dst-new-conn-check>命令删除 HTTP Flood 目的新建连接速率防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <dst-new-conn-check>	设置 DDoS 攻击防御方式。 配置目的新建连接速率的攻击防御策略。
alert-rate <*num*>	设置最大新建连接数。 实数类型。取值范围：0-400000；默认值：2000；单位：cps。
action <drop>	设置执行动作。

参数	说明
	丢弃。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <dst-rate-check> **alert-rate** <*num*> **action** <drop>

命令描述：

配置 HTTP Flood 目的并发连接速率防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <dst-rate-check>命令删除 HTTP Flood 目的并发连接速率防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <dst-rate-check>	设置 DDoS 攻击防御方式。 配置目的并发连接速率的攻击防御策略。
alert-rate <*num*>	设置最大并发连接数。 实数类型。取值范围：0-400000；默认值：2000；单位：cps。
action <drop>	设置执行动作。 丢弃。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <uri-monitor> **src-alert-ratio** <*num*>

命令描述：

配置 HTTP URI 监控策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <uri-monitor>命令删除 HTTP URI 监控策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <uri-monitor>	设置 DDoS 攻击防御方式。 配置 HTTP URI 监控策略。
src-alert-ratio <*num*>	设置客户端访问指定 URI 的比例上限。单位：percent；取值范围：1-100；默认值：30。 实数类型。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <slow-header-monitor> **max-time** <*num*> **max-abn-conns** <*num*>

命令描述：

配置 HTTP 慢速 header 监控防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <slow-header-monitor>命令删除 HTTP 慢速 header 监控防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <slow-header-monitor>	设置 DDoS 攻击防御方式。 配置慢速 header 监控防御策略。
max-time <*num*>	设置最大传输时间。 实数类型。单位：second；取值范围：1-65535；默认值：8。
max-abn-conns <*num*>	设置最大异常连接数。 实数类型。单位：conns；取值范围：1-65535；默认值：10。

ddos templet add name <*mstring*> **service** <http> **atk-defend** <slow-post-monitor> **max-time** <*num*> **min-speed** <*num*> **max-abn-conns** <*num*>

命令描述：

配置 HTTP 慢速 header 监控防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <http> **atk-defend** <slow-post-monitor>命令删除 HTTP 慢速 header 监控防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <http>	设置防护策略的协议类型。 配置基于 HTTP 协议的防护策略。
atk-defend <slow-post-monitor>	设置 DDoS 攻击防御方式。 配置慢速 header 监控防御策略。
max-time <*num*>	设置最大传输时间。 实数类型。单位：second；取值范围：1-65535；默认值：8。
min-speed <*num*>	可选项，设置最小传输速率。 实数类型。单位：Bps；取值范围：1-65535；默认值：1。
max-abn-conns <*num*>	设置最大异常连接数。 实数类型。单位：conns；取值范围：1-65535；默认值：10。

ddos templet add name <*mstring*> **service** <https> **atk-detect** <flood> [**alert-rate** <*num*>]

命令描述：

配置 HTTPS 洪水攻击检测防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-detect** <flood>命令删除 HTTPS 洪水攻击检测防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。

参数	说明
	字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-detect <flood>	设置 DDoS 攻击检测类型。 配置洪水类型的攻击检测。
alert-rate <*num*>	可选项，设置 HTTPS Flood 攻击检测的阈值。 实数类型。流量速率阈值单位：pps；取值范围：1-1200000；默认值：2000。

ddos templet add name <*mstring*> **service** <https> **atk-detect** <new-conn-flood> [**alert-rate** <*num*>]

命令描述：

配置 HTTPS 新建连接洪水攻击检测防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-detect** <new-conn-flood>命令删除 HTTPS 新建连接洪水攻击检测防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-detect <new-conn-flood>	设置 DDoS 攻击检测类型。 配置新建连接洪水攻击的攻击检测。
alert-rate <*num*>	可选项，设置 Flood 攻击的新建连接阈值。 实数类型。流量速率阈值单位：cps；取值范围：1-1200000；默认值：1000。

ddos templet add name <*mstring*> **service** <https> **atk-detect** <concur-conn-flood> [**alert-number** <*num*>]

命令描述：

配置 HTTPS 并发连接攻击检测防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-detect** <concur-conn-flood>命令删除 HTTPS 并发连接攻击检测防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-detect <concur-conn-flood>	设置 DDoS 攻击检测类型。 配置并发连接洪水攻击的攻击检测。
alert-number <*num*>	可选项，设置基于 HTTPS 协议的并发连接数。 实数类型。单位：conns；取值范围：1-1200000；默认值：1000。

ddos templet add name <*mstring*> **service** <https> **atk-defend** <src-concur-conn-check> **alert-num** <*num*> **action** <blacklist|drop>

命令描述：

配置 HTTPS Flood 源 IP 限速防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-defend** <src-concur-conn-check>命令删除 HTTPS Flood 源 IP 限速防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-defend <src-concur-conn-check>	设置 DDoS 攻击防御方式。 配置源 IP 限速的攻击防御策略

参数	说明
alert-num <*num*>	设置最大异常连接数。 实数类型。取值范围：0-20000；默认值：200。
action <blacklist|drop>	设置执行动作。 加入黑名单|丢弃。

ddos templet add name <*mstring*> **service** <https> **atk-defend** <src-new-conn-check> **alert-rate** <*num*> **action** <blacklist|drop>

命令描述：

配置 HTTPS Flood 源新建连接速率防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-defend** <src-new-conn-check>命令删除 HTTPS Flood 源新建连接速率防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-defend <src-new-conn-check>	设置 DDoS 攻击防御方式。 配置源新建连接速率的攻击防御策略。
alert-rate <*num*>	设置最大新建连接数。 实数类型。取值范围：0-6000；默认值：60。
action <blacklist|drop>	设置执行动作。 加入黑名单|丢弃。

ddos templet add name <*mstring*> **service** <https> **atk-defend** <src-rate-check> **alert-rate** <*num*> **action** <blacklist|drop>

命令描述：

配置 HTTPS Flood 源并发连接限速防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-defend** <src-rate-check>命令删除 HTTPS Flood 源并发连接限速防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-defend <src-rate-check>	设置 DDoS 攻击防御方式。 配置 HTTPS Flood 源限速的攻击防御策略。
alert-rate <*num*>	设置最大速率。 实数类型。单位：pps；取值范围：0-4294967295；默认值：20000。
action <blacklist|drop>	设置执行动作。 加入黑名单|丢弃。

ddos templet add name <*mstring*> **service** <https> **atk-defend** <ssl-dos-monitor> **cycle** <*num*> **max-renegotiation-times** <*num*> **max-abn-conns** <*num*>

命令描述：

配置 HTTPS 的 ssl-dos 攻击防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-defend** <ssl-dos-monitor>命令删除 HTTPS 的 ssl-dos 攻击防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-defend <ssl-dos-monitor>	设置 DDoS 攻击防御方式。 配置 ssl-dos 监控防御策略。
cycle <*num*>	设置 ssl-dos 攻击防范的周期。

参数	说明
	实数类型。单位：second；取值范围：1-65535；默认值：2。
max-renegotiation-times <*num*>	设置最大重协商次数。 实数类型。取值范围：1-65535；默认值：4。
max-abn-conns <*num*>	设置最大异常连接数。 实数类型。单位：conns；取值范围：1-65535；默认值：10。

ddos templet add name <*mstring*> **service** <https> **atk-defend** <src-auth> **max-failed-times** <*num*>

命令描述：

配置 HTTPS Flood 源认证防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-defend** <src-auth>命令删除 HTTPS Flood 源认证防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-defend <src-auth>	设置 DDoS 攻击防御方式。 配置源认证的攻击防御策略。
max-failed-times <*num*>	设置源认证的最大失败次数。 数值类型。取值范围：0-65535；默认值：0。

ddos templet add name <*mstring*> **service** <https> **atk-defend** <dst-concur-conn-check> **alert-num** <*num*> **action** <drop>

命令描述：

配置 HTTPS Flood 目的 IP 限速防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-defend** <dst-concur-conn-check>命令删除 HTTPS Flood 目的 IP 限速防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-defend <dst-concur-conn-check>	设置 DDoS 攻击防御方式。 配置目的 IP 限速的攻击防御策略。
alert-num <*num*>	设置最大并发连接数。 实数类型。取值范围：0-1200000；默认值：8000。
action <drop>	设置执行动作。 丢弃。

ddos templet add name <*mstring*> **service** <https> **atk-defend** <dst-new-conn-check> **alert-rate** <*num*> **action** <drop>

命令描述：

配置 HTTPS Flood 目的新建连接速率防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-defend** <dst-new-conn-check>命令删除 HTTPS Flood 目的新建连接速率防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-defend <dst-new-conn-check>	设置 DDoS 攻击防御方式。 配置目的新建连接速率的攻击防御策略。
alert-rate <*num*>	设置最大新建连接数。

参数	说明
	数值类型。取值范围：0-400000；默认值：2000。
action <drop>	设置执行动作。 丢弃。

ddos templet add name <*mstring*> **service** <https> **atk-defend** <dst-rate-check> **alert-rate** <*num*> **action** <drop>

命令描述：

配置 HTTPS Flood 目的并发连接限速防御策略。

可使用 **ddos templet del name** <*mstring*> **service** <https> **atk-defend** <dst-rate-check>命令删除 HTTPS Flood 目的并发连接限速防御策略。

参数说明：

参数	说明
name <*mstring*>	必选项，设置策略模板名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
service <https>	设置防护策略的协议类型。 配置基于 HTTPS 协议的防护策略。
atk-defend <dst-rate-check>	设置 DDoS 攻击防御方式。 配置 HTTPS Flood 目的限速的攻击防御策略。
alert-rate <*num*>	设置最大速率。单位：pps；取值范围：0-4294967295；默认值：20000。 实数类型。
action <drop>	设置执行动作。 丢弃。

ddos zone add name <*mstring*> [**baseline-learn switch** <on|off>]

命令描述：

添加防护对象，设置防护对象的基线学习开关。

参数说明：

参数	说明
name <*mstring*>	必选项，设置防护对象名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
baseline-learn switch <on|off>	设置基线学习开关。 打开|关闭。

命令示例：

TopsecOS# **ddos zone add name** *http* baseline-learn **switch** on

ddos zone add name <*mstring*> [**baseline-learn accept** <on|off>]

命令描述：

设置防护对象的基线学习结束后学习结果直接下发。

参数说明：

参数	说明
name <*mstring*>	必选项，设置防护对象名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
baseline-learn accept <on|off>	设置基线学习结束后的学习结果是否直接下发。 打开|关闭。

命令示例：

将防护对象基线学习结束后的学习结果直接下发的示例：

TopsecOS# **ddos zone add name** *http* baseline-learn **accept** on

ddos zone add name <*mstring*> [**baseline-learn learn-cfg** [**learn-interval** <*num*>] [**learn-sleep** <*num*>] [**learn-tolerance** <*num*>]]

命令描述：

添加防护对象，设置防护对象的基线学习时间。

可使用 **ddos zone del name** <*mstring*>[**templet**]命令删除防护对象。

参数说明：

参数	说明
name <*mstring*>	必选项，设置防护对象名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
baseline-learn learn-cfg	设置基线学习时间。
learn-interval <*num*>	设置基线学习的学习时间长度。 实数类型。单位：分钟；取值范围：1-65535；默认值：1。
learn-sleep <*num*>	设置基线学习周期。 实数类型。单位：分钟；取值范围：1-65535。
learn-tolerance <*num*>	设置学习结果下发时的容忍度。 实数类型。单位：百分比；取值范围：1-500；默认值：50。

命令示例：

TopsecOS# **ddos zone add name** *http* baseline-learn **learn-cfg learn-interval** *10*

ddos zone add name <*mstring*> [**baseline-learn loop** <on|off>]

命令描述：

添加防护对象，设置是否开启防护对象的基线周期学习功能。

可使用 **ddos zone del name** <*mstring*>[**templet**]命令删除防护对象。

参数说明：

参数	说明
name <*mstring*>	必选项，设置防护对象名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
baseline-learn loop <on|off>	设置基线学习循环。 打开|关闭。

命令示例：

TopsecOS# **ddos zone add name** *http* baseline-learn **loop** on

ddos zone add name <*mstring*> [**baseline-learn service** <http-flood|https-flood>]

命令描述：

添加防护对象，设置防护对象的基线学习结果手动下发的模块名称。

可使用 **ddos zone del name** <*mstring*>[**templet**]命令删除防护对象。

参数说明：

参数	说明
name <*mstring*>	必选项，设置防护对象名称。 字符串类型，不以'\\'结尾或不包含"<script>"字符串。最长不能超过 32 个字符。
baseline-learn service <http-flood|https-flood>	设置基线学习结果手动下发的模块名称。 HTTP 攻击防御|HTTPS 攻击防御。

命令示例：

TopsecOS# **ddos zone add name** *http* baseline-learn **service** http-flood

6.4 防火墙联动

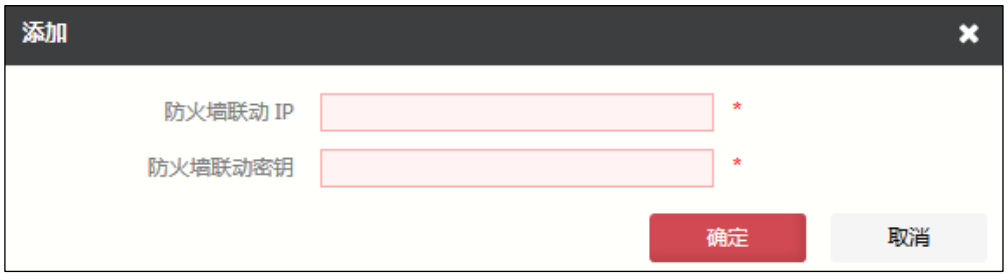
TopWAF 支持与防火墙联动功能。从而可以实现由 TopWAF 进行监听，由联动防火墙进行阻断的安全策略。

TopWAF 只能与天融信防火墙进行联动，要实现防火墙联动功能，需要在天融信防火墙中设置 IDS 联动，并开启 ids 服务。关于如何在天融信防火墙中设置 IDS 联动具体请参见天融信防火墙相关手册。

WEBUI 方式

步骤1 选择 **网络层防护 > 防火墙联动**，激活“联动配置”页签，如下图所示。

步骤2 点击『添加』，设置要联动的防火墙信息，如下图所示。



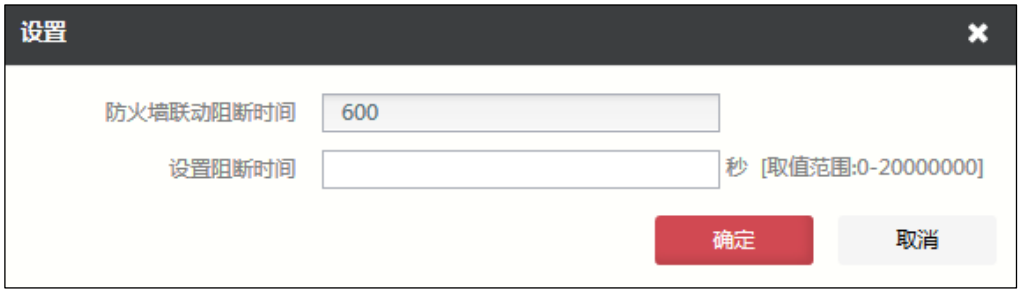
在设置联动配置时，各项参数的具体说明如下表所示。

参数	说明
防火墙联动 IP	输入要联动的防火墙 IP 地址。
防火墙联动密钥	设置共享密钥，该密钥由联动的防火墙生成。需联系防火墙管理员获取，具体请参见天融信防火墙相关手册。

点击【确定】按钮完成防火墙的添加。

步骤3 对已经添加的防火墙，可以点击『编辑』、『删除』、『清空』执行相应的操作。

步骤4 对于需要防火墙阻断的进程，用户可以自行设置对其进行阻断的时间。点击上方的『阻断时间设置』，如下图所示。



在设置阻断时间时，各项参数的具体说明如下表所示。

参数	说明
防火墙联动阻断时间	显示当前防火墙联动阻断的时间
设置阻断时间	在此处输入新的阻断时间。 单位：秒；取值范围：0-20000000，0 表示永远阻断。

输入新的阻断时间，点击【确定】按钮使设置生效。

步骤5 用户可以激活“联动状态”页签，查看防火墙联动是否成功。如下图所示。

CLI 方式

waf firewall-link add ip <*ip*> **key** <*string*>

命令描述：

添加一个防火墙联动。

可用 **waf firewall-link clean** 命令清空防火墙联动信息。

参数说明：

参数	说明
ip <*ip*>	必选项，设置联动的防火墙 IP 地址。
key <*string*>	必选项，设置防火墙联动共享密钥。 字符串类型，不包含" &\"\\'%<>" 中任意字符以及空格。

waf firewall-link modify id <*num*> **ip** <*ip*> **key** <*string*>

命令描述：

修改防火墙联动信息。

参数说明：

参数	说明
id <*num*>	必选项，指定要修改的防火墙联动配置 ID 号。 实数类型。
ip <*ip*>	必选项，指定要修改的联动的防火墙 IP 地址。 IPv4 地址类型。输入 0 或 0.0.0.0 或 255.255.255.255 是合法的
key <*string*>	必选项，指定要修改的防火墙联动共享密钥。 字符串类型，不包含" &\"\\'%<>" 中任意字符以及空格。

waf firewall-link block-time-set <*num*>

命令描述：

设置防火墙联动阻断时间。

参数说明：

参数	说明
block-time-set <*num*>	必选项，设置联动阻断时间。 实数类型，单位：秒。取值范围：0-20000000。

waf firewall-link show [server|status|block-time]

命令描述：

显示防火墙联动信息。

参数说明：

参数	说明
server|status|block-time	必选项，设置要显示的联动信息。 服务器配置|防火墙联动状态|联动阻断时间。

命令示例：

显示服务器配置。

TopsecOS# **waf firewall-link show** server

ID 8011 waf firewall-link add ip 192.168.25.211 key 6K2DW8CC33X6ZMZ9

ID 8019 waf firewall-link add ip 1.2.1.2 key 111111

显示防火墙联动状态。

TopsecOS# **waf firewall-link show** status

firewall ip: 192.168.25.211 status: running

firewall ip: 1.2.1.2 status: stop key wrong

显示联动阻断时间。

TopsecOS# **waf firewall-link show** block-time

waf firewall-link block-time-set 100

7 网络管理

TopWAF 作为一种防护 Web 服务器的专用网络安全设备，支持以在线串接和旁路的方式接入网络，能对需防护的 Web 服务器提供 Web 保护、离线检测、服务器负载均衡和反向代理的功能，具体部署模式详细介绍请参见 5.3 服务器策略。因此在安装 TopWAF 之前，网络管理人员应根据网络应用的实际情况以及网络中主机、服务器等设备的安全属性来规划安全区域，通过 TopWAF 的网络管理功能，合理设置 TopWAF。

本章主要内容包括：

- 接口：主要介绍如何设置 TopWAF 上的物理接口、MAC 子接口、VLAN、虚拟线、聚合接口以及联动接口。
- 路由：主要介绍 TopWAF 路由的设置方式。
- 邻居：主要介绍如何在 TopWAF 上设置 ARP 和 Neighbour 信息。
- MAC：主要介绍如何在 TopWAF 上设置 MAC。
- 链路探测：TopWAF 按照配置，周期性探测链路状态。

7.1 接口

接口是设备与网络中其他设备交换数据并相互作用的枢纽，按照性质分为物理接口和逻辑接口。物理接口是指真实存在于设备上的接口，如设备上的以太网接口 feth0 等，广义的物理接口包括 Console 口等。逻辑接口是指能够实现数据交换功能但物理上不存在，并且需要通过配置建立的接口。

TopWAF 的物理接口仅指以太网接口，逻辑接口包括 MAC 子接口、VLAN 虚接口、虚拟线和聚合接口。

- MAC 子接口是在路由模式的单个物理接口上配置的多个逻辑接口。子接口共用物理接口的物理参数配置，但有各自的链路层和网络层配置参数，如 MAC 地址和 IP 地址。在不增加物理接口的情况下，子接口是扩展路由接口的方案。

- VLAN 虚接口是 VLAN 内所有设备对外通信的出口。VLAN 虚接口是 VLAN 内所有以太网接口的集合，只要 VLAN 内有一个以太网接口处于 UP 状态，该 VLAN 虚接口就处于 UP 状态。
- 虚拟线是将 TopWAF 上的两个工作在路由模式的物理接口逻辑上相连，此时，可将 TopWAF 看做一根具有防护功能的网线。
- 聚合接口是将多个物理接口聚合成一个逻辑接口，可以使设备之间的带宽成倍增加、增强端口灵活性并提供链路冗余。当聚合接口内的某条链路出现故障时，该链路的流量将自动转移到其余链路上。

7.1.1 物理接口

物理接口支持快速以太网接口（速率为 10/100Mbit/s）、千兆以太网接口（速率为 1000Mbit/s）和万兆以太网网接口（速率为 10Gbit/s）。

TopWAF 的物理接口支持四种工作模式：路由模式、交换模式、虚拟线模式和嗅探模式。在实际应用中，管理员可根据需求进行配置。

- 路由模式

在路由模式下，接口为三层接口，工作在网络层，可配置 IPv4 或 IPv6 地址，对不同网段间的数据进行三层路由和转发。

- 交换模式

在交换模式下，接口为二层接口，工作在数据链路层。处于同一个交换域的主机加入 VLAN 后，可以互相通过该 VLAN 进行通信，实现对数据二层转发。接口工作模式可分为 Access 模式和 Trunk 模式。

1）Access 模式：在 Access 模式下，同一接口可发送一个 VLAN 的报文，通常用于连接终端设备，如 PC、服务器等。

2）Trunk 模式：在 Trunk 模式下，同一接口可发送多个 VLAN，通常用于网络设备间互联，如交换机，路由器等。

- 嗅探模式

接口工作在嗅探模式时，只接收报文，不进行转发。

- 虚拟线模式

在 TopWAF 设备中，一条虚拟线只有接口 A 和接口 B 两个工作接口，接口 A 接收到的数据包，除了目的地址为 TopWAF 的数据报文外，直接从接口 B 转发出去，关于虚拟线的配置具体请参见 7.1.4 虚拟线。

- SLAVE 模式

工作在路由模式的物理接口加入到聚合接口后，该物理接口将工作在 SLAVE 模式。关于聚合接口的配置具体请参见 7.1.5 链路聚合。

设备如果需要连接到网络中，并能正常通信，必须配置接口的 IP 地址。目前 IP 地址有 2 个版本：IPv4 和 IPv6。

WEBUI 方式

步骤1 选择 **网络管理** > **接口** > **物理接口**。

步骤2 点击某接口对应的操作图标“”，可设置该接口的相关属性参数。

1）设置接口的基本属性：包括接口工作模式、是否启用该接口以及接口描述信息。

在设置基本属性时，各项参数的具体说明如下表所示。

参数	说明
名称	显示接口名称。
状态	默认接口为“启用”状态，表示可以使用该接口；如勾选“停用”，则表示该接口将不会工作，该接口所在的区域将无法和其他接口进行通讯。
模式	设定接口的工作模式，可选项：路由模式、交换模式、嗅探模式、虚拟线和 SLAVE。接口默认工作在路由模式。当该接口处于 SLAVE 模式时，“模式”不可编辑，关于聚合接口的配置具体请参见 7.1.5 链路聚合。
描述	输入对该接口的简要描述。

2）设置接口在不同工作模式下的属性。

（a）路由模式

当在“基本信息”处设置接口工作在“路由”模式时，需要设置接口的 IP 地址及其掩码。

在设置接口地址时，各项参数的具体说明如下表所示。

参数	说明
非同步地址	如果在网络中配置了高可用性功能，则设置心跳口 IP 时必须要选择“非同步地址”，否则接口的 IP 地址信息会在主/从设备同步运行状态时被对方覆盖。热备组中的备设备的管理 IP 必须选择“非同步地址”，否则无法对备设备进行管理。关于高可用性的配置具体请参见 8.6 高可用性。
IPv4 地址/掩码	输入接口的 IPv4 地址及其子网掩码。 说明： 1）可以为路由接口设置多个 IPv4 地址。 2）TopWAF 不支持不同的物理接口配置相同的 IPv4 地址或 IPv4 地址在同一子网内。
添加	如果“地址/掩码”设置正确，点击“”图标，接口的 IPv4 地址会显示在列表中。
删除	点击 IPv4 地址对应的“”图标，在确认提示框中点击【确定】按钮，可以删除已添加的 IPv4 地址。
IPv6 地址	输入接口的 IPv6 地址/前缀长度。 说明： 1）可以为路由接口设置多个 IPv6 地址。 2）TopWAF 不支持不同的物理接口配置相同的 IPv6 地址或 IPv6 地址在同一子网内。
添加	如果“IPv6 地址”设置正确，点击“”图标，则新添加接口的 IPv6 地址会显示在列表中。
删除	点击 IPv6 地址对应的“”图标，然后在确认提示框中点击【确定】按钮，可以删除已添加的 IPv6 地址。

（b）交换模式

当在“基本信息”处设置接口工作在“交换”模式时，需要设置接口类型为“access”或“trunk”的接口。

在设置接口交换模式基本属性时，各项参数的具体说明如下表所示。

参数	说明
类型	设置该交换接口的类型。可选项：access 和 trunk。
VLAN ID	设置接口所属的 VLAN ID，取值范围：1-4094。 当“类型”为“access”时，此参数用于指定 Access 口所属的 VLAN ID 号码。 当“类型”为“trunk”时，此参数用于指定 Trunk 接口的 Native VLAN。
VLAN 范围	仅当“类型”为“trunk”时，需要设置该项。 用于设置该 Trunk 接口允许哪些 VLAN 的报文通过。VLAN 值的取值范围：1-4094。 格式举例：

参数	说明
	1-10 表示属于 VLAN1 到 VLAN 10； 1，10 表示属于 VLAN1 和 VLAN10。

（c）嗅探模式

在“基本信息”处选择接口工作为“嗅探”。

（d）虚拟线模式

当在“基本信息”处设置接口工作在“虚拟线”模式时，需要设置虚拟线的对端接口。设置完成后对端接口的工作模式自动设置为虚拟线模式。关于虚拟线功能说明，具体请参见 7.1.4 虚拟线。

（e）SLAVE 模式

当物理接口加入到聚合接口后，其工作模式为 SLAVE，关于聚合接口的配置具体请参见 7.1.5 链路聚合。

步骤3 点击『高级』进行高级属性的设置。

在设置高级属性时，各项参数的具体说明如下表所示。

参数	说明
MTU	设置指定接口的 MTU。单位：字节；取值范围：68-1500；默认值：1500。
MSS	设置指定接口的 MSS 值。可选项：自适应、关闭和自定义；设置为自定义时的取值范围：200-1460。
双工模式	设置物理接口的双工模式。可选项：自适应、半双工、全双工；默认值：自适应。
速率	设置物理接口的速率。可选项：自适应、10Mb/s、100Mb/s、1000Mb/s、10000Mb/s；默认值：自适应。

步骤4 设置完成后，点击【确定】按钮完成接口的设置。

步骤5 查看接口流量信息。点击接口名称，弹出接口的流量统计信息对话框，如下图所示。

CLI 配置

设置接口为路由模式，并配置相关属性。

默认情况下，TopWAF 的所有物理接口均工作在路由模式。如果接口被设置成工作在监听模式、交换模式或虚拟线模式时，通过执行如下命令，可以使接口工作在路由模式。

network interface <*string*> **ip add** <*hostip*> **[mask** <*string*>**] [**ha-static**]**

命令描述：

给接口添加 IPv4 地址，一个接口可添加多个 IPv4 地址。

可使用 **network interface** <*string*> **ip delete** 命令删除接口的 IPv4 地址。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待添加 IPv4 地址的接口。 字符串类型，可为物理接口或虚接口。
add <*hostip*>	必选项，添加 IPv4 地址。 IPv4 地址类型，IPv4 地址格式为 A.B.C.D。
mask <*string*>	可选项，设置子网掩码。 子网掩码类型。例如 255.255.255.0。
ha-static	可选项，设置接口 IP 地址为非同步地址。

使用说明：

✧ 如果在添加接口 IPv4 地址时，只设置了 IPv4 地址并没有设置掩码，系统根据 IPv4 地址自动为该 IPv4 添加主类子网掩码。

命令示例：

给 feth0 添加 IPv4 地址为：192.168.90.75。

TopsecOS# **network interface** *feth0* **ip add** *192.168.90.75*

network interface <*string*> **ip clean** <cr>

命令描述：

清空某接口所有的 IPv4 地址。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待清空 IPv4 地址的接口。 字符串类型，可为物理接口和虚接口。

使用说明：

✧ TopWAF 的物理接口支持 IPv4 地址和 IPv6 地址，虚接口不支持 IPv6 地址。

命令示例：

清空 feth2 接口上所有的 IPv4 地址。

TopsecOS# **network interface** *feth2* **ip clean**

network interface <*string*> **ipv6 add** <*ip6*> **prefix** <*num*> **[**ha-static**]**

命令描述：

添加接口的 IPv6 地址。

可使用 **network interface** <*string*> **ipv6 delete** 命令删除接口的 IPv6 地址。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待添加 IPv6 地址的接口。 字符串类型，可为物理接口和虚接口。
add <*ip6*>	必选项，添加 IPv6 地址。 IPv6 地址字符串，IPv6 地址格式为 X:X:X:X:X:X:X:X，其中 X 为一个四位十六进制整数。
prefix <*num*>	必选项，设置 IPv6 地址网络前缀。 实数类型。取值范围：0-128。
ha-static	可选项，设置接口 IP 地址为非同步地址。

命令示例：

添加 feth0 接口的 IPv6 地址为 12AB::CD30/64。

TopsecOS# **network interface** *feth0* **ipv6 add** *12ab::cd30* **prefix** *64*

TopsecOS# **network interface** *feth0* **show** configuration

network interface feth0 vsid 0

network interface feth0 mtu 1500

network interface feth0 ip add 192.168.90.78 mask 255.255.255.0 label 0

network interface feth0 ipv6 add 12ab::cd30 prefix 64

network interface feth0 speed auto

network interface feth0 duplex auto

network interface feth0 no switchport

network interface feth0 switchport mode access

network interface feth0 switchport trunk native-vlan 1

network interface feth0 switchport access-vlan 1

network interface feth0 switchport trunk allowed-vlan 1-1000

network interface feth0 mss-adjust 1460

network interface feth0 no shutdown

network interface <*string*> **ipv6 clean** <cr>

命令描述：

清除某接口所有的 IPv6 地址。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待清除地址的接口。 字符串类型，可为物理接口或虚接口。

命令示例：

清空 feth2 接口上所有的 IPv6 地址。

TopsecOS# **network interface** *feth2* **ipv6 clean**

network interface <*string*> **shutdown** <cr>

命令描述：

关闭指定接口。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待关闭的接口。 字符串类型，可为物理接口或虚接口。

network interface <*string*> **switchport** <cr>

命令描述：

设置某物理接口的工作模式为交换模式，TopWAF 物理接口默认工作在路由模式下，更改工作模式使其工作在交换模式时，接口上的所有 IP 地址将被删除。

可使用 **network interface** <*string*> **no switchport** 命令取消设置某物理接口的工作模式为交换模式。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待设置工作在交换模式的接口。

命令示例：

设置接口 feth2 的工作模式为交换模式。

TopsecOS# **network interface** *feth2* **switchport**

network interface <*string*> **switchport mode** <access|trunk>

命令描述：

设置交换接口的工作模式。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待设置工作模式的交换接口。
mode <access|trunk>	必选项，设置当前交换接口的工作模式。 access 模式：该交换接口只属于一个 VLAN。 trunk 模式：该交换接口可以允许多个 VLAN 的报文通过。

命令示例：

设置 feth0 接口为 trunk 接口。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **switchport mode** trunk

network interface <*string*> **switchport trunk allowed-vlan** <*string*>

命令描述：

设置 trunk 接口的属性。即该 trunk 端口属于哪些 VLAN。

参数说明：

参数	说明
interface *<string>*	必选项，输入接口名称，指定待设置 Trunk 属性的接口。
allowed-vlan *<string>*	必选项，设置端口所属 VLAN 范围。 字符串类型，表示 VLAN 范围，格式为 N1，N2，……，N3-N4（N 表示数值，且 N3 <=N4）。例如：1-10 表示 VLAN1，VLAN2，……，VLAN10；1，10 表示 VLAN1 和 VLAN10；1，10，11-12，表示 VLAN1，VLAN10，VLAN11 和 VLAN12。

network interface *<string>* **switchport trunk native-vlan** *<num>*

命令描述：

设置该 Trunk 接口的本地 VLAN。

参数说明：

参数	说明
interface *<string>*	必选项，输入接口名称，指定待设置本地 VLAN 的 Trunk 接口。
native-vlan *<num>*	必选项，trunk 端口的缺省 VLAN ID。由于 Trunk 端口属于多个 VLAN，所以需要设置缺省 VLAN ID，用于当该交换接口接收到没有标记的报文时，该 Trunk 端口将此报文发往缺省 VLAN ID 标识的 VLAN。 实数类型，指定 VLAN ID 值。

命令示例：

设定 feth0 接口为 trunk 接口，且只允许 vlan1 和 vlan5 通过。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **switchport mode** trunk

TopsecOS# **network interface** *feth0* **switchport trunk allowed-vlan** *1,5*

设定 feth0 接口为 trunk 接口，且只允许 vlan1、vlan2、vlan3、……、vlan10 通过。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **switchport mode** trunk

TopsecOS# **network interface** *feth0* **switchport trunk allowed-vlan** *1-10*

设定 feth0 接口为 trunk 接口，并将本地 vlan 设置为 vlan5。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **switchport mode** trunk

TopsecOS# **network interface** *feth0* **switchport trunk native-vlan** *5*

network interface <*string*> **switchport access-vlan** <*num*>

命令描述：

设置 access 接口所属的 VLAN。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待设置所属 VLAN 的 access 接口。
access-vlan <*num*>	必选项，设置该 access 交换接口所属的 VLAN ID 号。 数值类型，表示 VLAN 的 ID。

命令示例：

设置 feth0 接口为 access 接口，且将其添加到 vlan2。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **mode** access

TopsecOS# **network interface** *feth0* **switchport access-vlan** *2*

network interface <*string*> **show [**configuration**]**

命令描述：

查看设备接口配置信息。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待查看接口信息的接口。如果不指定该参数，将查看所有接口的配置信息。
show [configuration**]**	查看接口信息，如果不输入 configuration，查看接口所有的信息；输入 configuration，只查看接口的配置信息。

命令示例：

查看接口 feth1 的配置。

```
TopsecOS# network interface feth1 show
feth1       Link encap:Ethernet    HWaddr 00:0c:29:ea:39:70
            Link status: established, Autoneg enable
            Full-duplex, 10000Mb/s
            inet addr:1.1.1.1    Bcast:1.1.1.255    Mask:255.255.255.0
            inet6 addr:fe80::20c:29ff:feea:3970/64    Scope:Link
            UP BROADCAST RUNNING MULTICAST    MTU:1500
            Rx packets:212 Tx packets:6 Dropped:0
            RX bytes:9752 (9.5 kb)    TX bytes:480 (480.0 b)
            Vsys:root_vsys    Ifindex:14
            Commtype:routing
```

查看接口 feth1 的功能配置。

```
TopsecOS# network interface feth1 show configuration
network interface feth1 mtu 1500
network interface feth1 ip add 1.1.1.1 mask 255.255.255.0
network interface feth1 speed auto
network interface feth1 duplex auto
network interface feth1 switchport mode access
```

network interface feth1 switchport trunk native-vlan 1

network interface feth1 switchport access-vlan 1

network interface feth1 switchport trunk allowed-vlan 1-1000

network interface feth1 no switchport

network interface feth1 mss-adjust off

network interface feth1 gratuitous-arp-interval 0

network interface feth1 ha-virtual-mac-address enable

network interface feth1 tgid 0

network interface feth1 no shutdown

network interface <*string*> **description** <*string*>

命令描述：

设置接口的描述信息。

使用 **network interface** <*string*> **no description** 命令可以删除该描述信息。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待配置描述信息的网络接口。
description <*string*>	可选项，设置该接口的描述信息。 字符串类型。不包含“ &\"\\'%<>” 中任意字符，且不能包含空格。

命令示例：

给 feth0 添加“guanlikou”的描述信息。

TopsecOS# **network interface** *feth0* **description** *guanlikou*

network interface <*string*> **duplex** <half|full|auto>

命令描述：

设置物理接口的工作模式。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待设置工作模式的接口。
duplex <half|full|auto>	必选项。半工|全工|自动，默认为自动协商模式。

命令示例：

设置接口 feth0 的工作模式为全工。

TopsecOS# **network interface** *feth0* **duplex** full

network interface <*string*> **mac-address** <*macaddress*>

命令描述：

设置物理接口的 MAC 地址。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待设置 MAC 地址的接口。
mac-address <*macaddress*>	必选项，设置接口的 MAC 地址。 MAC 地址字符串，格式为 aa:bb:cc:dd:ee:ff。

命令示例：

设置接口 feth3 的 MAC 地址为 f2:ab:12:6c:56:bb。

TopsecOS# **network interface** *feth3* **mac-address** *f2:ab:12:6c:56:bb*

TopsecOS# **network interface** *feth3* **show**

feth3 Link encap:Ethernet HWaddr f2:ab:12:6c:56:bb

Link status: established, Autoneg enable

Unknown-duplex, unknown speed

UP BROADCAST RUNNING MULTICAST MTU:1500

Rx packets:0 Tx packets:0 Dropped:0

RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

Vsysid:0 Vrid:0 Ifindex:29

Commtype:routing

network interface <*string*> **restore mac**

命令描述：

恢复接口的 MAC 地址为默认配置。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待恢复 MAC 为默认配置的接口。

命令示例：

恢复接口 feth3 的 MAC 地址为默认配置。

TopsecOS# **network interface** *feth3* **restore mac**

network interface <*string*> **mss-adjust** <auto|off|*number*>

命令描述：

对某物理接口的 MSS 值进行自动调整，即根据接口的 mtu 值对该接口的 MSS 值进行调整，调整的数值是接口的 MTU–60，留部分空间给可能的 IP 选项。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待设置 MSS 的接口。
mss-adjust <auto|off|*number*>	自动调整|关闭自动调整|设置 MSS 数值，其中 *number* 取值范围：200-1460。

命令示例：

关闭接口 feth0 的 MSS 调整功能。

TopsecOS# **network interface** *feth0* **mss-adjust** off

network interface <*string*> **mtu** <*number*>

命令描述：

设置物理接口的 MTU。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待设置 MTU 的接口。
mtu <*number*>	数值类型，单位为字节，取值范围为 68-1500，默认值为 1500。

命令示例：

设置接口 feth0 的 MTU 为 1460。

TopsecOS# **network interface** *feth0* **mtu** *1460*

network interface <*string*> **speed** <10|100|1000|10000|auto>

命令描述：

设置物理接口的工作速率。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待设置工作速率的接口。
speed <10|100|1000|10000|auto>	必选项，10Mbps|100Mbps|1000Mbps|10000Mbps|自动，接口默认为自动获取工作速度。

命令示例：

设置接口 feth0 的工作速率为 1000Mbps。

TopsecOS# **network interface** *feth0* **speed** 1000

7.1.2 子接口

在 VLAN 虚拟局域网中，通常一个物理接口对应一个 VLAN。在多个 VLAN 的网络中，无法使用单个物理接口实现 VLAN 间通信。为打破物理接口的这种局限性，子接口应运而生。子接口是通过协议和技术将路由模式的物理接口虚拟出来的多个逻辑接口，它的出现打破了每个设备存在物理接口数量有限的局限性。通过在物理接口上配置子接口可实现多个 VLAN 的互连互通。

相对于子接口而言，这个物理接口为父接口。每个子接口从功能、作用上来说，与父接口是没有区别的。子接口共用父接口的物理层参数，又可以分别配置各自的链路层和网络层参数。子接口的状态不会对父接口产生影响，但父接口状态的变化会对子接口产生影响，只有父接口处于连通状态时子接口才能正常工作。

7.1.2.1 MAC 子接口

MAC 子接口是在工作于路由模式下的物理接口上配置的逻辑接口，子接口与其关联的物理接口在数据链路层和网络层相对独立，通过在物理接口上配置子接口可实现多个网络互连互通。

子接口提供了在一个物理接口上支持多个网络互连的功能，为管理员提供了很高的灵活性。工作在路由模式下的 TopWAF 的每个物理接口均可支持多达 32 个子接口。

WEBUI 方式

只有在路由模式的物理接口上才能配置 MAC 子接口，关于接口属性的配置具体请参见 7.1.1 物理接口。

步骤1 选择 **网络管理** > **接口** >**子接口**，激活“MAC 子接口”页签。

步骤2 添加 MAC 子接口。

1）点击界面左上角的『添加』，弹出添加 MAC 子接口界面。

在添加子接口时，各项参数的具体说明如下表所示。

参数	说明
接口	选择要在其下添加子接口的物理接口，该接口必须为路由接口。
添加单个子接口	添加单个子接口的 ID 号，取值范围：0-31。添加后，子接口的名称为“以太网接口名+mv+子接口 ID”，如 feth0mv02，表示以太网接口 feth0 的 ID 号为 2 的子接口。
添加子接口范围	一次性在某个物理接口下添加多个名称连续的子接口。取值范围：0-31。如在 feth0 接口下输入范围“2-10”，则一次性添加 feth0mv02、feth0mv03、feth0mv04……feth0mv10。

2）点击【确定】按钮完成子接口的添加。添加完成后，子接口默认处于“停用”状态。

步骤3 设置子接口属性。

1） 勾选子接口，点击『编辑』，弹出编辑子接口窗口。如下图所示。

关于属性参数的配置具体请参见 7.1.1 物理接口。

2）点击【确定】按钮，完成子接口属性的设定。

CLI 方式

network interface <*string*> **macvif add id** <*num*>

命令描述：

在物理接口上添加一个 mac 子接口。每个物理接口都可支持多达 32 个子接口，其中子接口的名称由以太网接口名+mv+子接口 ID 组成，如果在路由接口 feth1 上添加 ID 为 2 的子接口，则该子接口的名称为 feth1mv02。

使用 **network interface** <*string*> **macvif delete id** 命令删除添加的 mac 子接口。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待添加子接口的物理接口。 说明： 只有工作在路由模式下的物理接口才可以添加子接口。
id <*num*>	必选项，设置子接口 ID。 实数类型，取值范围：0-31。

命令示例：

在物理接口 feth2 上添加名称为 feth2mv01 的 mac 子接口。

TopsecOS# **network interface** *feth2* **macvif add id** *1*

network interface <*string*> **macvif add range** <*string*>

命令描述：

在物理接口上一次性添加多个 ID 连续的 mac 子接口。

使用 **network interface** <*string*> **macvif delete range** 命令删除添加的多个 mac 子接口。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待添加多个子接口的物理接口。 说明： 只有工作在路由模式下的物理接口才可添加子接口。
range <*string*>	必选项，设置所添加子接口的 ID 范围。 字符串类型，格式：N1-N2（N 为数值类型，且 N1 <=N2），N 的取值范围：0-31，如 5-20。

命令示例：

在物理接口 feth2 上添加名称为 feth2mv10、feth2mv11……feth2mv20 的 mac 子接口。

TopsecOS# **network interface** *feth2* **macvif add range** *10-20*

network interface <*string*> **macvif clean** <cr>

命令描述：

清空某物理接口上的所有 mac 子接口。

参数说明：

参数	说明
interface <*string*>	必选项，输入物理接口名称，指定待清空 MAC 子接口的物理接口。

命令示例：

清空 feth2 接口上所有的 mac 子接口。

TopsecOS# **network interface** *feth2* **macvif clean**

network interface <*string*> **macvif show** <cr>

命令描述：

查看某物理接口上的所有 mac 子接口。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待查看 MAC 子接口的物理接口。

命令示例：

在物理接口 feth2 上查看已添加的 mac 子接口。

TopsecOS# **network interface** *feth2* **macvif add id** *1*

TopsecOS# **network interface** *feth2* **macvif add range** *10-20*

TopsecOS# **network interface** *feth2* **macvif show**

feth2mv01	feth2mv10	feth2mv11	feth2mv12
feth2mv13	feth2mv14	feth2mv15	feth2mv16
feth2mv17	feth2mv18	feth2mv19	feth2mv20

7.1.2.2 配置 TAG 子接口

TAG 子接口通过将物理口虚拟为多个逻辑接口的方式实现了基于标签的分流，为区分到特定的虚系统奠定了基础。TAG 子接口处理报文时根据报文的标签遍历所有子接口，选择匹配的子接口作为入口。

在配置 TAG 子接口之前，需要先进行如下步骤：

- 配置子接口对应物理接口的工作模式为路由模式，关于接口属性的配置具体请参见 7.1.1 物理接口。

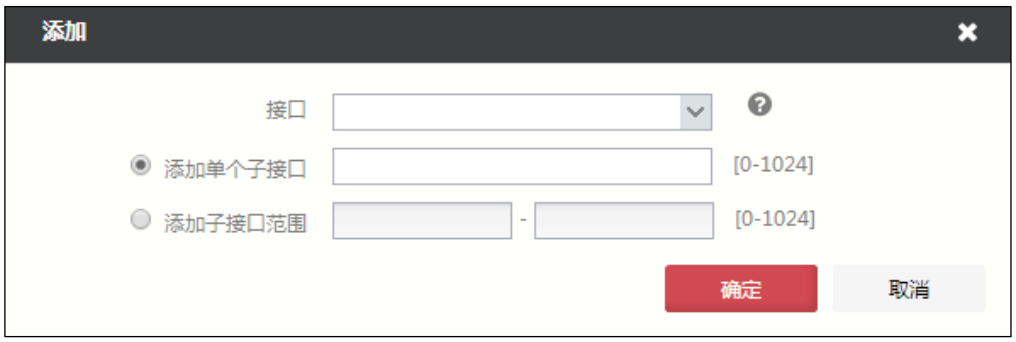
✧ 不能在同一个物理接口上同时添加 MAC 子接口和 TAG 子接口。

WEBUI 配置

步骤1 选择**网络管理** > **接口** >**子接口**，激活“TAG 子接口”页签。

步骤2 添加子接口。

1）点击“『添加』”添加 MAC 子接口。如下图所示。



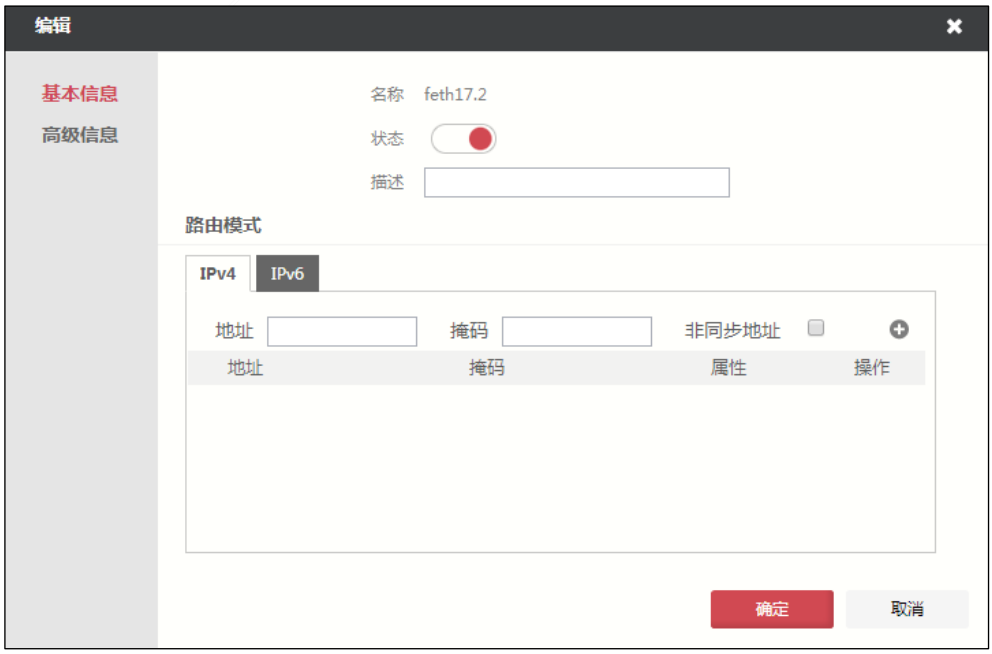
在添加 TAG 子接口时，各项参数的具体说明如下表所示。

参数	说明
接口	选择要在其下添加子接口的物理接口，该接口必须为路由接口。
添加单个子接口	添加单个子接口的 ID 号，取值范围为 1-4094。添加后，子接口的名称为“以太网接口名.子接口 ID”，如 feth1.2，表示以太网接口 feth1 的 ID 号为 2 的子接口。
添加子接口范围	一次性在某个物理接口下添加多个名称连续的子接口。取值范围为 1-4094。如在 feth1 接口下输入范围“2-10”，则一次性添加 feth1.2、feth1.3、feth1.4……feth1.10。

2）点击【确定】按钮完成 TAG 子接口的添加。添加完成后，TAG 子接口默认处于“下行”状态。

步骤3 设置 TAG 子接口属性。

1）勾选已添加的 TAG 子接口，点击上方 『编辑』。如下图所示。



关于属性参数的配置具体请参见 7.1.1 物理接口。

2）点击【确定】按钮，完成 TAG 子接口属性的设定。

CLI 配置

network interface <*string*> **tagvif add tagid** <*num*>

命令描述：

在物理接口上添加一个 tag 子接口。每个物理接口都可支持多达 1024 个子接口，其中子接口的名称由以太网接口名+“.”+子接口 ID 组成，如果在路由接口 feth1 上添加 ID 为 2 的子接口，则该子接口的名称为 feth1.02。

使用 **network interface** <*string*> **tagvif delete id** <*num*>命令删除添加的 tag 子接口。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待添加 tag 子接口的物理接口。 字符串类型。该接口需工作在路由模式下。
tagid <*num*>	必选项，设置子接口 ID。 实数类型。取值范围：0-1024。

命令示例：

在物理接口 feth2 上添加名称为 feth2.1 的 tag 子接口。

TopsecOS# **network interface** *feth2* **tagvif add tagid** *1*

network interface <*string*> **tagvif add range** <*string*>

命令描述：

在物理接口上一次性添加多个 ID 连续的 tag 子接口。

使用 **network interface** <*string*> **tagvif delete range** 命令删除添加的多个 tag 子接口。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待添加多个 tag 子接口的物理接口。 字符串类型，该接口需工作在路由模式下。
range <*string*>	必选项，设置所添加子接口的 ID 范围。 字符串类型，格式：N1-N2（N 为数值类型，且 N1 <=N2），N 的取值范围：0-1024，如 5-20。

命令示例：

在物理接口 feth2 上添加名称为 feth2mv10、feth2mv11……feth2mv20 的 tag 子接口。

TopsecOS**#network interface** *feth2* **tagvif add range** *10-20*

network interface <*string*> **tagvif clean** <cr>

命令描述：

清空某物理接口上的所有 tag 子接口。

参数说明：

参数	说明
interface <*string*>	必选，输入接口名称，指定待清空 tag 子接口的物理接口。 字符串类型。

命令示例：

清空 feth2 接口上所有的 tag 子接口。

TopsecOS**#network interface** *feth2* **tagvif clean**

network interface <*string*> **tagvif show** <cr>

命令描述：

查看某物理接口上的所有 tag 子接口。

参数说明：

参数	说明
interface <*string*>	必选项，输入接口名称，指定待查看子接口的物理接口。 字符串类型。

命令示例：

在物理接口 feth2 上查看已添加的 tag 子接口。

TopsecOS# **network interface** *feth2* **tagvif add tagid** *1*

TopsecOS# **network interface** *feth2* **tagvif add range** *10-20*

TopsecOS# **network interface** *feth2* **tagvif show**

feth2.1	feth2.10	feth2.11	feth2.12
feth2.13	feth2.14	feth2.15	feth2.16
feth2.17	feth2.18	feth2.19	feth2.20

7.1.3 VLAN

VLAN（Virtual Local Area Network，虚拟局域网）是一种从逻辑上将局域网划分的技术。一个 VLAN 即一个广播域。在二层网络中，同一 VLAN 互连互通，不同 VLAN 间相互隔离。要实现 VLAN 间的通信，需通过三层路由技术。

VLAN 划分不受物理位置限制，同一 VLAN 中的主机可以连接在同一交换机，也可连接在不同的交换机上。如下图所示，PC 1 和 PC 3，虽然都连接了 Switch A，但是分别划分到了 VLAN 1 和 VLAN 2 中，所以 PC 1 和 PC 3 不能直接通信。

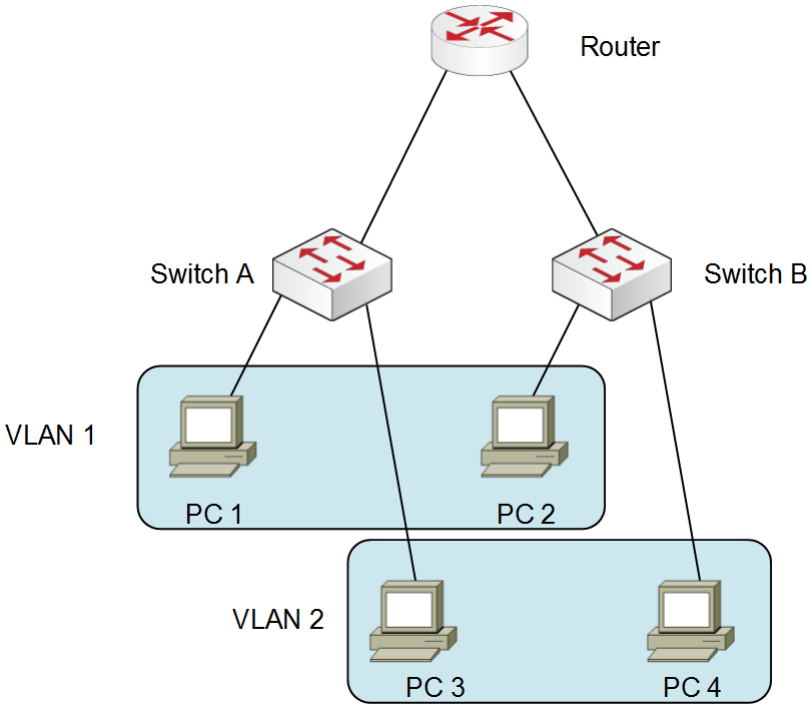


图 7-1 VLAN 示意图

VLAN 虚接口是 VLAN 内所有设备对外通信的出口，其命名方式为“vlan.”加上四位 VLAN 的 ID 组成，如“vlan.0009”。

WEBUI 方式

步骤1 选择 **网络管理** > **接口** > **VLAN**。

步骤2 添加 VLAN。

1）点击『添加』，弹出“添加”窗口。

在添加 VLAN 时，各项参数的具体说明如下表所示。

参数	说明
添加单个 VLAN	添加单个 VLAN 的 ID 号，取值范围：1-4094。 说明： VLAN 的名称为“vlan. ID 号”，如 vlan.0001。
添加 VLAN 范围	一次性添加多个名称连续的 VLAN。ID 号取值范围：1-4094。 说明： 1）起始 VLAN ID 和终止 VLAN ID 中设置的数值既可以相同也可以不同，但起始 VLAN ID 一定不能大于终止 VLAN ID。数值不同时，表示添加的是一段 ID 连续的 VLAN；数值相同时，表示添加的是某一个 VLAN。 2）一次性添加多个名称连续的 VLAN 时，单次最多添加 500 个。

2）设置完成后，点击【确定】按钮完成 VLAN 的添加。如果添加 VLAN 成功，则新添加的 VLAN 会显示在界面中。

步骤3 设置 VLAN 虚接口属性。

添加 VLAN 后，需要给 VLAN 虚接口配置接口 IP 地址和子网掩码等属性。

1）选中待配置 VLAN 虚接口，点击『编辑』，弹出“编辑”窗口。

在设置 VLAN 虚接口时，各项参数的具体说明如下表所示。

参数	说明
状态	默认接口为“启用”，表示可以使用该 VLAN；如果选择“停用”，则该 VLAN 将不会工作，该 VLAN 所在的区域将无法和其他接口进行通讯。
描述	输入对该接口的简要描述。
IPv4 地址/掩码	输入 VLAN 虚接口的 IPv4 地址及其子网掩码。 说明： TopWAF 不同的 VLAN 虚接口之间、及与路由接口之间不能配置相同的 IPv4 地址或 Ipv4 地址不能在同一子网内。
非同步地址	如果在网络中配置了高可用性功能，则设置心跳口 IP 时必须要选择“非同步地址”，否则接口的 IP 地址信息会在主/从设备同步运行状态时被对方覆盖。热备组中的备设备的管理 IP 必须选择“非同步地址”，否则无法对备设备进行管理。关于双机热备的配置具体请参见 8.6 高可用性。
添加	点击“⊕”按钮，如果设置正确，则新添加接口的 IP 地址会显示在列表中。
IPv6 地址	输入 VLAN 虚接口的 IPv6 地址。 说明： 1）可以为 VLAN 虚接口设置多个 IPv6 地址。 2）不同的 VLAN 虚接口不能配置相同的 IPv6 地址或 IPv6 地址不能在同一子网内。
添加	如果“IPv6 地址”设置正确，点击“⊕”按钮，则新添加接口的 IPv6 地址会显示在列表中。

2）参数设置完成后，点击【确定】按钮完成 VLAN 虚接口的属性设置。

CLI 方式

network vlan add id <*num*>

命令描述：

添加一个 VLAN。

使用 **network vlan delete id** 命令删除一个 VLAN。

参数说明：

参数	说明
id <*num*>	必选项，设置 VLAN 号。 数值类型，取值范围为 1-4094。

命令示例：

添加 VLAN10。

TopsecOS# **network vlan add id** *10*

network vlan add range <*string*>

命令描述：

一次添加一个或多个连续 VLAN。

使用 **network vlan delete range** 命令删除一个或者多个 VLAN。

参数说明：

参数	说明
range <*string*>	必选项，设置 VLAN 号。 字符串类型，格式：A-B 或 A，A 和 B 为数值，取值范围为 1-4094。 说明：如果添加一个 VLAN，可输入一个数值，也可输入 A-A；如果添加多个 VLAN，输入 A-B，且 A 需小于 B。

命令示例：

添加 VLAN10、VLAN11、VLAN12……VLAN100。

TopsecOS# **network vlan add range** *10-100*

network vlan clean <cr>

命令描述：

清除所有 VLAN。

命令示例：

TopsecOS# **network vlan clean**

TopsecOS# **network vlan show**

Number of existing VLANS :0

VLAN status ports

---

network vlan show [id<*num*> |all**]**

命令描述：

显示所有 VLAN。

参数说明：

参数	说明
id<*num*> |all	可选项。 显示指定 ID 的 VLAN 信息|显示所有 VLAN 信息

命令示例：

TopsecOS# **network vlan add id** *11*

TopsecOS# **network vlan add id** *20*

TopsecOS# **network vlan add range** *15-18*

TopsecOS# **network vlan show**

Number of existing VLANS :6

VLAN status ports

---

11 active

15 active

16	active
17	active
18	active
20	active

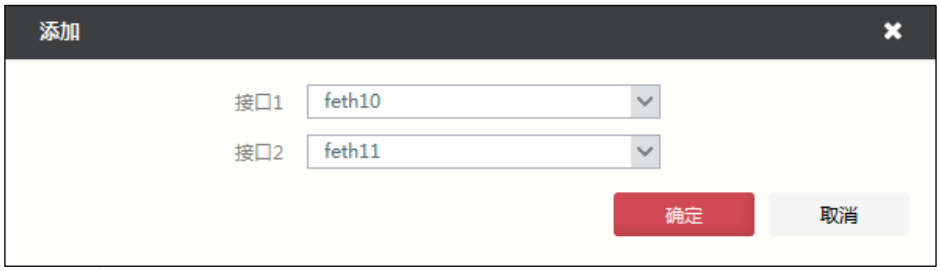
7.1.4 虚拟线

接口工作在虚拟线模式，管理员只需在 TopWAF 设定一个接口组 AB 作为一条虚拟线，如数据包从虚拟线接口组 AB 中的 A 口进入 TopWAF 后，除了目的地址为 TopWAF 的数据包外，均强制从虚拟线接口组 AB 中的 B 口进行转发，即不经过二层交换以及三层路由的检查过程就将报文直接发送出去。

WEBUI 方式

步骤1 选择 **网络管理** > **接口** > **虚拟线**。

步骤2 点击『添加』，如下图所示。



步骤3 设置好虚拟线路两端的接口后，点击【确定】按钮完成虚拟线路的添加。

✧ 只有工作在路由模式的接口才可添加到虚拟线中。

CLI 方式

network virtual-line add dev1 <*string*> **dev2** <*string*>

命令描述：

添加一条虚拟线。

参数说明：

参数	说明
dev1 <*string*>	必选项，设置虚拟线路左端的接口名。 字符串类型。
dev2 <*string*>	必选项，设置虚拟线路右端的接口名。 字符串类型。

命令示例：

将 feth0 和 feth1 加入到一条虚拟线中。

TopsecOS# **network virtual-line add dev1** *feth0* **dev2** *feth1*

TopsecOS# **network virtual-line show**

ID 8006 dev1:feth0 dev2:feth1

network virtual-line clean <cr>

命令描述：

清空所有虚拟线路。

命令示例：

TopsecOS# **network virtual-line clean**

network virtual-line delete id <*num*>

命令描述：

删除某条虚拟线路。

参数说明：

参数	说明
id <*num*>	必选项，设置虚拟线路的 ID 号。

参数	说明
	数值类型。

命令示例：

将 feth0 和 feth1 组成的虚拟线删除。

TopsecOS# **network virtual-line show**

ID 8006 dev1:feth0 dev2:feth1

TopsecOS# **network virtual-line delete id** *8006*

network virtual-line show <cr>

命令描述：

查看所有虚拟线路。

命令示例：

TopsecOS# **network virtual-line show**

ID 8006 dev1:feth0 dev2:feth1

7.1.5 链路聚合

链路聚合功能，是将多个物理接口聚合成一个逻辑上的聚合组。在聚合组中，被捆绑在一起的物理接口称为成员接口，聚合所形成的逻辑接口称为聚合接口。物理接口加入聚合组后，工作模式为 SLAVE 模式。通过链路聚合方式连接的两端设备，逻辑上设备间可看成只是通过单接口相连，如下图所示。

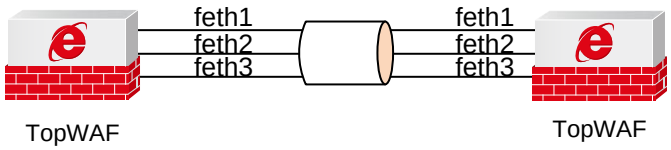


图 7-2 链路聚合示意图

链路聚合有如下优点：

- 聚合接口性能接近各个物理接口的性能总和，大大提高端口间的通信速度。
- 配置链路聚合功能时，无需重新布线，直接使用现有网络中的设备，减少网络维护工作。
- 聚合组内部的物理链路共同完成数据收发任务并相互备份，只要还存在能正常工作的链路，整个聚合组就不会失效，从而提高链路的可靠性。
- 聚合组内的成员接口可随时加入或者离开聚合组，管理员可根据实际需求灵活配置。

TopWAF 支持手工方式链路聚合，手工链路聚合需要手工将物理接口加入到到聚合组中，所有的物理接口均处于转发状态，聚合组通过预先设置的负载均衡算法分担链路流量到聚合组中的不同链路，实现链路的负载均衡。

TopWAF 通过采用不同的负载分担算法选择报文的发送接口，保证具有相同属性的报文能够从同一接口发送，可以灵活地实现对聚合组内业务流量的负载分担。

管理员既可以指定系统按照报文中携带的端口号、IP 地址、MAC 地址等信息之一或其组合来选择所采用的负载分担模式。TopWAF 支持的负载分担算法包括：

- src-mac：根据源 MAC 地址均衡，表示对发送的报文的源 MAC 地址进行哈希计算，根据计算结果选择数据转发接口。
- dst-mac：根据目的 MAC 地址均衡，表示对发送的报文的目的 MAC 地址进行哈希计算，根据计算结果选择数据转发接口。
- src-dst-mac：根据源和目的 MAC 地址组合均衡，表示对发送的报文的源和目的 MAC 地址进行哈希计算，根据计算结果选择数据转发接口。
- src-ip：根据源 IP 地址均衡，表示对发送的报文的源 IP 地址进行哈希计算根据计算结果选择数据转发接口。
- dst-ip：根据目的 IP 地址均衡，表示对发送的报文的目的 IP 地址进行哈希计算，根据计算结果选择数据转发接口。
- src-dst-ip：根据源和目的 IP 地址组合均衡，表示对发送的报文的源和目的 IP 地址进行哈希计算，根据计算结果选择数据转发接口。
- src-port：根据源 TCP/UDP 端口地址均衡，表示对发送的报文的源端口进行哈希计算，根据计算结果选择数据转发接口。
- dst-port：根据目的 TCP/UDP 端口地址均衡，表示对发送的报文的目的端口进行哈希计算，根据计算结果选择数据转发接口。

- src-dst-port：根据源和目的 TCP/UDP 端口地址均衡，表示对发送的报文的源和目的端口进行哈希计算，根据计算结果选择数据转发接口。
- quinary：根据五元组均衡，表示根据源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算，根据计算结果选择数据转发接口。
- per-packet：根据发送端口轮询均衡，表示发送数据时进行轮询，依次使用从第一个到最后一个可用的成员接口。

TopWAF 支持 8 个聚合组，每个聚合组最多支持 8 个成员接口。

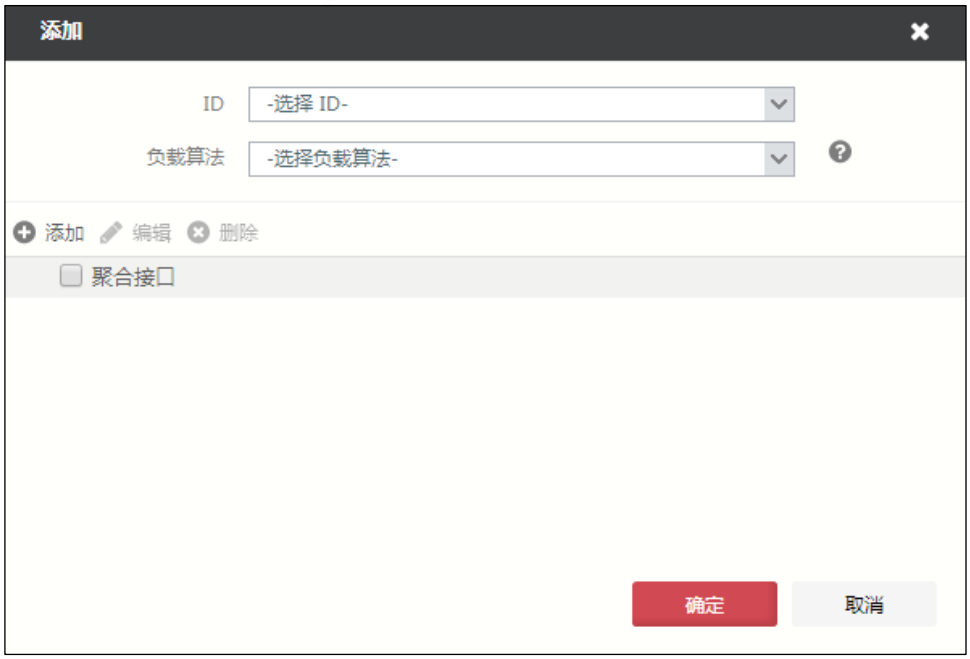
- ✧ 在 TopWAF 上，只有路由工作模式的物理接口可以加入到聚合接口中，不支持 VLAN 虚接口或子接口等其他逻辑接口加入聚合接口中。
- ✧ 一个物理接口只能属于一个聚合接口。

WEBUI 方式

步骤1 选择 **网络管理 > 接口 > 聚合接口**。

步骤2 添加新的聚合接口。

1）点击『添加』，添加新的聚合接口，如下图所示。



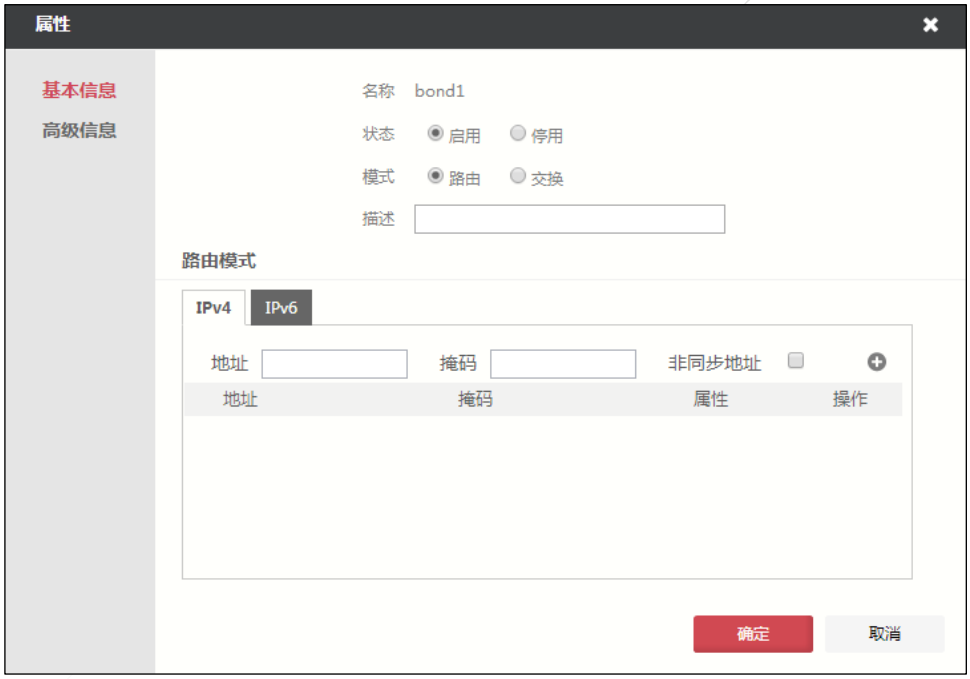
在添加聚合接口时，各项参数的具体说明如下表所示。

参数	说明
ID	必选项，选择聚合接口的 ID 号，可选项：0、1、2、3、4、5、6、7，聚合接口命名为 bond＋ID 号，例如此处设定为 0，则新添加的 bond 端口为 bond0。
负载算法	必选项，设置负载均衡算法，根据计算结果，选择聚合组内不同的物理接口转发流量。
聚合接口	点击『添加』，选择将哪些物理接口加入到该聚合接口中。

2）参数设置完成后，点击【确定】按钮完成聚合链路添加，新添加的逻辑端口将显示在界面中。

步骤3 设置聚合接口。

勾选聚合接口，点击『属性』，可以设置聚合接口，如下图所示。



关于属性参数的配置具体请参见 7.1.1 物理接口。不同的是，在该界面中，不能设置聚合接口的双工模式、接口速率参数。加入链路聚合的端口其属性显示为“SLAVE”，可工作在路由模式或交换模式。

CLI 方式

network bond add id <*num*> **load-balance** <

per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip|src-port|dst-port|src-dst-port|quinary>

命令描述：

增加一个聚合接口，同时指定负载均衡算法。

使用 **network bond delete id** 命令删除聚合接口。

使用 **network bond modify** 命令修改聚合接口。

参数说明：

参数	说明
id <*num*>	必选项，指定接口 ID 号。 实数类型，取值范围为 0-7。
load-balance< per-packet|src-mac| dst-mac|src-dst-mac |src-ip|dst-ip|src-dst -ip|src-port|dst-port| src-dst-port|quinary >	必选项，指定负载均衡算法，将流量分配给聚合链路内不同的物理接口。 说明： 1）per-packet：发送数据时进行轮询，依次使用从第一个到最后一个可用的 bond 接口。 2）src-mac：对发送的报文的源 MAC 地址进行哈希计算。 3）dst-mac：对发送的报文的目的 MAC 地址进行哈希计算。 4）src-dst-mac：对发送的报文的源和目的 MAC 地址进行哈希计算。 5）src-ip：对发送的报文的源 IP 地址进行哈希计算。 6）dst-ip：对发送的报文的目的 IP 地址进行哈希计算。 7）src-dst-ip：对发送的报文的源和目的 IP 地址进行哈希计算。 8）src-port：对发送的报文的源端口进行哈希计算决定分配给聚合接口内哪个 bond 接口。 9）dst-port：对发送的报文的目的端口进行哈希计算决定分配给聚合接口内哪个 bond 接口。 10）src-dst-port：对发送的报文的源和目的端口进行哈希计算决定分配给聚合接口内哪个 bond 接口。 11）quinary：根据源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算。

使用说明：

- ✧ 一个物理接口只能属于一个聚合接口。
- ✧ 支持在聚合接口上做 GRE（但是反过来不行，GRE 是虚接口，不可以把 GRE 接口加入端口聚合）。
- ✧ 当物理接口加入聚合接口成为 bond 接口后，不能对该物理接口再进行 IP 层以上的配置，即禁止设置 bond 设备的 ip 地址、MAC 地址、MTU 值、mss-adjust 值、子接口，禁止设置 bond 设备为交换口。只能启用/禁用接口，配置接口 speed、配置 MTU 值。

命令示例：

添加 ID 号为 1 的聚合接口，采用轮询算法进行负载均衡。

TopsecOS# **network bond add id** *1* **load_blance** per-packet

network bond clean <cr>

命令描述：

清空所有聚合接口。

network bond join id <*num*> **dev** <*string*>

命令描述：

将物理接口加入到聚合接口。

参数说明：

参数	说明
id <*num*>	必选项，指定接口 ID 号。 实数类型，取值范围为 0-7。
dev <*string*>	必选项，输入接口名称。 字符串类型。

使用说明：

✧ 加入到聚合接口的物理接口必须满足如下条件：1）路由模式；2）还没有加入其他 bond；3）没有子接口；4）在静态 arp 表里没有对应项。

命令示例：

将接口 feth0 加入到 ID 号为 1 的聚合接口。

TopsecOS# **network bond join id** *1* **dev** *feth0*

network bond leave id <*num*> **dev** <*string*>

命令描述：

将物理接口从聚合接口删除。

参数说明：

参数	说明
id <*num*>	必选项，指定接口 ID 号。 实数类型，取值范围为 0-7。
dev <*string*>	必选项，指定物理接口。 字符串类型。

命令示例：

将接口 feth0 从 ID 号为 1 的聚合接口删除。

TopsecOS# **network bond leave id** *1* **dev** *feth0*

network bond show [<all|verbose>**]**

命令描述：

显示聚合链路信息。

参数说明：

参数	说明
<all|verbose>	可选项。 查询全部聚合链路|查看全部聚合链路详细信息

network bond set id <*num*> **work-mode** <handmade|s-lacp>

命令描述：

设置链路聚合接口工作模式。

参数说明：

参数	说明
id <*num*>	必选项，通过 ID 指定聚合接口。 实数类型。
work-mode <handmade|s-lacp>	必选项。设置聚合接口工作模式。 手工|负载均衡

7.1.6 接口联动

接口联动主要用于 TopWAF 工作在双机热备、负载均衡、连接保护模式或者链路备份时，在短时间内根据单一接口的状态调整组内所有接口的状态，保证转发设备出接口和入接口状态的一致性，以防止在设备链路出现故障时，出现丢包情况。例如：当连接保护模式下的设备 A 负责转发数据的出口 down 掉时，属于同联动组的入口状态也同步 down，则入口所连设备将会判断入口 down 了，就可以及时将数据通过其它的设备 B 进行传输。

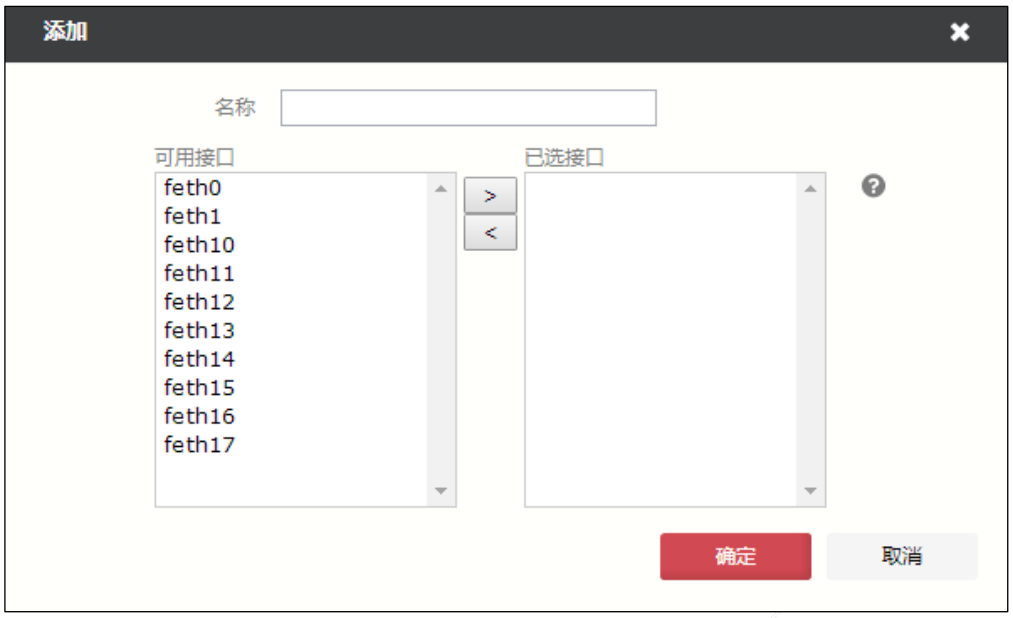
WEBUI 方式

步骤1 选择 **网络管理 > 接口> 接口联动**。

步骤2 添加联动组。

接口联动功能处于“ ”状态时，不能对接口联动组进行相关操作，必须停止联动组后，才可进行配置。

1）点击『添加』，进入“添加”对话框，如下图所示。



在添加接口联动组时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，输入接口联动组的名称。最多不能超过 31 个字符。
接口	选择接口联动组中的接口成员。 选择“可用接口”文本框中的接口后，点击“ > ”按钮将其添加到联动组“已选接口”中。 说明： 1）联动组的接口成员可以是 TopWAF 的物理接口或链路聚合口，不支持子接口和 VLAN； 2）同一个物理接口不能同时属于不同的联动组，并且每个联动组的成员数不能低于两个，不能高于八个。

2）点击【确定】按钮完成接口联动组的创建。刚创建成功的接口联动组处于“disable”状态。

步骤3 启动接口联动功能总开关。

点击“接口联动”下面的“状态”按钮，启动接口联动功能。此时，接口联动组处于“”状态。此后，当该联动组内的一个物理接口 down 后，该组内所有的物理接口都同步 down 掉。

步骤4 启用/停用单个接口联动组。

勾选已添加的接口联动组，点击『启用』，启用接口联动功能；点击『禁用』，禁用接口联动功能。说明：只有启用接口联动总开关后，单个接口联动组的启用开关才有效。

CLI 方式

network suitstate add name <*nstring*> **member** <*mstring*>

命令描述：

添加接口联动组。

可使用 **network suitstate delete name** 命令删除接口联动组。

参数说明：

参数	说明
name <*nstring*>	必选项，设置接口联动组名称。 字符串类型，不包含“!@#$%^&+=|?\"\\\'><`~”中任意字符，且不能包含空格。
member <*mstring*>	必选项，设置接口联动组成员。 字符串类型，至少设置 2 个成员接口，多个接口间用空格隔开。 例如：feth1 feth2。

使用说明：

✧ 接口联动组的成员只能是物理接口。

命令示例：

添加接口联动组“feth1-2”，设置参与联动的物理接口为 feth1 和 feth2。

TopsecOS# **network suitstate add name** *feth1-2* **member** ‘*feth1 feth2’*

network suitstate clean <cr>

命令描述：

删除所有接口联动组。

命令示例：

TopsecOS# **network suitstate clean**

network suitstate enable <cr>

命令描述：

启用接口联动功能总开关。

使用 **network suitstate disable** <cr>命令禁用接口联动功能。

network suitstate set name <*nstring*> <up|down>

命令描述：

设置被指定联动组的状态。

参数说明：

参数	说明
name <*nstring*>	必选项，设置接口联动组名称。 字符串类型。不包含“!@#$%^&+=|?\"\\'><`~”中任意字符，且不能包含空格。
up|down	启用|禁用，只有接口联动总开关处于开启状态，才可启用/禁用指定联动组，否则，所有的接口联动组处于禁用状态。

network suitstate show <configuration|status>

命令描述：

显示接口联动的配置或状态。

参数说明：

参数	说明
configuration|status	显示接口联动的配置|显示接口联动的状态。

命令示例：

TopsecOS# **network suitstate show** status

7.2 路由

路由指利用网络层协议将数据包从源主机通过寻址方案最终转发到目标主机的过程，最终实现不同网段间网络节点的互联互通。TopWAF 工作在路由模式下时，转发数据报文的关键是路由表，表中每条路由项都指明分组到某子网或某主机应通过 TopWAF 的哪个接口发送出去。

TopWAF 支持的路由类型包括：直连路由、静态路由、策略路由和 ISP 路由，其中，策略路由优先级高于静态路由。

- 直连路由：指路由接口所连接子网的路由，随路由接口的启用自动生成。
- 静态路由：基于数据报文的目的地址选路。由管理员手工添加，具有简单、稳定、安全、不随网络的变化而自动更新特征，网络故障或网络结构发生变化时，需由管理员手工修改，因此，静态路由适用于网络结构较简单的网络。
- 策略路由：可基于数据报文的源地址、源端口、目的地址、目的端口和协议选路。由管理员手工添加，具有不随网络的变化动态更新、可精细控制路由选路行为等特征。
- ISP 路由：目的地址是 ISP 地址文件中的 IP 地址，下一跳是出接口上配置的网关地址。这些静态路由称为运营商路由，也称为 ISP 路由，他们的优先级与普通静态路由相同。

数据报文经过 TopWAF 路由模块时，路由的查找原则如下：

1）如果入接口绑定了策略路由，报文将匹配该入接口绑定的所有策略路由项，有匹配项，则根据策略路由网关和出接口转发数据报文。

2）如果入接口没有绑定策略路由或者策略匹配失败时，则查找静态路由，有匹配项，则根据静态路由网关和出接口转发数据报文。

3）静态路由匹配失败时，则根据缺省路由处理数据报文。

✧ 报文命中路由表中多条路由条目后，遵循以下标准：（a）最小度量值路由优先；（b）度量值相同，最大权重值路由优先；（c）度量值和权重值均相同，通过此多条链路负载分担流量。

7.2.1 静态路由

天融信 TopWAF 支持 IPv4 静态路由和 IPv6 静态路由，静态路由需由管理员手工添加，不随网络结构的变化而发生任何变化。其表项的各字段包括：目的地址、掩码、网关、出接口、度量值、标记。

数据报文匹配静态路由时，如果数据报文满足路由表项的目的地址和掩码匹配条件，TopWAF 则根据该路由表项的网关和出接口确定从哪个接口转发报文；如果数据报文同时匹配多条静态路由，TopWAF 通过负载分担方式处理报文。IPv4 静态路由用于实现 IPv4 网络互连互通，IPv6 静态路由用于实现 IPv6 网络互连互通，其主要区别是地址格式不同，配置 IPv4 静态路由时使用 IPv4 地址，配置 IPv6 静态路由时使用 IPv6 地址。静态路由表项各字段说明如下：

- 目的地址（必选）：标识 IP 数据包的目的地址或目的网络。
- 网关（网关和出接口至少一个必选）：一般指 IP 数据包经过 TopWAF 后下一跳路由设备的 IP 地址。
- 出接口（网关和出接口至少一个必选）：指定目的地址为非 TopWAF 的 IP 数据包经哪个接口转发出去。
- 度量值：标识路由至目的地址的开销，路由度量值只在同一路由协议内起作用，不同路由协议的路由的度量值没有可比性。度量值表明路由表项的优先级，度量值越小路由优先级越高。对于去往同一目的地的多条路由，如果此多条路由优先级不同，可实现路由备份，优先级最高的路由为主路由，优先级次高的路由为备份路由；如果此多条路由优先级相同，此多条路由为等价路由，可实现流量的负载均衡。
- 标记（系统根据路由自动标记）：表明路由表项的路由类别及其所处状态，S：静态路由；C：直连路由；L：回环路由；H：主机路由；I：指定出接口；G：指定网关；U：路由处于启用状态。

WEBUI 方式

在配置静态路由之前，需要先进行如下步骤：

- 配置路由接口 IP 地址。关于接口的配置具体请参见 7.1.1 物理接口。

- 确定 TopWAF 路由表中的直连路由。
- 确定所添加的静态路由的目标地址。
- 明确数据通信是双向过程，确保通过 TopWAF 的数据包具备来和回路由。

步骤1 选择 **网络配置** > **路由** > **静态路由**。

步骤2 点击『添加』，如下图所示。

在添加静态路由时，各项参数的具体说明如下表所示。

参数	说明
目的地址/掩码	必选项，用来标识 IPv4/IPv6 包的目的地址或目的网络。 说明： 1）IPv4 目标地址格式：x.x.x.x/(0-32)；IPv6 目标地址格式：x:x:x:x:x:x:x:x/(0-128)。 2）IPv4 目的地址设置为 0.0.0.0/0，IPv6 目的地址设置为::/0 时，配置的为缺省路由，当数据包查找路由表没有匹配项后，TopWAF 根据缺省路由进行数据包的转发。
网关	指定路由的网关地址，通常为下一跳路由器的入口 IP 地址。 说明： 1）网关和出接口至少指定一个。 2）对于点对点网络，配置路由时可以不指定网关而只指定出接口；但对于以太网多路访问链路中，必须指定网关，否则 TopWAF 通过 ARP 协议获取下一跳网络设备的 MAC 地址时，无法获取到下一跳设备相应接口的 MAC 地址，导致数据包在发送前封装失败。
接口	指定数据报文从 TopWAF 的哪个接口进行转发。可以选择物理接口或虚接口。 说明： 网关和出接口至少指定一个。
度量值	设置路由的优先级，值越小，优先级越高。 说明： 同一目的地存在多条路由时，优先级高的路由将成为当前的最优路由。

步骤3 参数设置完成后，点击【确定】按钮完成路由的添加。

CLI 方式

network route add [family <ipv4|ipv6>**] dst** <*string*> **gw** <*string*> **[dev** <*string*>**] [metric** <*num*>**] [id** <*num*>**]**

命令描述：

添加一条静态路由。配置静态路由时，必须指定目的地址和网关。

对于同一目的地存在多条静态路由时，度量值 metric 最小路由将优先级最高，度量值相同时，可实现到达同一目的流量的负载分担。

参数说明：

参数	说明
family <ipv4|ipv6>	添加 IPv6 静态路由时，该参数为必选参数。用于设置静态路由的类型，默认为 IPv4 静态路由。 IPv4 静态路由|IPv6 静态路由
dst <*string*>	必选项，设定目标地址/掩码。 字符串类型，添加 IPv4 静态路由时，格式为 A.B.C.D/(0-32)；添加 IPv6 静态路由时，格式为 X:X:X:X:X:X:X:X/(0-128)，其中 X 为一个 4 位十六进制整数。
gw <*string*>	必选项，设定路由的下一跳。 网关地址字符串，对于 IPv4 静态路由，格式为 A.B.C.D；对于 IPv6 静态路由，格式为 X:X:X:X:X:X:X:X，其中 X 为一个四位十六进制整数。
dev <*string*>	可选项，设定路由出接口，可为物理接口或虚接口。 字符串类型，如 feth0。
metric <*num*>	可选项，指定路由度量值，metric 值越小，路由优先级越高。 数值类型。
id <*num*>	可选项，指定路由的 id 号，建议不要指定。 实数类型，取值范围为 100-13000，不能与已有策略 ID 相冲突。

命令示例：

添加一条目的地址为 202.103.96.0/24、网关为 192.168.90.1、出接口为 feth2 的 IPv4 静态路由。

TopsecOS# **network route add dst** *202.103.96.0/24* **gw** *192.168.90.1* **dev** *feth2*

TopsecOS# **network route show family** ipv4

Flags: U-Up, G-Gateway, H-Host, S-Static, L-Local, C-Connected, i-Interface

ID	Destination	Gateway	Flags	Metric	Iface
100	202.103.96.0/24	192.168.90.1	GSi	0	feth2

添加一条目的地址为 2fbb:aabb::/64、网关为 3faa::aaaa 的 IPv6 静态路由。

TopsecOS# **network route add family** ipv6 **dst** *2fbb:aabb::/64* **gw** *3faa::aaaa*

TopsecOS# **network route show family** ipv6

Flags: U-Up, G-Gateway, H-Host, S-Static, L-Local, C-Connected, i-Interface

ID	Destination	Next Hop	Flags	Metric	Iface
101	2fbb:aabb::/64	2faa::aaaa	GS	1024	*

network route set back-to-source <on|off|show>

命令描述：

设置路由回源功能。

参数说明：

参数	说明
back-to-source <on|off|show>	必选项，设置路由回源功能。 开启|关闭|显示

network route show [family <ipv4|ipv6>**] [dst** <*string*>**] [gw** <*string*>**]**

命令描述：

查看静态路由。

参数说明：

参数	说明
family <ipv4|ipv6>	可选项，设置查看静态路由的类型。 IPv4 静态路由|IPv6 静态路由

参数	说明
dst <*string*>	可选项，设置目标地址。 字符串类型，CIDR 形式的目的网络地址，格式 x.x.x.x/x。
gw <*string*>	可选项，设置网关地址。 IP 地址字符串类型，如 192.168.16.1。

命令示例：

查看所有静态路由。

TopsecOS# **network route show**

Flags: U-Up, G-Gateway, H-Host, S-Static, L-Local, C-Connected, i-Interface

==========IPv4==========

ID	Destination	Gateway	Flags	Metric	Iface
100	202.103.96.0/24	192.168.90.1	GSi	0	feth0

==========IPv6==========

ID	Destination	Next Hop	Flags	Metric	Iface
101	2fbb:aabb::/64	2faa::aaaa	GS	1024	*

查看 IPv4 静态路由。

TopsecOS# **network route show family** ipv4

Flags: U-Up, G-Gateway, H-Host, S-Static, L-Local, C-Connected, i-Interface

ID	Destination	Gateway	Flags	Metric	Iface
100	202.103.96.0/24	192.168.90.1	GSi	0	feth0

network route clean family <ipv4|ipv6>

命令描述：

清除静态路由。

参数说明：

参数	说明
family <ipv4|ipv6>	必选项，设置清除静态路由的类型。 IPv4 静态路由|IPv6 静态路由

命令示例：

清除所有 IPv6 静态路由。

TopsecOS# **network route clean family** ipv6

7.2.2 策略路由

策略路由不仅能够根据目的地址和目的端口，而且能够根据 IP 地址、端口和协议类型条件来确定报文的转发路径，可使不同类型的流量分别走不同的链路，达到保证类应用走优质链路，非保证类应用走另外链路的目的。此外，策略路由还可根据其度量值和权重值属性实现多链路的负载均衡和链路备份。

TopWAF 的策略路由可与入接口绑定，数据报文匹配策略路由时，首先匹配其进入 TopWAF 时的入接口所绑定的策略路由，如果无匹配项，则再匹配其他的策略路由。本节介绍策略路由的相关配置：包括策略路由的添加、删除、清空操作，以及改变策略路由中路由条目的排列顺序。

WEBUI 方式

步骤1 选择 **网络配置** > **路由** > **策略路由**。

步骤2 点击『添加』，如下图所示。

在添加策略路由时，各项参数的具体说明如下表所示。

参数	说明
绑定接口或 vr	绑定策略路由的入接口。
源地址	用来标识 IP 包的源地址或源网络。
目的地址	用来标识 IP 包的目的地址或目的网络。
源端口	标识数据包的源端口的范围，如果为单个端口，则只填写起始端口即可。默认是所有端口。
目的端口	标识数据包的目的端口的范围，如果为单个端口，则只填写起始端口即可。默认是所有端口。
协议	通过下拉框选择协议，可选项：TCP、UDP、ICMP、ICMPv6。
网关	指定数据报文从 TopWAF 的转发出去的下一跳地址。
度量值	接口跃点数。取值范围：1-255。度量值的大小决定了路由的优先级，度量值越小，优先级越高。
权重值	设置该策略路由的权重值。取值范围：1-255。 说明： 如果策略路由表中存在多个度量值相同的下一跳，则根据权重值分配各链路负载网络流量的百分比。

步骤3 点击【确定】按钮完成策略路由的创建。

CLI 方式

network route-policy add-entry gw <*string*>**[dev** <*string*>**] [interface** <*string*>**] [src** <*string*>**]**

[sport <*num*>**] [sport2** <*num*>**] [dst** <*string*>**] [dport** <*num*>**] [dport2** <*num*>**] [protocol** <tcp|udp|icmp|icmpv6>**] [metric** <*num*>**] [weight** <*num*>**]**

命令描述：

添加一条策略路由。

删除策略路由命令：**network route-policy del-entry**

参数说明：

参数	说明
gw <*string*>	必选项，设定网关地址。 表示网关 IP 地址。
dev <*string*>	可选项，指定转发接口。包括物理接口、虚接口和子接口。 字符串类型。如 feth0。
interface <*string*>	可选项，指定策略路由绑定的入接口名称。 字符串类型。如 feth0。
src <*string*>	可选项，设定源地址/掩码。 格式为 A.B.C.D 或 A.B.C.D/（0-32）的字符串，表示源地址/掩码。
sport <*num*>	可选项，标识数据包的源端口的起始端口，如果为单个端口，则只填写起始端口即可。 实数类型。取值范围：1-65535。
sport2 <*num*>	可选项，标识数据包的源端口的结束端口，如果为单个端口，可以不必填写该项，也可以填写与起始端口相同的端口号。 数值类型，应大于等于 sport 设定的端口号。 实数类型。取值范围：1-65535。
dst <*string*>	可选项，用来标识 IP 包的目的地址或目的网络。需要填写目的地址转换后的真实地址。 格式为 A.B.C.D 或 A.B.C.D/（0-32）的字符串，表示目的地址字符串。
dport <*num*>	可选项，标识数据包的目的端口的起始端口，如果为单个端口，则只填写起始端口即可。 实数类型。取值范围：1-65535。
dport2 <*num*>	可选项，标识数据包的目的端口的结束端口，如果为单个端口，可以不必填写该项，也可以填写与起始端口相同的端口号。 实数类型。取值范围：1-65535。
protocol <tcp|udp|icmp|icmpv6>	可选项，设置数据包使用的协议。
metric <*num*>	可选项，指定路由度量值，metric 值越小，路由优先级越高。默认为 1。 实数类型。

参数	说明
weight <*num*>	可选项，设置该策略路由的权重值。 实数类型。

命令示例：

对于源地址为 192.168.90.0/24，目的地址为 192.168.83.0/24，且从 TopWAF 的 feth0 进入的数据报文，网关为 192.168.16.1。

TopsecOS# **network route-policy add-entry interface** *feth0* **gw** *192.168.16.1* **src** *192.168.90.0/24* **dst** *192.168.83.0/24*

network route-policy clean-entry id <*num*> **[interface** <*string*>**]**

命令描述：

通过 ID 删除一条策略路由。

参数说明：

参数	说明
id <*num*>	必选项，设置需要删除的策略路由条目的 ID。 实数类型。
interface <*string*>	必选项，设置虚拟路由绑定的入接口名称。 字符串类型。

命令示例：

删除一条 ID 为 2 的策略路由。

TopsecOS# **network route-policy clean-entry id** *2*

network route-policy move id <*num*> **to** <before|after> **id** <*num*> **[interface** <*string*>**]**

命令描述：

移动策略路由条目。

参数说明：

参数	说明
id <*num*>	必选项，指定待移动的策略路由条目的 ID 号。 实数类型。
to <before|after>	必选项，指定策略路由移动方式。 移动到基准策略路由条目之前|之后
id <*num*>	必选项，指定基准策略路由条目的 ID 号。 实数类型。
interface <*string*>	必选项，输入接口名称，指定策略路由绑定的接口。 字符串类型。

命令示例：

移动 ID 为 101 且绑定接口 feth0 策略路由移动到 ID 为 103 的策略路由之后。

TopsecOS# **network route-policy move id** *101* **to** after **id** *103*

network route-policy show [interface <*string*>**]**

命令描述：

显示策略路由。

参数说明：

参数	说明
interface <*string*>	可选项，输入接口名称，指定只显示某接口所绑定的策略路由。 字符串类型。

命令示例：

显示与接口 feth0 绑定的策略路由。

TopsecOS# **network route-policy show interface** *feth0*

network route-policy list <cr>

命令描述：

显示所有策略路由。

命令示例：

TopsecOS# **network route-policy list**

network route-policy clear <cr>

命令描述：

删除所有策略路由。

命令示例：

TopsecOS# **network route-policy clear**

7.2.3 ISP 路由

ISP（Internet Service Provider）是向广大用户提供互联网接入服务和增值业务的互联网服务提供商。当用户可以通过多个 ISP 接入网络时，为避免跨运营商网络通信影响通信效率，通过 ISP 路由，即对数据包根据目的 ISP 选择出接口，可以大大提高网络的访问速度。

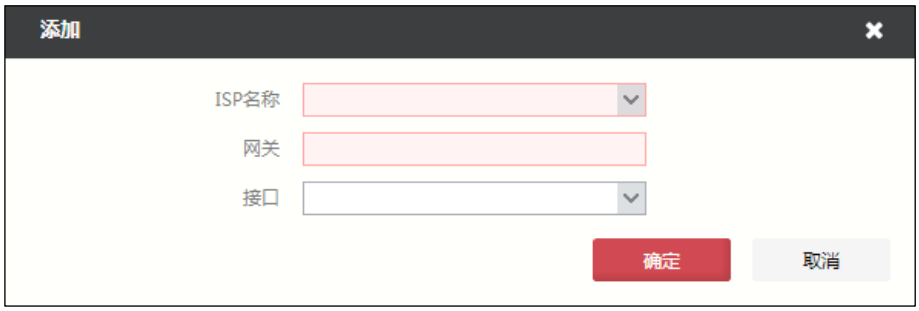
TopWAF 预定义了中国 7 大主要互联网服务提供商的 ISP 地址库，并支持管理员根据实际情况自定义 ISP 地址库。管理员只需基于 ISP 地址库配置 ISP 路由，系统即会自动将 ISP 路由添加到全局路由表，使数据包采用最优的通信线路，避免跨运营商通信问题。

WEBUI 配置

步骤1 选择 **网络管理 > 路由 > ISP 路由**。

步骤2 添加 ISP 路由。

1）点击『添加』，如下图所示。

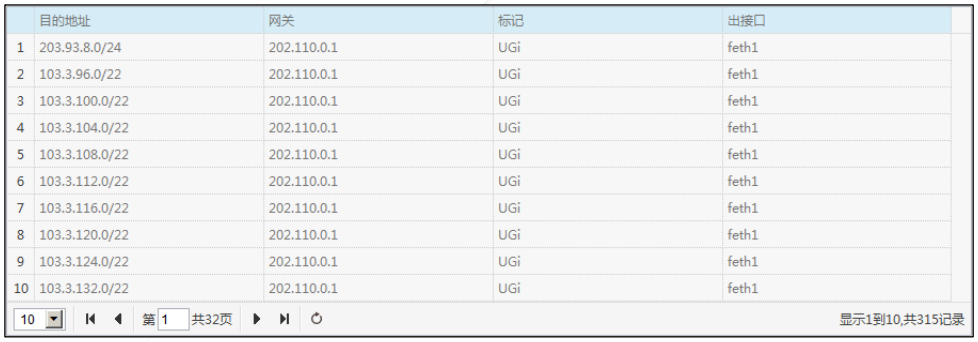


在添加 ISP 路由时，各项参数的具体说明如下表所示。

参数	说明
ISP 名称	选择目的 ISP 的类型。可选项：铁通宽带、网通宽带、移动宽带、长城宽带、教育网、联通宽带、电信宽带。
网关	该 ISP 路由的网关地址，通常为下一跳路由器的入口 IP 地址。
接口	指定 ISP 路由的出接口。可以选择物理接口或虚接口。

2）点击【确定】按钮完成 ISP 路由的添加。

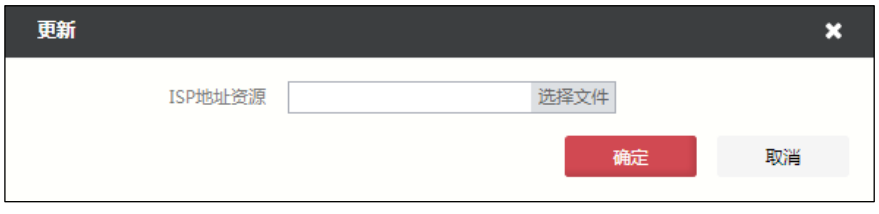
3）点击已添加 ISP 路由左侧的“ ”，显示该 ISP 路由中所有的路由信息，如下图。



	目的地址	网关	标记	出接口
1	203.93.8.0/24	202.110.0.1	UGi	feth1
2	103.3.96.0/22	202.110.0.1	UGi	feth1
3	103.3.100.0/22	202.110.0.1	UGi	feth1
4	103.3.104.0/22	202.110.0.1	UGi	feth1
5	103.3.108.0/22	202.110.0.1	UGi	feth1
6	103.3.112.0/22	202.110.0.1	UGi	feth1
7	103.3.116.0/22	202.110.0.1	UGi	feth1
8	103.3.120.0/22	202.110.0.1	UGi	feth1
9	103.3.124.0/22	202.110.0.1	UGi	feth1
10	103.3.132.0/22	202.110.0.1	UGi	feth1

4）更新 ISP 地址库。

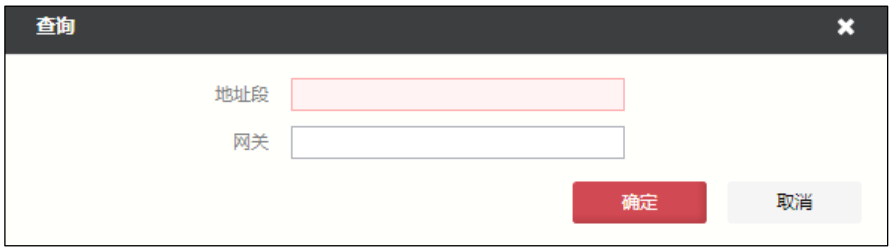
（a）点击『更新』，弹出 ISP 地址库更新界面，如下图所示。



（b）选择本地存储的 ISP 地址库文件，点击【确定】按钮，完成 ISP 地址库的更新。

5）查询 ISP 路由。

（a）点击『查询』按钮，如下图所示。



（b）输入 ISP 路由的目的地址和网关，点击【确定】按钮，符合查询条件的 ISP 路由将筛选出来。

CLI 配置

network route-isp add isp <*string*> **gw** <*ip*> **[dev** <*string*>**]**

命令描述：

根据 ISP 地址库添加 ISP 路由。

使用 **network route-isp delete isp** 命令删除 ISP 路由。

参数说明：

参数	说明
isp <*string*>	必选项，设置 ISP 地址库的名称。 字符串类型。输入系统 ISP 地址库名称。 说明： 系统预定义的 ISP 地址库对应的 ISP 名称为：CRTC（铁通宽带）、CNCGROUP（网通宽带）、CMNET（移动宽带）、GWBN（长城宽带）、CERNET（教育网）、UNICOM（联通宽带）CHINANET（电信宽带）。
gw <*ip*>	必选项，设置该 ISP 路由的网关，一般为 ISP 路由的下一跳设备的接口地址。 IPv4 地址类型，格式：A.B.C.D。
dev <*string*>	可选项，设置该 ISP 路由的出接口。 字符串类型。

命令示例：

添加一条通往中国电信 ISP 的路由，该路由的出接口为 feth12，网关为 202.100.23.98。

TopsecOS# **network route add isp** *CHINANET* **gw** *202.100.23.98* **dev** f*eth12*

network route-isp isp-name <cr>

命令描述：

显示 TOPWAF 系统预定义的 ISP 地址库对应的 ISP 名称。

命令示例：

TopsecOS# **network route-isp isp-name**

The ISP file name is:

CRTC	铁通宽带
CNCGROUP	网通宽带
CMNET	移动宽带
GWBN	长城宽带
CERNET	教育网
UNICOM	联通宽带
CHINANET	电信宽带

network route-isp isp-version <cr>

命令描述：

显示 TOPWAF 目前 ISP 地址库的版本。

命令示例：

TopsecOS# **network route-isp isp-version**

the current version is V1.0

network route-isp show [isp <*string*>**][verbose** <cr>**]**

命令描述：

显示 ISP 路由。

参数说明：

参数	说明
isp <*string*>	可选项，设置 ISP 地址库的名称，显示指定 ISP 地址库的 ISP 路由。 说明： 系统预定义的 ISP 地址库对应的 ISP 名称为：CRTC（铁通宽带）、CNCGROUP（网通宽带）、CMNET（移动宽带）、GWBN（长城宽带）、CERNET（教育网）、UNICOM（联通宽带）CHINANET（电信宽带）。
verbose <cr>	可选项，显示 ISP 路由详细信息。

network route-isp show [dst <*string*>**] [gw** <*string*>]

命令描述：

查询通过 ISP 库添加的路由条目。

参数说明：

参数	说明
dst <*string*>	可选项，设定目标地址/掩码。 字符串类型，格式为 A.B.C.D/(0-32)。
gw <*string*>	可选项，设定路由的下一跳。 网关地址字符串，格式为 A.B.C.D。

7.3 邻居

ARP（Address Resolution Protocol，地址解析协议）是根据 IP 地址获取 MAC 地址的 TCP/IP 协议。以太网设备在发送数据包前需封装第二层报头（包含 MAC 地址）和第三层报头（包含 IP 地址），封装数据包中 MAC 地址通过查询 ARP 表确定 MAC 地址。如果 ARP 表中存在目的 IP 地址对应的 MAC 地址，直接封装数据包；否则，则通过 ARP 协议根据已知目的 IP 地址解析出 IP 地址对应的 MAC 地址，再进行封装数据包。

主机根据 ARP 协议获取目的 IP 地址对应的 MAC 地址时，根据目的地址与主机是否处于同一个网段，处理方式不同（以 PC A 向 PC D 发送数据报文为例）。

- 目的地址与主机处于同一个子网。

1）PC A 在 ARP 表中查找到 PC D 表项，直接利用其中的 MAC 地址对 IP 报文进行数据帧封装，发送给 PC D。

2）PC A 在 ARP 表中未查找到 PC D 表项，ARP 工作过程如下图所示。

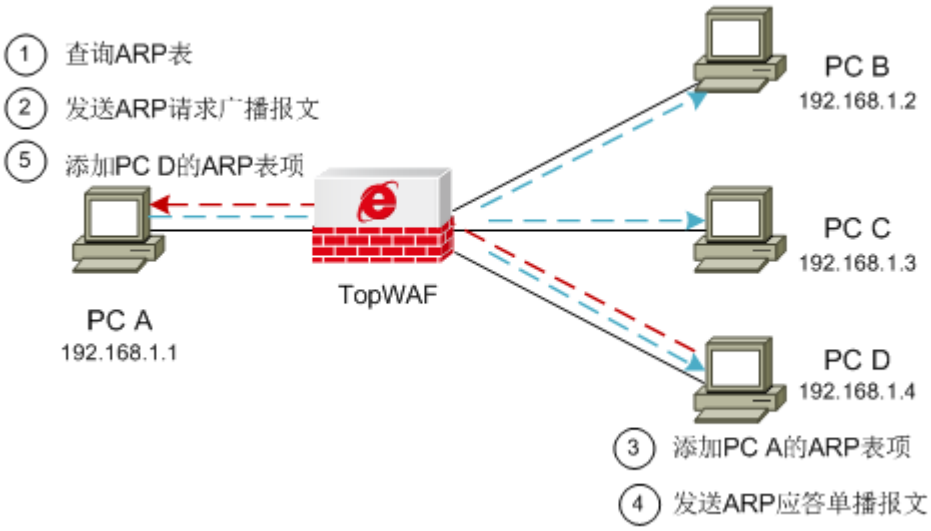


图 7-3 ARP 工作过程示意图

- PC A 以广播方式发送一个 ARP 请求报文。该报文的源 IP 地址和源 MAC 地址为 PC A 的 IP 地址和 MAC 地址，目的 IP 地址为 PC D 的 IP 地址、目的 MAC 地址为全 0。
- 处于同一广播域内的所有设备均可接收到该 ARP 请求报文，并将自己的 IP 地址与报文中的目的 IP 地址比较，若不同则丢弃报文，不做任何应答。
- PC D 在发现请求报文中 IP 地址与自身的 IP 地址相同，于是将 ARP 请求报文中的源 IP 地址和源 MAC 地址的映射关系存入自己的 ARP 表中，发送 ARP 响应报文给 PC A。ARP 响应报文以单播方式发送，其中包含 PC D 的 MAC 地址。
- PC A 收到 ARP 响应报文后，在 ARP 表中加入 PC D 的 MAC 地址用于后续的报文转发，并将 IP 报文进行数据帧封装，发送给 PC D。

- 目的地址与主机处于不同子网

PC A 会广播 ARP 请求报文，此时网关进行应答，发送 ARP 响应报文给 PC A。PC A 则将网关的 MAC 地址写入对应目的地址的该 ARP 表项。之后，PC A 则会根据网关的 MAC 对数据进行封装。

Neighbor

IPv6 协议扩大了地址空间，使得网络节点只需要知道链路层地址及本地网络的子网前缀，就能够通过无状态或有状态自动配置得到唯一的 IPv6 地址而成为网络的一部分。同时，IPv6 还支持网络节点的移动性。这些功能都是通过邻居发现协议（NDP，Neighbor Discovery Protocol）来实现的，同一个子网内所有主机与路由器之间的交互也都是通过邻居发现协议来实现的。

邻居发现协议是 IPv6 协议的关键组成部分，包括路由器请求（RS，Router Solicitation）、路由器通告（RA，Router Advertisement）、邻居请求（NS，Neighbor Solicitation）、邻居通告（NA，Neighbor Advertisement）和重定向 5 种类型的 IPv6 控制信息报文（ICMPv6，Internet Control Management Protocol Version 6），实现了在 IPv4 中的地址解析协议（ARP）、控制报文协议（ICMP）中的路由器发现协议和重定向协议的所有功能，并具有邻居不可达检测机制。

- 路由器请求报文：主机启动后，向路由设备发出路由器请求，路由设备则会以路由器通告报文响应。
- 路由器通告报文：路由设备周期性的发布路由器通告报文，或者响应主机的路由器请求，其中包括前缀和一些标志位的信息。
- 邻居请求报文：IPv6 节点发送邻居请求报文，请求邻居的链路层地址，检查邻居是否可达，也可以验证邻居的地址是否是唯一的。
- 邻居通告报文：邻居通告报文是 IPv6 节点对邻居请求报文的响应，或者 IPv6 节点在链路层变化时也可以主动发送邻居通告报文。
- 重定向报文（Redirect）报文：路由设备通过发送重定向报文，通知链路上报文的发送节点，网络中存在更优的转发数据报文的路由设备。节点接收到重定向报文后，修改本地路由表项，选择最优路径转发。

邻居发现协议由邻居表实现，邻居表记录了主机 IPv6 地址和 MAC 地址的映射关系，主要用来完成与 IPv4 中的地址解析协议（ARP）相同的功能。当 TopWAF 发送数据报文时，会查看邻居表，如果目的 IP 地址已经在邻居表中，则根据邻居表中该 IP 地址对应的 MAC 地址封装数据报文；否则，TopWAF 需发送组播报文以获取目的主机的 MAC 地址来封装数据报文。

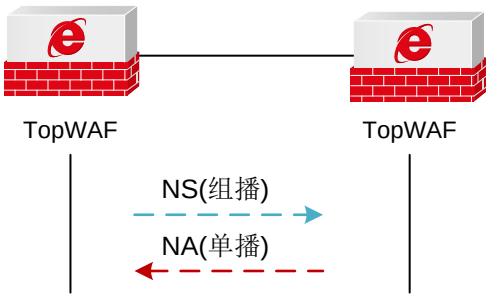


图 7-4 邻居地址解析过程示意图

如上图所示，以 TopWAF A 为例，TopWAF A 要获取 TopWAF B 的 MAC 地址，邻居地址解析过程如下。

1)TopWAF A 通过组播方式发送 NS 消息。其中 NS 消息的源地址是 TopWAF A 的 IPv6 地址，目的地址是被请求节点 TopWAF B 的组播地址，NS 消息中还包含了 TopWAF A 的 MAC 地址。

2）TopWAF B 收到 NS 消息后，判断报文的目的地址是否为自己的 IPv6 地址对应的被请求设备组播地址。如果是，则 TopWAF B 可以学习到 TopWAF A 的 MAC 地址，并以单播方式发送 NA 消息，其中包含了自身的 MAC 地址。

3）TopWAF A 收到 TopWAF B 发送的 NA 消息，获得 TopWAF B 的 MAC 地址。

7.3.1 ARP

ARP 表包括动态 ARP 表项和静态 ARP 表项两种。其中，动态 ARP 表项由设备动态学习，通过 ARP 协议动态更新，超过 ARP 表项老化时间后将被自动删除；静态 ARP 表项由管理员手工添加，则不存在老化问题，而且能够有效地防止 ARP 欺骗。

WEBUI 方式

TopWAF 工作在路由模式下，才需要通过 ARP 表封装数据包的 MAC 地址。

步骤1 选择 **网络管理** > **邻居** > **ARP**。

步骤2 点击『添加』，弹出“添加”窗口。

在添加 ARP 表项时，各项参数的具体说明如下表所示。

参数	说明
接口	设置 IP 地址所在区域所对应的路由接口或虚接口。
IP 地址	输入 IPv4 地址。
MAC 地址	输入 IPv4 地址对应的 MAC 地址。

步骤3 查询邻居表项。

点击『查询』，在弹出的对话框中，输入需要查询的邻居表项对应的接口、IP 地址或者 MAC 地址后，点击【确定】按钮，可以筛选出相应的邻居表项。

CLI 方式

network arp add ip <*string*> **mac-address** <*string*> **dev** <*string*>

命令描述：

添加一条静态 ARP 表项。

可通过 **network arp delete** 命令删除一条静态 ARP 表项。

参数说明：

参数	说明
ip <*string*>	必选项，设置 IPv4 地址。 字符串类型，IPv4 地址格式为 A.B.C.D。
mac-address <*string*>	必选项，设置 MAC 地址。 字符串类型，格式为 AA:BB:CC:DD:EE:FF。
dev <*string*>	必选项，设置出接口。 字符串类型，可为物理接口或虚接口。

命令示例：

添加一条主机地址为 192.168.99.100、MAC 地址为 18:a9:05:26:aa:8c、出接口为 feth0 的 ARP 表项。

TopsecOS#**network arp add ip** *192.168.99.100* **mac-address** *18:a9:05:26:aa:8c* **dev** *feth0*

network arp show [ip <*string*>**][mac-address** <*string*>**] [dev** <*string*>**] [type** <static|dynamic>**]**

命令描述：

查看静态 ARP 表详细信息。

参数说明：

参数	说明
ip <*string*>	可选项， 设置 IP 地址。 字符串类型。地址格式为 A.B.C.D。
mac-address <*string*>	可选项，设置 MAC 地址。 字符串类型，MAC 地址格式为：AA:BB:CC:DD:EE:FF。
dev <*string*>	可选项，设置接口名称。 字符串类型。
type <static|dynamic>	可选项，设置 ARP 表类型。 静态 ARP 表|动态 ARP 表

命令示例：

TopsecOS#**network arp show**

network arp clean [**dev** <*string*>]

命令描述：

清空静态 ARP 表。

参数说明：

参数	说明
dev <*string*>	可选项，输入接口名称，清空与该接口相关的所有静态 ARP 表项。 字符串类型。

命令示例：

TopsecOS#**network arp clean**

7.3.2 Neighbour

邻居表包括动态邻居表和静态邻居表。动态邻居表由 TopWAF 动态学习而生成，可根据通过 TopWAF 的数据流量自动更新；静态邻居表由管理员手工添加，不会随网络的变化自动更新。

WEBUI 方式

步骤1 选择 **网络管理** > **邻居** > **NEIGH**。

步骤2 添加邻居表项。

1）点击『添加』，弹出“添加”窗口。

在添加邻居表项时，各项参数的具体说明如下表所示。

参数	说明
接口	设置 IP 地址所在区域所对应的路由接口或虚接口。
IPv6 地址	输入接口的 IPv6 地址。
MAC 地址	输入 IPv6 地址所对应的 MAC 地址。

2）参数设置完成后点击【确定】按钮即可完成邻居表项的添加。

步骤3 查询邻居表项。

点击『查询』，输入需要查询的邻居表项对应的接口、IP 地址或者 MAC 地址后，点击【确定】按钮，可以筛选出相应的邻居表项。

CLI 方式

network neighbour add ip <*string*> **mac-address** <*string*> **dev** <*string*>

命令描述：

添加一条静态邻居表项。

使用 **network neighbour delete** 命令删除一条静态邻居表项。

参数说明：

参数	说明
ip <*string*>	必选项，设置 IPv6 地址。 字符串类型，IPv6 地址格式为 X:X:X:X:X:X:X:X，其中 X 为一个 4 位十六进制整数。
mac-address <*string*>	必选项，设置 MAC 地址。 字符串类型，MAC 地址格式为 AA:BB:CC:DD:EE:FF。
dev <*string*>	必选项，设置出接口，可为物理接口或虚接口。 字符串类型。

命令示例：

添加一条主机地址为 fe80::252a:b38d:93c7:91f0、MAC 地址为 18:a9:05:26:3f:e6、出接口为 feth0 的邻居表项。

TopsecOS# **network neighbour add ip** *fe80::252a:b38d:93c7:91f0* **mac-address** *18:a9:05:26:3f:e6* **de***v feth0*

network neighbour clean [dev <*string*>**]**

命令描述：

清空静态邻居表。

参数说明：

参数	说明
dev <*string*>	可选项，清空与相应接口相关的所有静态邻居表项。 字符串类型，输入接口名称。

命令示例：

TopsecOS# **network neighbour clean**

network neighbour show [dev <*string*>**] [type** <static|dynamic>**] [ip** <*string*>**] [mac-address** <*string*>**]**

命令描述：

查看静态邻居表详细信息。

参数说明：

参数	说明
dev <*string*>	可选项，设置接口。 字符串类型。
type <static|dynamic>	可选项，设置类型。 静态|动态
ip <*string*>	可选项，设置 IP 地址。 字符串类型。
mac-address <*string*>	可选项，设置 MAC 地址。 字符串类型。

命令示例：

TopsecOS# **network neighbour show**

7.4 MAC

当接口工作在交换模式时，根据 MAC 地址表来对报文进行转发。MAC 地址表的表项包含 MAC 地址、VLAN、转发的物理接口号。设备在转发报文时，将首先查询 MAC 地址表项中是否包含与目的 MAC 地址匹配的表项。如果有匹配的表项，则将报文通过相应的端口进行转发。如果没有相应的匹配项，则采取广播方式向除接收端口外的所有接口转发该数据报文。

当 TopWAF 进行报文转发时，根据 MAC 地址表中是否包含报文的目的地址，可进行如下处理。

- 如果 MAC 地址表中存在目的 MAC 地址表项，则按照 MAC 地址表进行单播转发。

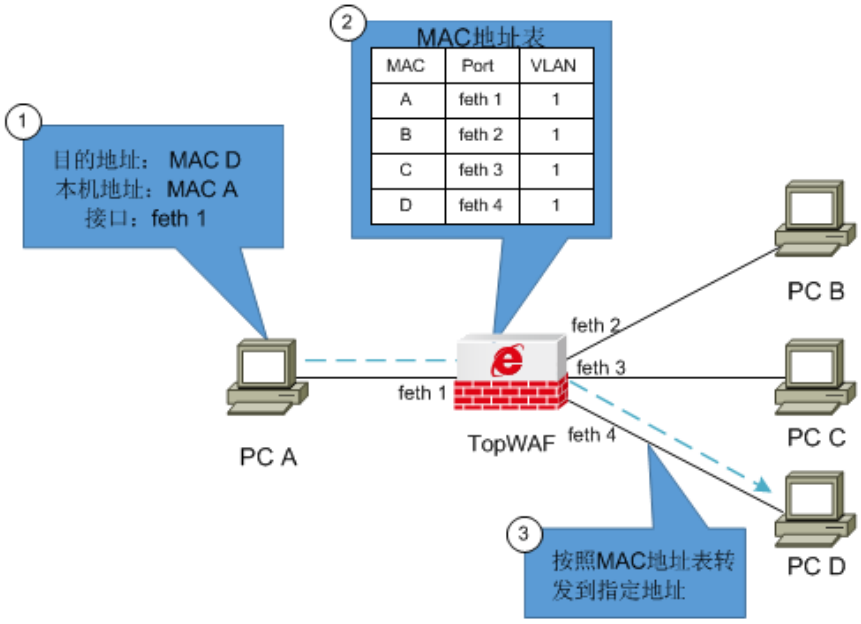


图 7-5 MAC 地址单播示意图

- 如果 MAC 地址表中不存在目的 MAC 地址表项，或者报文的目的地址为广播地址，则在该广播域中进行广播转发。如果在广播域中存在目的 MAC 地址，目的设备响应广播包，TopWAF 将目的地址加入到 MAC 地址表中；如果广播域中没有设备响应，则再有报文的目的地址为该 MAC 地址时，依然进行广播。

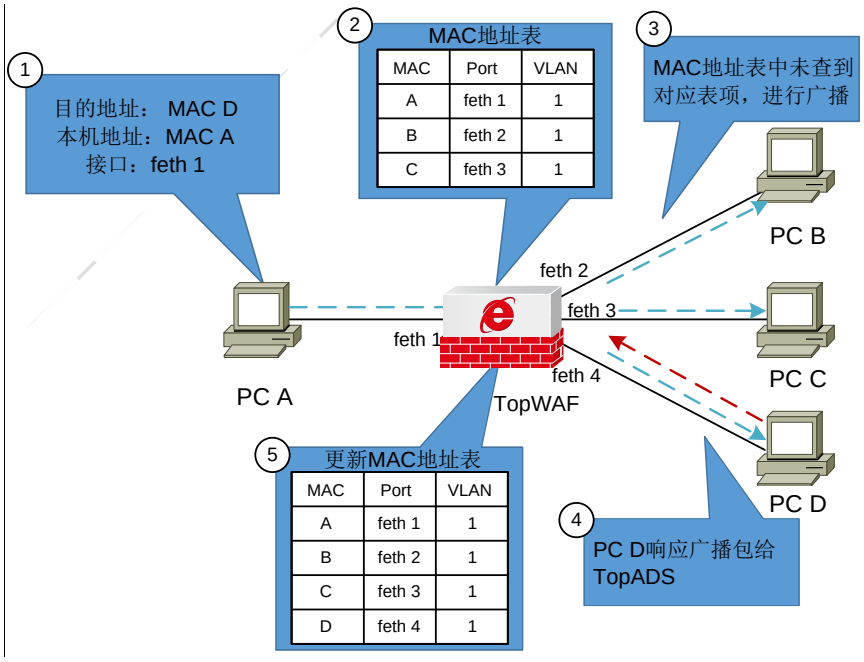


图 7-6 MAC 地址广播示意图

MAC 地址表中的表项包括静态表项和动态表项两种：

- 静态表项

静态表项由管理员配置，不会随着时间而老化。

- 动态表项

动态 MAC 表项由设备自动生成并更新，无需管理员配置。交换接口接收到数据帧时，分析收到数据帧中的源 MAC 地址，如果 MAC 地址表中包含该 MAC 地址对应的表项则更新表项；如果 MAC 地址表中没有该表项，则建立该地址同端口的映射，并将其写入 MAC 地址表中，生成新的动态 MAC 表项。

TopWAF 支持添加和删除静态表项，查看动态表项。

WEBUI 方式

步骤1 配置静态 MAC 表。

1）选择 **网络管理** > **MAC** > **静态 MAC**。

2）点击『添加』，弹出“添加”窗口。

在添加静态项时，各项参数的具体说明如下表所示。

参数	说明
VLAN	选择通过哪个 VLAN 虚拟接口进行转发。 说明： 当“接口”处设定的交换接口工作在“access”模式时，必须选择其所属的 VLAN 的 ID 号；当“接口”处设定的交换接口工作在“Trunk”模式时，可以选择 VLAN 范围中的一个 ID 号。
接口	选择转发的物理接口。只能选择工作在交换模式的物理接口。
物理地址	输入 MAC 地址。

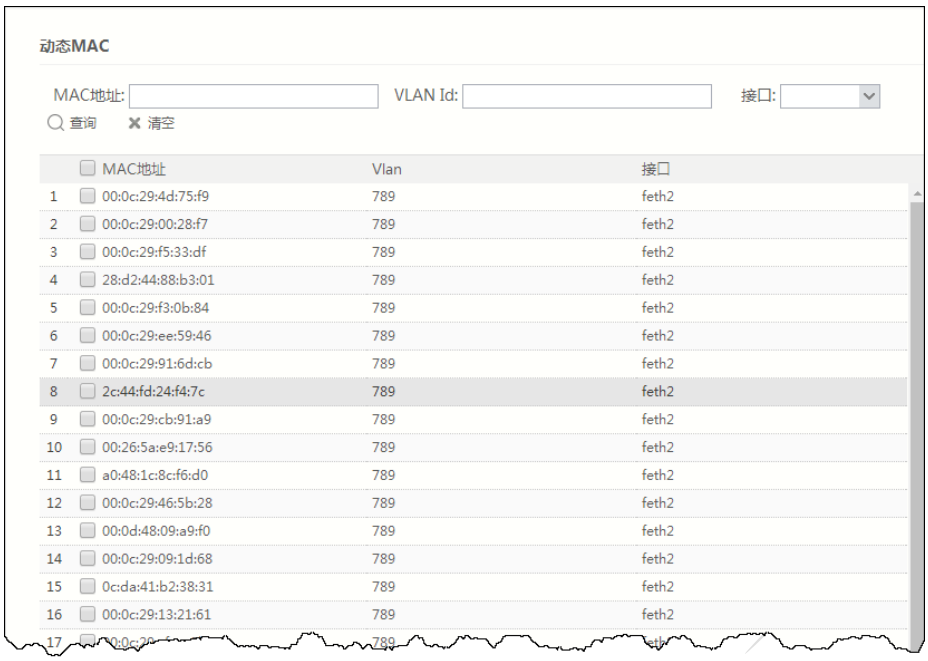
3）设置完成后，点击【确定】按钮完成静态 MAC 的添加。

步骤2 查询静态 MAC 地址表。

在静态 MAC 地址界面中的 VLAN ID 和 MAC 文本框中，输入 VLAN ID 和 MAC 地址，点击『查询』，界面将显示符合查询条件的结果。

步骤3 查看动态 MAC 地址表。

1）选择 **网络管理** > **MAC** > **动态 MAC**，展示自动学习的 MAC 地址表，如下图。



2）在界面 MAC 地址、VLAN ID 文本框中输入 MAC 地址和 VLAN ID，并选择 MAC 地址表的出接口，点击『查询』，界面将显示符合查询条件的结果。

CLI 方式

network mac add <static> **address** <*mac*> **vlan** <*num*> **interface** <*string*>

命令描述：

添加一条静态 MAC 表项。

使用 **network mac delete** 命令删除一条静态 MAC 表项。

参数说明：

参数	说明
address <*mac*>	必选项，设置 MAC 表项的 MAC 地址。 MAC 地址字符串，格式为 AA:BB:CC:DD:EE:FF。
vlan <*num*>	必选项，设置 MAC 表项的 VLAN。 实数类型，取值范围：1-4094。
interface <*string*>	必选项，设置 MAC 表项的接口。 字符串类型，如 feth3。

命令示例：

添加一条 MAC 地址为 a9:0f:ac:dd:56:f9、VLAN 为 10、出接口为 feth3 的 MAC 表项。

TopsecOS# **network interface** *feth3* **switchport**

TopsecOS# **network interface** *feth3* **switchport mode** access

TopsecOS# **network vlan add id** *10*

TopsecOS# **network interface** *feth3* **switchport access-vlan** *10*

TopsecOS# **network mac add** static **address** *a9:0f:ac:dd:56:f9* **vlan** *10* **interface** *feth3*

network mac clean <static|dynamic>

命令描述：

清空 MAC 表。

参数说明：

参数	说明
clean <static|dynamic>	必选项，清空静态 MAC 表项|清空动态 MAC 表项

命令示例：

TopsecOS# **network mac clean** static

network mac show [address <*mac*>**] [type** <static|dynamic >**] [vlan** <*num*>**] [interface** <*string*>**]**

命令描述：

查看 MAC 表。

参数说明：

参数	说明
address <*mac*>	可选项，指定只查看相应 MAC 地址的 MAC 表项。 MAC 地址类型，格式为 AA:BB:CC:DD:EE:FF。
type <static|dynamic >	可选项，指定查看 MAC 表项的类别，默认全部显示。 静态 MAC 表|动态 MAC 表

参数	说明
vlan <*num*>	可选项，指定只查看相应 VLAN 的 MAC 表项。 实数类型，取值范围：1-1024。
interface <*string*>	可选项，输入接口名称，指定只查看该接口的 MAC 表项。 字符串类型。

命令示例：

TopsecOS# **network mac show type dynamic**

Total:10240 Static:2 Link:4

vcom mac vlan dev flags

---

0 4e:b2:bc:3b:a7:bc 1 feth1 dynamic

0 1e:a6:6e:19:2a:c1 1 feth0 dynamic

2 matched mac entries.

7.5 链路探测

链路探测指防火墙每隔一定时间周期性地向预先设定的 IP 发送 ping 包，来检测链路的状况，并会将检测结果在设备 WEBUI 界面上显示，展示链路的连接状况。

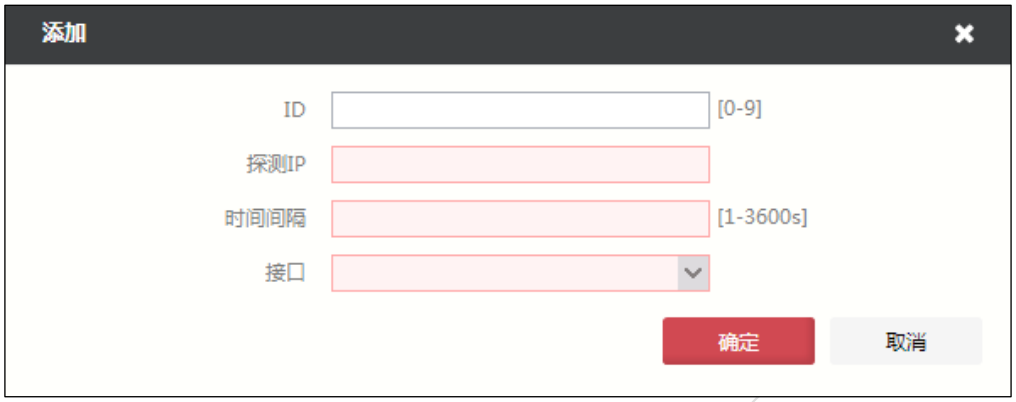
TopWAF 的高可用性（链路备份、双机热备、负载均衡和连接保护）功能依赖于链路探测功能。管理员在配置高可用性功能时，通过引用探测链路的 ID 号使用探测链路功能，TopWAF 即可根据 IP 探测的结果判定某条链路是否可用，确定是否启动主从链路/主从设备切换进程。关于高可用性的介绍具体请参见 8.6 高可用性。

✧ 默认情况下，TopWAF 的链路探测功能处于开启状态。如果探测链路已配置，但暂时还不需要启用该探测链路的探测功能，管理员可登录 CLI 界面，通过命令**#network ip-probe set mode** <enable|disable> **[probe-id** <*number*> **dev**<*string*>**]**，确认是否启用相应链路的探测功能。

WEBUI 配置

步骤1 在左侧导航树中选择 **网络管理** > **链路探测。**

步骤2 点击『添加』，弹出“添加”窗口。如下图所示。



在设置探测链路时，各项参数的具体说明如下表所示。

参数	说明
ID	可选项，设置探测链路 ID，取值范围：0-9。
探测 IP	必选项，设置一个链路外部信任的 IP 地址，TopWAF 通过设定的网络接口定时向该 IP 地址发送 ping 包来探测链路通讯是否正常。 说明： 探测 IP 必须是在正常状态下 TopWAF 能够 ping 通的 IP 地址。
时间间隔	必选项，设置发送 ping 报文的时间间隔。单位：秒；取值范围：1-3600。 说明： 探测时间间隔为上次探测结束的时间和下一次探测开始之间的时间间隔。
接口	必选项，选择探测的设备出接口。可以是物理接口、VLAN 虚接口、bond 口、子接口、ppp0 虚接口等。

步骤3 点击【确定】按钮完成探测链路的创建。

CLI 配置

network ip-probe add probe-ip <*string*> **dev**<*string*>**[interval**<*num*>**] [probe-id** <*num*> **]**

命令描述：

添加链路探测条目。

参数说明：

参数	说明
probe-ip <*string*>	必选项，设置探测 IP。 字符串类型。满足 ipv4 或者 ipv6 的地址类型的要求。
dev<*string*>	必选项，设置出接口名称。 字符串类型。
interval <*num*>	必选项，设置探测间隔。 实数类型。范围：1-3600，单位：秒。
probe-id <*num*>	可选项，设置探测 ID 号。 实数类型。取值范围：0-9。

命令示例：

设置探测 IP 为 192.168.18.5，对应的时间间隔为 20 秒，接口为 feth1，ID 号为 8。

TopsecOS# **network ip-probe add probe-ip** *192.168.18.5* **interval** *20* **dev** *feth1* **probe-id** *8*

network ip-probe set mode <enable|disable> **[dev**<*string*> **] [probe-id** <*num*> **]**

命令描述：

设置是否启用链路探测功能。

参数说明：

参数	说明
mode <enable|disable>	必选项，设置是否启用链路探测功能。 使能|去使能。使能表示启用该功能，去使能表示禁止该功能。
dev<*string*>	可选项，指定探测链路的出接口的名称。 字符串类型。
probe-id <*num*>	可选项，指定链路探测的 ID 号。 实数类型。取值范围 0-9。

命令示例：

TopsecOS# **network ip-probe set mode** *enable*

8 系统管理

TopWAF 的系统管理模块用于关联各功能模块，并可协调、控制各个功能模块的功能和性能，保证系统正常稳定运行。系统的稳定性是 TopWAF 稳定、高效运作的基础。本章主要介绍如何管理、配置、维护、优化系统的基本操作，主要包括以下内容：

- 系统设置：介绍查看及配置系统的基本信息、系统参数、系统时间，配置 SNMP 功能和配置本地域名解析服务器。
- 系统维护：介绍维护配置文件、升级固件、获取健康记录、重启系统、规则库升级、许可证升级和数据库维护。
- 系统诊断：管理员可通过诊断工具和抓包工具对网络的连通性进行探测，以更好地了解网络运行状况并进行相关问题的定位。
- 管理员：介绍一员模式下管理员及其权限管理方法。
- 系统日志：介绍配置日志记录条件、配置日志服务器。
- 高可用性：介绍 TopWAF 的双机热备、负载均衡和连接保护功能的实现方法。

8.1 系统设置

系统设置包括查看系统基本信息、设置系统参数、本机服务和系统时间等。

8.1.1 系统信息

“系统信息”界面显示了 TopWAF 的硬件组成部分和软件组成部分的详细信息。

WEBUI 查看方式

选择 **系统管理** > **系统设置** > **系统信息**，如下图所示。

界面中显示了 TopWAF 的产品型号、产品序列号、操作系统、软件版本、许可证版本号、系统名称、终端超时时间、系统时间、系统运行时间以及许可证过期时间。关于系统名称、终端超时和系统时间的配置具体请参见 8.1.2 系统参数。

CLI 查看方式

system product model <cr>

命令描述：

查看系统产品型号。

命令示例：

TopsecOS# **system product model**

TOPSEC-XX

system product sn <cr>

命令描述：

查看系统产品序列号。

命令示例：

TopsecOS # **system product sn**

001631ffccd4.001

system version <cr>

命令描述：

显示系统版本信息。

命令示例：

TopsecOS# **system version**

VERSION: v3.2242.0038.1_waf_ali

PSN: Unkonw

system devname show <cr>

命令描述：

该命令用于查看 TopWAF 名称。

命令示例：

TopsecOS# **system devname show**

system devname set TopsecOS

system terminal show <cr>

命令描述：

显示终端空闲超时时间。

命令示例：

TopsecOS# **system terminal show**

terminal idle timeout: 60 seconds

system time show <cr>

命令描述：

显示系统日期。

命令示例：

TopsecOS# **system time show**

+08 2018-12-27 15:59:29

system uptime <cr>

命令描述：

显示系统启动后运行的总时间。

命令示例：

TopsecOS# **system uptime**

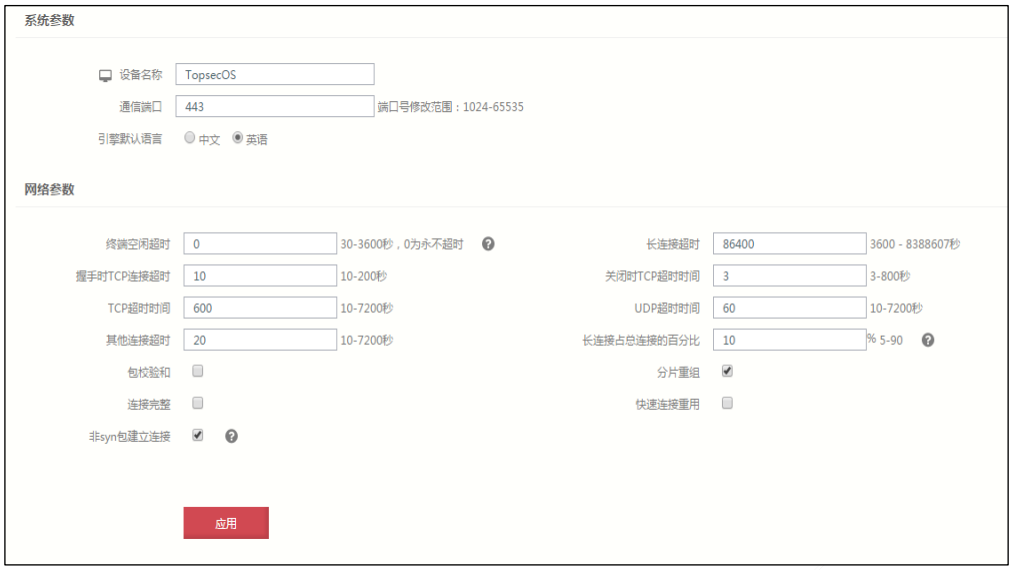
UP 1 day, 00:19:56

8.1.2 系统参数

“系统参数”界面包括标识设备的名称、设备在处理数据报文时的基本网络参数。

WEBUI 方式

选择 **系统管理** > **系统设置** > **系统参数**，如下图所示。



在设置系统参数时，各项参数的具体说明如下表所示。

参数	说明
设备名称	设置 TopWAF 的设备名称，默认为 TopsecOS。
通信端口	设置 WEBUI 访问 WAF 使的端口。取值范围 1024-65535。默认为 443。
引擎默认语言	设置 TopWAF 的语言，可选项：中文、英语。
终端空闲超时	设置管理员通过 WEBUI 方式对 TopWAF 进行管理的空闲超时时间，超过该空闲时间，如果管理员没有对 TopWAF 执行任何操作，该管理连接自动中断。 单位：秒；取值范围：0，30-3600；默认值：180，设置为 0，表示永不超时。
长连接超时	设置长连接的超时时间。 单位：秒；取值范围：3600-8388607；默认值：86400。
握手时 TCP 连接超时	设定建立 TCP 连接的三次握手的超时时间。 单位：秒；取值范围：10-200；默认值：100。
关闭时 TCP 超时时间	设置关闭 TCP 连接的超时时间。 单位：秒；取值范围：3-800；默认值：20。
TCP 超时时间	设置建立 TCP 连接后的空闲超时时间。TCP 连接建立后，在空闲超时时间内，如果无相同五元组的 TCP 连接通过 TopWAF，TopWAF 则将该建立的连接删除。 单位：秒；取值范围：10-7200；默认值：1800。
UDP 超时时间	设置建立 UDP 连接后的空闲超时时间。UDP 连接建立后，在空闲超时时间内，如果没有相同五元组的 UDP 连接通过 TopWAF，TopWAF 则将该建立的连接删除。 单位：秒；取值范围：10-7200；默认值：60。
其他连接超时	设置除 TCP、UDP 连接外其他类型连接的超时时间。 单位：秒；取值范围：10-7200；默认值：20。
长连接占总连接	设置长连接占总连接百分比的上限。单位：%；取值范围：5-90。

参数	说明
的百分比	说明： 当长连接占总连接的百分比超过此处设置的值，TopWAF 将自动删除存在时间较长的长连接，以避免大量的长连接一直占用内存。
包校验和	设置是否对 IP/TCP/UDP/ICMP 数据包进行校验。
分片重组	设置是否支持对接收到的分片 IP 数据包进行重组。
连接完整	是否启用 TCP 连接完整性状态检测开关。 说明： 1）TCP 连接完整性状态检测开关处于开启状态下时，TopWAF 会跟踪 TCP 连接的状态，TCP 连接必须通过完整的三次握手，TopWAF 才允许其建立连接；TCP 连接经过四次结束握手或者收到 RST 数据包，TopWAF 才终结其连接。 2）在特殊情况下，对于某种 TCP 连接，如果建立的时候并没有经过 TopWAF，连接建立以后需要经过 TopWAF，则需要关闭状态检测开关，否则，该种连接会因不符合 TopWAF 的 TCP 连接完整性标准而被丢弃。
快速连接重用	是否启用快速连接重用开关。采用 TCP 连接复用技术后，客户端与 TopWAF 之间进行三次握手并发送 HTTP 请求。TopWAF 收到请求后，会检测服务器是否存在空闲的长连接，如果不存在，服务器将建立一个新连接。当 HTTP 请求响应完成后，客户端则与 TopWAF 协商关闭连接，而 TopWAF 则保持与服务器之间的这个连接。当有其它客户端需要发送 HTTP 请求时，TopWAF 会直接向与服务器之间保持的这个空闲连接发送 HTTP 请求，避免了由于新建 TCP 连接造成的延时和服务器资源耗费。
非 syn 包建立连接	对于 TCP 连接，设置是否允许第一个报文不是 SYN 报文的连接建立新连接。

系统参数设置完成后，点击【应用】按钮完成系统参数的配置。

CLI 方式

system devname set <*nstring*>

命令描述：

该命令用于配置 TopWAF 名称。

参数说明：

参数	说明
devname set <*nstring*>	设置 TopWAF 的名称。 字符串类型，默认值：TopsecOS。

命令示例：

修改系统名称为 TopOS。

TopsecOS# **system devname set** *TopOS*

system terminal idle-timeout <*num*>

命令描述：

设置终端空闲超时时间。

参数说明：

参数	说明
idle-timeout <*num*>	设置终端空闲超时时间。 实数类型。单位：秒；取值范围：0，30-3600；默认值：60，0 表示永不超时。

命令示例：

设置终端空闲超时时间为 60 秒。

TopsecOS# **system terminal idle-timeout** *60*

network session timeout never-expire <*num*|default>

命令描述：

设置长连接的超时时间。

参数说明：

参数	说明
never-expire <*num*|default>	设置长连接的超时时间。 实数类型，单位：秒；取值范围：3600-8388607；default 表示默认超时值，默认为 86400。

命令示例：

设置长连接的超时时间为 2 天。

TopsecOS#**network timeout never-expire** *172800*

network session timeout handshake <*num*|default>

命令描述：

设置 TCP 三次握手的超时时间。

参数说明：

参数	说明
timeout handshake <*num*|default>	设置 TCP 三次握手的超时时间。 实数类型，单位：秒；取值范围：10-200；default 表示默认超时值，默认为 100。

命令示例：

设定三次握手阶段 TCP 连接的超时时间为 150 秒。

TopsecOS#**network session timeout handshake** *150*

设定三次握手阶段 TCP 连接的超时时间为默认值。

TopsecOS# **network session timeout handshake** default

network session timeout close <*num*|default>

命令描述：

设置关闭 TCP 连接的超时时间。

参数说明：

参数	说明
timeout close <*num*|default>	设置关闭 TCP 连接的超时时间。 实数类型，单位：秒；取值范围：3-800；default 表示默认超时值，默认为 20。

命令示例：

设定关闭 TCP 连接的超时时间为默认值 20 秒。

TopsecOS#**network session timeout close** default

设定关闭 TCP 连接的超时时间为 200 秒。

TopsecOS#**network session timeout close** *200*

network session timeout established <*num*|default>

命令描述：

设置建立 TCP 连接后的空闲超时。

参数说明：

参数	说明
timeout established <*num*|default>	设置建立 TCP 连接后的空闲超时。 实数类型，单位：秒；取值范围：10-7200；default 表示默认超时值，默认为 1800。

命令示例：

设定已建立 TCP 连接的超时时间为默认值。

TopsecOS# **network session timeout established** default

network session timeout udp <*num*|default>

命令描述：

设置 UDP 连接的超时时间。

参数说明：

参数	说明
timeout udp <*num*|default>	设置 UDP 连接的超时时间。 实数类型，单位：秒；取值范围：10-7200；default 表示默认超时值，默认为 60。

命令示例：

设定 UDP 连接的超时时间为默认值 60 秒。

TopsecOS#**network session timeout udp** default

设定 UDP 连接的超时时间为 200 秒。

TopsecOS#**network session timeout udp** *200*

network session timeout other <*num*|default>

命令描述：

设置除 TCP、UDP 连接外其他类型连接的超时时间。

参数说明：

参数	说明
timeout other <*num*|default>	设置除 TCP、UDP 连接外其他类型连接的超时时间。 实数类型，单位：秒；取值范围：10-7200；default 表示默认超时值，默认为 20。

命令示例：

设定其他类型连接的超时时间为默认值 20 秒。

TopsecOS#**network session timeout other** default

设定其他类型连接的超时时间为 200 秒。

TopsecOS#**network session timeout other** *200*

network session timeout default <cr>

命令描述：

将所有连接的超时参数设置为默认值。

命令示例：

TopsecOS#**network session timeout default**

network session never-expire-percent <*num*>

命令描述：

设置长连接占总连接百分比的上限。

参数说明：

参数	说明
never-expire-percent	设置长连接占总连接百分比的上限。

参数	说明
<*num*>	实数类型，单位：%；取值范围：5-90；默认值：10。

命令示例：

设置长连接占总连接百分比的上限为 20%。

TopsecOS# **network session never-expire-percent** *20*

network session packet-checksum <on|off>

命令描述：

设定是否对 TCP、UDP、ICMP 的 IP 数据报文进行校验。

命令示例：

TopsecOS# **network session packet-checksum** on

network session defrag <on|off>

命令描述：

设置 TopWAF 是否支持对分片的 IP 报文具有重组的功能，默认情况下，TopWAF 的重组开关处于开启状态。

命令示例：

TopsecOS# **network session defrag** off

network session session-integrity <on|off>

命令描述：

TCP 连接完整性状态检测开关设置。

命令示例：

TopsecOS# **network session session-integrity** off

network session syn-reset <on|off>

命令描述：

快速连接重用设置。

命令示例：

TopsecOS# **network session syn-reset** on

network session only-syn-create <on|off>

命令描述：

TopWAF 对接收的 TCP 数据包的第一个 TCP 报文进行限定，如果第一个报文为 SYN 报文才允许建立连接。

命令示例：

TopsecOS# **network session only-syn-create** on

8.1.3 本机服务

8.1.3.1 服务设置

服务就是管理员对设备的访问权限控制，TopWAF 支持通过 WEBUI、Telnet、SSH 方式进行远程访问。

通过服务模块，管理员可设置允许访问 TopWAF 的方式，提高设备的安全性。

WEBUI 方式

步骤1 选择 **系统管理** > **系统设置** > **本机服务**。

在设置本地服务时，各项参数的具体说明如下表所示。

参数	说明
sshd 服务	设置是否允许通过 SSH 方式远程访问 TopWAF。可选项：开启和关闭。
telnet 服务	设置是否允许通过 Telnet 方式远程访问 TopWAF。可选项：开启和关闭。
httpd 服务	设置是否允许通过 WEBUI 方式远程访问 TopWAF。可选项：开启和关闭。

步骤2 参数配置完成后，点击【应用】按钮完成设置。

步骤3 （可选）点击【重置】按钮，可以恢复本地服务的设置为出厂配置，此时将关闭通过 WEBUI、Telnet、SSH 方式进行远程访问 TopWAF。

CLI 方式

system service sshd <on|off>

命令描述：

设置是否允许通过 SSH 方式远程访问 TopWAF。

命令示例：

TopsecOS# **system service sshd** on

system service telnetd <on|off>

命令描述：

设置是否允许通过 Telnet 方式远程访问 TopWAF。

命令示例：

TopsecOS# **system service telnetd** on

system service httpd <on|off>

命令描述：

设置是否允许通过 WEBUI 方式远程访问 TopWAF。

命令示例：

TopsecOS# **system service httpd** on

system service default <cr>

命令描述：

恢复本地服务的设置为出厂配置，此时将关闭通过 WEBUI、Telnet、SSH 方式进行远程访问 TopWAF。

命令示例：

TopsecOS# **system service default**

8.1.3.2 服务

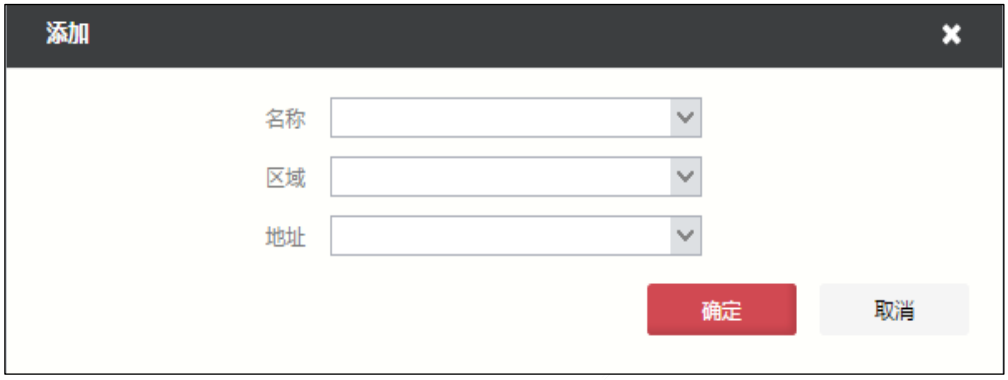
服务就是设备本身提供的管理服务或者信息服务，如 WEBUI、Telnet、SSH、DHCP 等。通过服务模块，管理员可对区域对象或地址对象添加支持的本机服务，并通过配置对本机端口的访问控制规则，允许设备在相应的物理接口接收用户的连接请求。如果设备要接收管理员

发出的管理或监控的连接请求，设备上相应的系统服务进程还必须处于“启动”状态，否则无法接收用户的连接请求。

WEBUI 方式

步骤1 选择 **系统管理** >**系统设置** > **本机服务**。

步骤2 点击『添加』，弹出“添加”窗口。如下图所示。



在设置本机服务时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置 TopWAF 支持规则控制的服务类型。可选项：snmp、ssh、ping、telnet、ntp、dhcp、webui、dns、tp、bgp。 1）snmp：允许设备与 snmp 管理主机进行通信。 2）ssh：接收 SSH 协议远程管理请求；允许管理员通过 SSH 方式对设备进行配置和管理。 3）ping：允许管理员可以 PING 到设备的物理接口地址、VLAN 虚接口和子接口的地址，还支持 TopWAF PING 其他网络设备的 IPv6 接口，以及支持其他网络设备 PING 防火墙的 IPv6 接口。 4）telnet：接收 Telnet 协议远程管理请求。 5）ntp：用于计算机时间同步化的一种协议，能够使计算机对其服务器或时钟源做同步化，提供高精准度的时间校正。TopWAF 作为 NTP 服务器为其他网络设备提供 NTP 服务； 6）dhcp：允许设备作为 DHCP/DHCPv6 服务器、DHCP/DHCPv6 客户端或 DHCP/DHCPv6 中继使用。 7）webui：开放该服务用于允许管理员通过 WEBUI 对设备进行配置和管理。 8）dns：允许设备作为 DNS 服务器进行域名解析。 9）tp：允许设备与 topolicy 管理工具进行通信，以便对 TopWAF 设备进行管理。 10）bgp：允许使用 BGP 动态路由协议。
区域	必选项，设置本机服务支持的区域对象。关于区域对象的配置具体请参见 6.1.1 区域。

参数	说明
地址	可选项，指定本机服务支持的地址对象。关于地址对象的配置具体请参见 6.1.2 地址。 说明： 当本机服务为“dhcp”时，该参数不可配置。

步骤3 点击【确定】按钮完成本机服务的添加。

CLI 方式

pf service add name <telnet|webui|ssh|ping|ntp|dhcp|snmp|dns|tp|bgp> **area** <*string*> **addressname** <*string*>

pf service add name dhcp **area** <*string*>

命令描述：

添加本机服务。

可使用 p**f service delete** 命令删除本机服务配置。

可使用 **pf service modify** 命令修改本机服务访问控制规则。

参数说明：

参数	说明
name <telnet|webui|ssh|ping|ntp|dhcp|snmp|dns|tp|bgp>	必选项，设置服务名称。 1）telnet：接收 Telnet 协议远程管理请求。 2）webui：当 TopWAF 不包含 SSL VPN 模块时，开放该服务用于允许管理员通过 WEBUI 的 443 端口对设备进行配置和管理。 3）ssh：接收 SSH 协议远程管理请求；允许管理员通过 SSH 方式对设备进行配置和管理。 4）ping：允许管理员可以 PING 到设备的物理接口地址、VLAN 虚接口和子接口的地址。 5）ntp（Network Time Protocol）：用于计算机时间同步化的一种协议，能够使计算机对其服务器或时钟源做同步化，提供高精准度的时间校正。TopWAF 作为 NTP 服务器为其他网络设备提供 NTP 服务。 6）dhcp：允许设备作为 DHCP/DHCPv6 服务器、DHCP/DHCPv6 客户端或 DHCP/DHCPv6 中继使用。 7）dns：允许设备作为 DNS 服务器进行域名解析。 8）snmp：允许设备与 snmp 管理主机进行通信。

参数	说明
	9）tp：允许设备与 topolicy 管理工具进行通信，以便对 TopWAF 设备进行管理。 10）bgp：允许使用 BGP 动态路由协议。
area <*string*>	必选项，设置本机服务支持的区域对象。 说明： 字符串类型。不能包含“&\”\\’%<>”中任意字符，也不能包含空格。 区域参数和地址参数不能全部为空。
addressname <*string*>	必选项，设置本机服务支持的地址对象。 字符串类型。不能包含“&\”\\’%<>”中任意字符，也不能包含空格。

命令示例：

添加名称为 telnet 的本机服务，支持的区域对象为 area_feth0。

TopsecOS# **define area add name** *area_feth0* **interface** *feth0*

TopsecOS# **pf service add name** telnet **area** *area_feth0*

pf service clean<cr>

命令描述：

清除所有本机服务访问控制规则。

pf service show <cr>

命令描述：

查看所有本机服务访问控制规则。

命令示例：

TopsecOS# **pf service show**

ID 8001 pf service add name ssh area area_feth0

ID 8002 pf service add name telnet area area_feth0

ID 8003 pf service add name webui area area_feth0

```
ID 8004 pf service add name ping area area_feth0
ID 12400 pf service add name snmp area area_feth0
```

8.1.4 系统时间

TopWAF 内置时钟，是记录日志信息、安全策略、监控系统等事件的时间基准，因此，TopWAF 时间对具有时间戳的策略发生作用产生直接影响。TopWAF 为确保时间的精准性提供了系统时间管理功能，管理员可以手动修改系统时间，可以简单地根据管理主机的内置时钟对 TopWAF 时钟进行同步，也可以启动 NTP（Network Time Protocol，网络时间协议）服务根据设定的 NTP 服务器上的时间来同步 TopWAF 的系统时钟。其中，通过 NTP 可使用户网络中的应用服务器、其他安全产品及网络管理系统等保持系统时间的严格一致，使 TopWAF 几乎零时差防护用户网络成为可能。

NTP 基于 UDP 传输，使用端口号 123，是为网络设备向参考时间源提供高精准度时间同步的协议。TopWAF 既可以作为 NTP 服务器也可作为 NTP 客户端，NTP 服务器提供参考时间可为网络设备提供授时服务，为整个网络传递统一、标准的时间；NTP 客户端周期向 NTP 服务器设备发送 NTP 报文以同步其时间。

假设 TopWAF 作为 NTP 客户端，TopWAF 系统时间为 11:00:00am，NTP 服务器系统时间为 12:00:00am，NTP 数据包在 TopWAF 与 NTP 服务器间单向传输需要 1s，TopWAF 和 NTP 服务器处理 NTP 数据包的时间均为 1s，NTP 同步时间实现原理简要描述如下图所示。

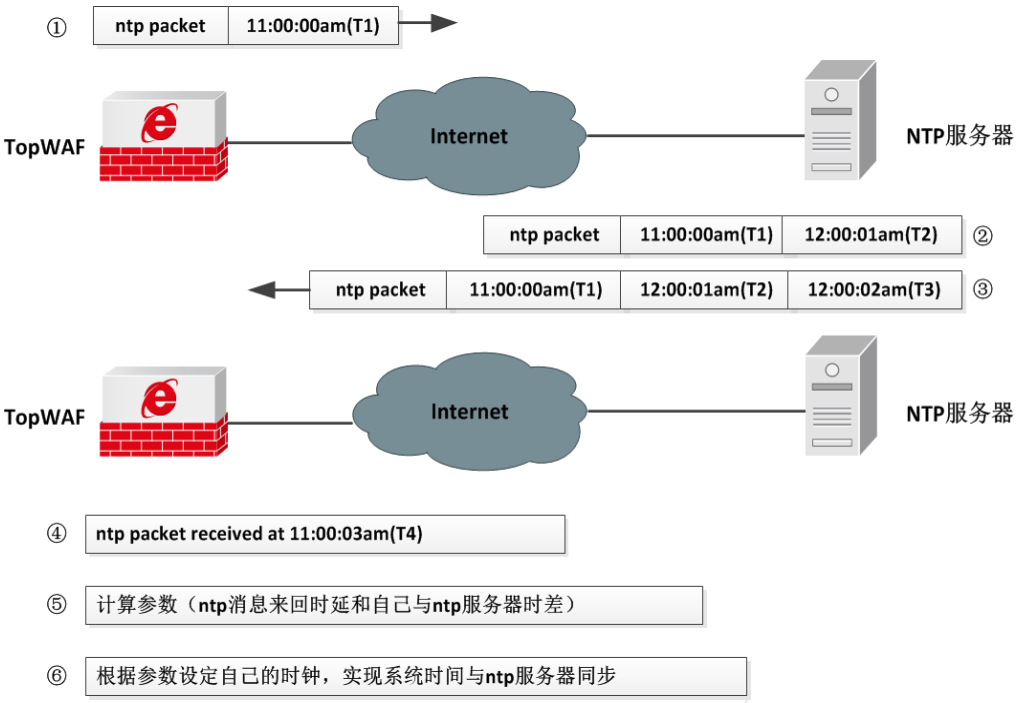


图 8-1 NTP 实现过程图

- TopWAF 向 NTP 服务器发送 NTP 报文，报文中带有报文离开 TopWAF 时的时间戳 11:00:00am（T1）。
- NTP 服务器接收到该 NTP 报文，在该报文中加上报文到达时间戳 12:00:01am（T2），然后再加上其向 TopWAF 回复确认 NTP 报文的时间戳 12:00:02am（T3），发送给 TopWAF。
- TopWAF 接收到该 NTP 报文时，加上接收到该报文的时间戳 11:00:03am（T4）。至此，TopWAF 获取了 TopWAF 相对于 NTP 服务器的时间差为（（T2-T1）+（T3-T4））/2 和 NTP 消息来回一个周期的时延为（T4-T1）-（T3-T2），最后 TopWAF 根据获取的其与 NTP 服务器的时间差及 NTP 消息来回时延设定自己的时钟，实现其与 NTP 服务器的时钟同步。

TopWAF 作为 NTP 客户端时，会向 NTP 服务器定期发送 NTP 报文以同步时间，同步时间时，首先向主 NTP 服务器同步时间，如果主 NTP 服务器不可达时，则向备份 NTP 服务器同步时间。

本节主要介绍系统时间的配置。

WEBUI 方式

步骤1 选择 **系统管理** > **系统设置** > **系统时间**。

步骤2 设置时区。在“时区”下拉框中选择 TopWAF 设备所处区域的时区。

步骤3 设置系统时间。修改系统时间的方式有三种，下面分别予以详细介绍。

- 手动修改：选中“手动设置”，点击“系统日期时间”右侧文本框后的时间设置工具设置系统时间。
- 与管理主机时间同步：选中“本地同步”。
- 与 NTP 服务器时间同步：选中“NTP 设置”，在服务器地址文本框中输入 NTP 服务器的 IP 地址。

在设置 NTP 服务器时，各项参数的具体说明如下表所示。

参数	说明
服务器地址 1	输入首选的 NTP 服务器的 IP 地址。
服务器地址 2	在有备用 NTP 服务器的情况下，输入备用 NTP 服务器的 IP 地址。 说明： TopWAF 无法通过首选 NTP 服务器同步时间时，将尝试与备用 NTP

参数	说明
	服务器的时间同步。
同步地址	需通过 NTP 服务器手动即时同步系统时间时，该参数为必选项。输入 NTP 服务器的 IP 地址，点击【立即同步】按钮，TopWAF 立即与该 NTP 服务器时间同步。 说明： “同步地址”处配置的 NTP 服务器为 TopWAF 一次同步时间 NTP 服务器。

- ✧ 通过 NTP 服务器周期性同步系统时间之前，建议尽可能先将系统时间设置为接近正确的时间。
- ✧ 在“NTP 服务器地址 1”/“NTP 服务器地址 2”处配置了 NTP 服务器地址，TopWAF 即作为 NTP 客户端周期性发送 NTP 报文向 NTP 服务器地址 1”/“NTP 服务器地址 2”处配置的 NTP 服务器同步时间，也同时作为 NTP 服务器为其他网络设备提供时间基准。

步骤4 时区和时间设置完成后，点击【应用】按钮完成 TopWAF 系统时间的修改。

CLI 方式

system time set [**clock** <*string*>] [**date** <*string*>] [**timezone** <*string*>]

命令描述：

手工设置系统日期。

参数说明：

参数	说明
clock <*string*>	可选项，设置时间，时、分、秒。 字符串类型，形为 HH:MM:SS。不能包含“&\”\\’%<>”中任意字符，也不能包含空格。
date <*string*>	可选项，设置日期，年、月、日。 字符串类型，形为 YYYY-MM-DD。不能包含“&\”\\’%<>”中任意字符，也不能包含空格。
timezone <*string*>	可选项，设置时区。 字符串类型，不能包含“&\”\\’%<>”中任意字符，也不能包含空格。格式为<+|->TZ，“+”表示东区，“-”表示西区，“TZ”取值范围：1-12。

命令示例：

设置时间为 2013-10-01 的 12:00:00，时区为东八区。

TopsecOS# **system time set clock** *12:00:00* **date** *2013-10-01* **timezone** *+8*

system ntp start [**addr** <*mstring*>] [**addr2** <*mstring*>]

命令描述：

当不指定 IP 参数时，启动 TopWAF 作为 NTP 服务器。当指定 IP 参数时，启动 TopWAF 作为 NTP 客户端与 IP 参数设置的 NTP 服务器进行时间同步。

参数说明：

参数	说明
addr <*mstring*>	可选项，当 TopWAF 作为 NTP 客户端时，设定 NTP 服务器 IPv4 地址。 IPv4 地址字符串，形为 A.B.C.D，不以“\\”结尾且不包含“<script>”字符串。
addr2 <*mstring*>	可选项，当 TopWAF 作为 NTP 客户端时，设定备份 NTP 服务器 IPv4 地址。 IPv4 地址字符串，形为 A.B.C.D，不以“\\”结尾且不包含“<script>”字符串。

命令示例：

启动 NTP 同步，服务器为 192.168.90.20。

TopsecOS# **system ntp start addr** *192.168.90.20*

启动 NTP 服务器。

system ntp start

system ntp show <cr>

命令描述：

显示 NTP 的配置信息和状态。

命令示例：

TopsecOS# **system ntp show**

NTP Config :

Mode : Client

Status : Running

Server1 : 1.1.1.1

Last sync time : none

system ntp stop <cr>

命令描述：

停止 NTP 同步进程。

命令示例：

TopsecOS# **system ntp stop**

TopsecOS# **system ntp show**

NTP Config :

Mode : Server

Status : Stopped

system ntp update addr <*mstring*>

命令描述：

TopWAF 上的时间和 NTP 服务器立即同步时间。

参数说明：

参数	说明
addr <*mstring*>	必选项。设定 NTP 服务器的 IPv4 地址。 IPv4 地址字符串，格式为 A.B.C.D，不以“\\”结尾且不包含“<script>”字符串。

命令示例：

通过 NTP 服务器 172.16.1.23 立即同步时间。

TopsecOS# **system ntp update addr** *172.16.1.23*

8.1.5 SNMP

SNMP（Simple Network Management Protocol，简单网络管理协议），是 TCP/IP 网络基于 UDP 协议的网络管理标准协议，用于网络管理员集中管理网络中的网络设备。其网络管理模型包括以下部件：SNMP 管理站、SNMP 代理、被管理设备、MIB，各部件的联系如下图所示。

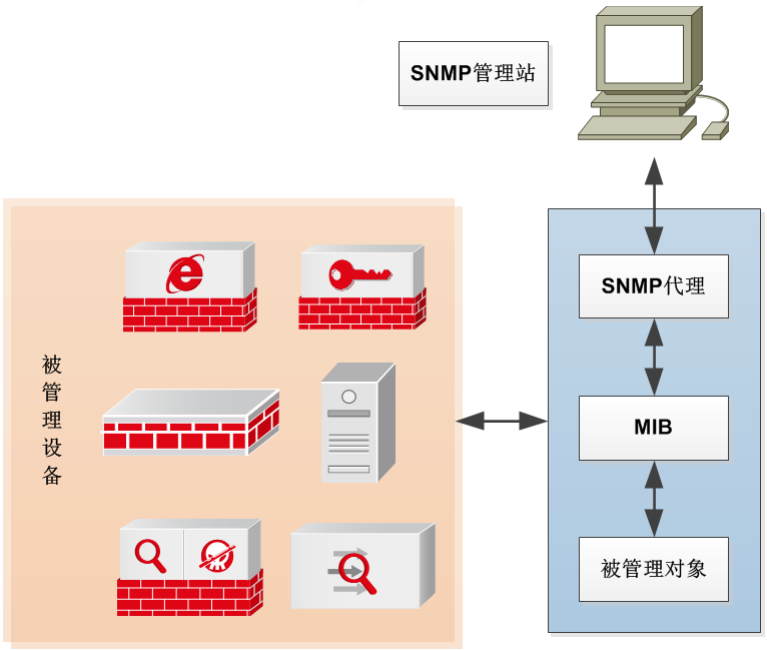


图 8-2 SNMP 网络管理模型

1）SNMP 管理站，是运行 SNMP 网络管理软件的独立设备（一般为 PC），作为网络管理员集中管理网络设备的接口。其基本构成包括：一组具有分析数据、发现故障等功能的管理程序；一个用于监控网络的接口；一个从被管网络实体的 MIB 中抽取信息的数据库。管理站可以实现以下功能：

- 向网络设备发送“读”请求报文。
- 接收网络设备的响应报文、Trap 消息以及报警消息。

2）SNMP 代理，嵌入到网络设备中的功能模块，即指网络上设备支持的 SNMP 代理服务。通过在某网络设备上启动 SNMP 服务，网络管理员则可通过 SNMP 管理站远程获取网络设备的配置信息和实时信息。SNMP 代理可以实现以下功能：

- 接收来自 SNMP 管理站的请求报文。
- 响应来自 SNMP 管理站的“读”请求。
- 根据系统内部设定，主动地向 SNMP 管理端发送 TRAP 消息。

3）被管理设备，指运行 SNMP 代理服务的网络设备，如计算机、路由器、交换机、防火墙、VPN、IPS 等支持 SNMP 代理服务的网络设备。

4）MIB（Management Information Base，管理信息库），提供了标识网络设备所有可能被管理对象的集合，向管理站表明被管理设备的哪些部件可被管理。SNMP 管理站通过读取 MIB 中具体的对象来获取设备配置或运行状况进行网络监控，并可以通过修改 MIB 中对象的变量值改变 SNMP 代理处资源的配置。

网络设备中任何一个可被管理的对象都用 MIB 集合中的一个元素表示，为唯一标识设备中的可被管理对象，MIB 采用树形结构命名方案来标识网络对象。网络对象由 MIB 中从根开始的路径唯一识别，根据如下 MIB 结构图，interface 由{1.3.6.1.2.1.2}唯一表示。

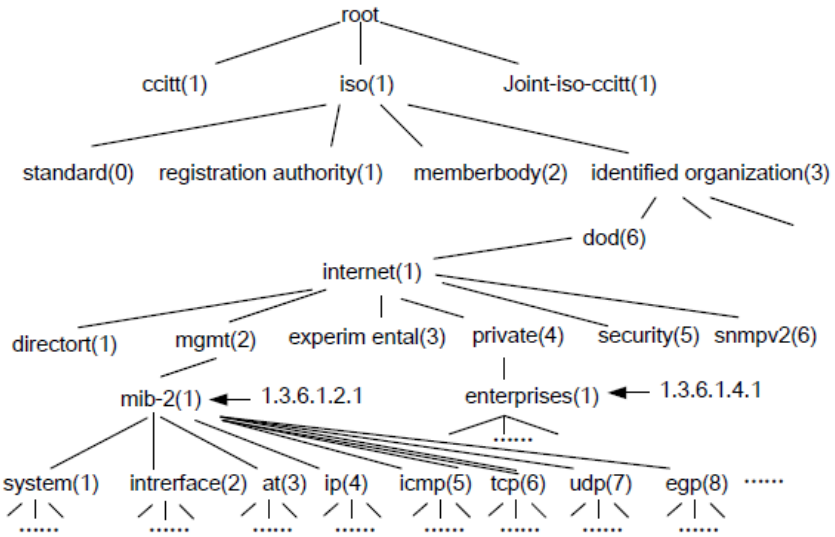


图 8-3 MIB 结构图

MIB 包括公有标准 MIB 库和厂商私有 MIB 库，天融信根据自身产品的特点自定义了 TOPSEC MIB 库，方便网络管理员获取天融信产品各功能模块的“读”权限。

TopWAF 内嵌 SNMP 代理服务功能模块，兼容 SNMPv1、SNMPv2 以及 SNMPv3，支持主流的 SNMP 管理软件（如 PRTG Network Monitor、SolarWinds、HP 的 Open View 等等）对其进行管理，也可以响应 SNMP 管理站的查询请求，并可主动向 SNMP 陷阱主机发送 TRAP 消息及报警信息，其可实现功能如下图所示。

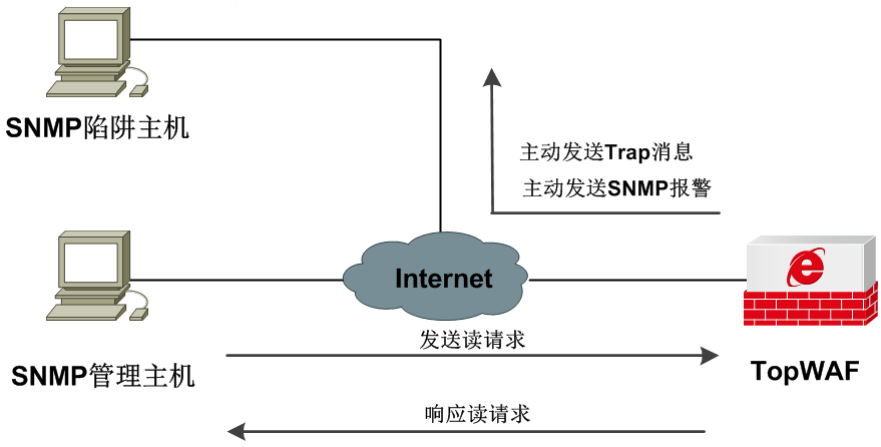


图 8-4 TopWAF 的 SNMP 功能示意图

网络管理员要通过 SNMP 管理软件管理 TopWAF，以及能接收 TopWAF 能主动发送其 Trap 消息及报警信息，需要进行如下设置：

- 配置管理主机/陷阱主机。

  1）在管理主机/陷阱主机上安装 SNMP 管理软件（比如 PRTG Network Monitor、SolarWinds、HP OPENVIEW 软件）。

  2）导入公有 MIB 库或 TOPSEC MIB 库（可从随机光盘中获得）并做简单配置，关于 SNMP 管理软件的安装及相关配置具体请参考相关管理软件的使用手册。

- 配置 TopWAF。

  1）对 SNMP 管理区域的管理/陷阱主机开放 SNMP 服务。

  2）添加管理主机对象。

  3）添加陷阱主机对象。

  4）可选。如果采用 SNMPV3 版本，需添加 SNMP V3 用户。

  5）启动 SNMP 服务。

8.1.5.1 SNMP 服务控制

TopWAF 上必须启动 SNMP 服务才能支持 SNMP 管理主机管理以及向 SNMP 陷阱主机主动发送 Trap 消息。下面介绍 TopWAF 如何启动 SNMP 服务。

WEBUI 方式

步骤1 选择 **系统管理** > **系统设置** > **SNMP**，“SNMP 服务控制”界面如下图所示。

在配置 SNMP 服务控制的参数时，各项参数的具体说明如下表所示。

参数	说明
位置	记录设备在网络环境中的位置。设备出现故障问题时，方便管理员快速定位设备存放地点，默认显示天融信公司官方网站地址。

参数	说明
联系	记录设备直接责任人的联系方式，可以为电话号码或 Email 地址。通过配置此参数，将重要信息存储在 TopWAF 中，以便出现紧急问题时查询使用。默认显示天融信公司客服的邮件地址。

✧ 修改参数的配置后，管理员必须重新启动 SNMP 服务才能使参数生效。

步骤2 参数设置完成后点击【应用】按钮保存参数修改。若没有修改默认参数，略去此步骤。

步骤3 点击【启动】按钮，启动 SNMP 服务；点击【停止】按钮，则停止 SNMP 服务。

CLI 方式

system snmp set location <*mstring*>

命令描述：

设置启用了 SNMP 服务的 TopWAF 在网络环境中的位置。

参数说明：

参数	说明
location <*mstring*>	设置启用了 SNMP 服务的 TopWAF 在网络环境中的位置。字符串类型。不以“\\”结尾且不包含“<script>”字符串。

命令示例：

设置 TopWAF 位置为 www.topsec.com.cn。

TopsecOS# **system snmp set location** *www.topsec.com.cn*

system snmp set contact <*mstring*>

命令描述：

设置 TopWAF 设备直接责任人的联系方式。

参数说明：

参数	说明
contact <*mstring*>	设置 TopWAF 设备直接责任人的联系方式。可为电话号码、邮箱地址等信息。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。

命令示例：

设置 TopWAF 设备负责人信息为 support@topsec.com.cn。

TopsecOS# **system snmp set contact** *support@topsec.com.cn*

system snmp start <cr>

命令描述：

启动 TopWAF 的 SNMP 服务，启动 SNMP 服务后，将不能配置管理主机、陷阱主机以及 SNMPV3 用户。

命令示例：

TopsecOS# **system snmp start**

system snmp stop <cr>

命令描述：

停止 TopWAF 的 SNMP 服务。

命令示例：

TopsecOS# **system snmp stop**

system snmp show <config|status>

命令描述：

查看 SNMP 配置和运行状态信息。

参数说明：

参数	说明
show <config|status>	查看 SNMP 的配置和运行状态信息。可选项为：配置信息|状态信息。

命令示例：

TopsecOS# **system snmp show** status

snmpd is not running!

8.1.5.2 SNMP 管理主机

SNMP 采用 C/S 架构，管理站使用知名端口号 162 接收 Trap 消息及报警消息，客户端使用知名端口号 161 接收查询设备信息。网络管理员通过 SNMP 管理主机管理 TopWAF 的原理图如下。

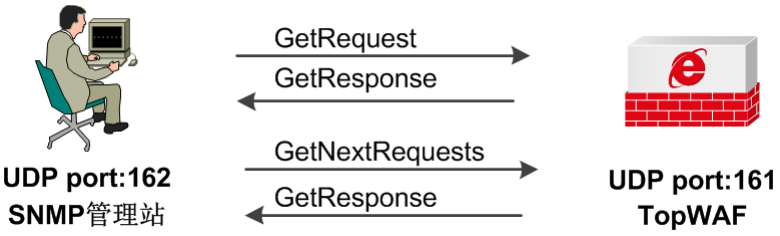


图 8-5 SNMP 管理主机管理网络设备示意图

网络管理员通过管理主机查询 TopWAF 的操作命令说明如下：

- GetRequest：管理站向网络设备某功能节点发起“读”请求，获取设备某功能节点的配置信息或实时状态信息。
- GetNextRequests：管理站向网络设备某功能节点发起“读”请求，在 GetRequest 的基础上获取其相邻另一个功能节点的配置信息或实时状态信息。

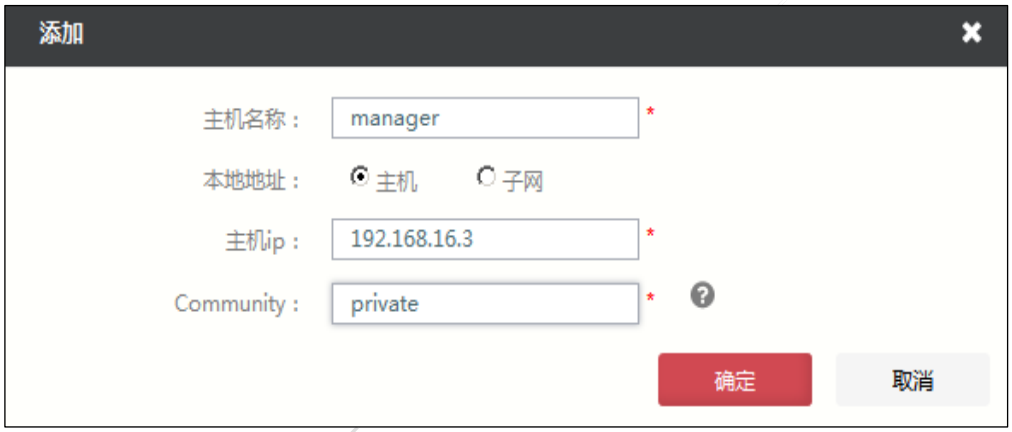
- GetBulk：管理站向网络设备发起“读”请求，相当于连读多次执行 GetNextRequests 操作，方便管理员批量查询网络设备信息，提示管理效率。
- GetResponse：网络设备响应管理站发起的 GetRequest、GetNextRequests、GetBulk 操作。

管理主机安装 SNMP 管理软件并导入了公有 MIB 库或 TOPSEC MIB 库后，还需要在 TopWAF 上添加管理主机信息。下面介绍如何在 TopWAF 上添加 SNMP 管理主机。

WEBUI 方式

步骤1 选择 **系统管理** > **系统设置** > **SNMP**。

步骤2 激活“SNMP 管理主机”页签，点击『添加』，如下图所示。



在添加 SNMP 管理主机时，各项参数的具体说明如下表所示。

参数	说明
主机名称	必选项，添加该管理主机的名称。
本地地址	设置管理主机的类型，可选项：主机和子网。 “主机”指设定 SNMP Manager 为一台主机；“子网”指设定 SNMP Manager 为一个子网，该子网内的主机都可以配置为 SNMP 管理主机。 说明： 1）当管理主机只有一个时，添加“主机”类型的管理主机对象； 2）当管理主机具有多个且正好位于一个子网时，可以添加多个“主机”类型的管理主机对象，也可以添加一个“子网”类型的管理主机对象。
子网 IP/子网 IP	管理主机类型选择“主机”时，用于指定 SNMP 管理主机对象的 IP 地址；管理主机类型选择“子网”时，用于指定 SNMP 管理子网对象的子网地址及其掩码。
Community	必选项，指定 SNMP 管理主机访问 TopWAF 时的团体名。 说明： SNMPv1 和 SNMPv2c 的管理主机与设备使用团体名认证，管理主机

参数	说明
	端配置的团体名必须此处设置的团体名一致，否则，网络管理员不能通过管理主机管理该 TopWAF。

步骤3 点击【确定】按钮完成管理主机对象的添加。

CLI 方式

system snmp managehost add name <*nstring*> **hostip** <*ip*> **community** <*mstring*>

命令描述：

增加 SNMP 管理主机对象。

参数说明：

参数	说明
name <*nstring*>	必选项，指定 SNMP 管理主机对象的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
hostip <*ip*>	必选项，指定 SNMP 管理主机对象的 IP 地址。 Ipv4 地址类型，格式为 A.B.C.D，可输入 0 或 0.0.0.0 或 255.255.255.255。
community <*mstring*>	必选项，指定 SNMP 管理主机访问 TopWAF 时的团体名。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： SNMP V1/V2 支持团体名认证方案，与 TopWAF 认可的团体名不符的 SNMP 报文将被丢弃。

命令示例：

新增一个名称为 abc，IP 地址为 192.168.10.11，团体名为 public 的 SNMP 管理主机。

TopsecOS# **system snmp managehost add name** *abc* **hostip** *192.168.10.11* **community** *public*

system snmp managehost delete name <*string*>

命令描述：

删除 SNMP 管理主机。

参数说明：

参数	说明
name <*string*>	必选项，指定待删除 SNMP 管理主机对象的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。

命令示例：

删除名称为“manage_host1”的 SNMP 管理主机对象。

TopsecOS# **system snmp managehost delete name** *manage_host1*

system snmp managehost show <cr>

命令描述：

显示所有的 SNMP 管理主机对象。

命令示例：

TopsecOS# **system snmp managehost show**

system snmp managehost clean <cr>

命令描述：

清空所有的 SNMP 管理主机对象。

命令示例：

TopsecOS# **system snmp managehost clean**

system snmp managesubnet add name <*nstring*> **subnet** <*string*> **community** <*mstring*>

命令描述：

增加 SNMP 管理子网对象。

参数说明：

参数	说明
name <*nstring*>	必选项，指定 SNMP 管理子网对象的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
subnet <*string*>	必选项，指定 SNMP 管理子网对象的地址。 字符串类型，格式为 A.B.C.D/E。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
community <*mstring*>	必选项，指定 SNMP 管理子网访问 TopWAF 时的团体名。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： SNMP V1/V2 支持团体名认证方案，与 TopWAF 认可的团体名不符的 SNMP 报文将被丢弃。

命令示例：

增加一个名称为 manage_subnet1，子网地址为 192.168.83.0，子网掩码为 255.255.255.0，团体名为“community2”的 SNMP 管理子网对象。

TopsecOS# **system snmp managehost add name** *manage_subnet1* **subnet** *192.168.83.0/24* **community** *community2*

system snmp managesubnet delete name <*nstring*>

命令描述：

删除 SNMP 管理子网对象。

参数说明：

参数	说明
name <*nstring*>	必选项，指定需要删除 SNMP 管理子网对象的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。

命令示例：

删除名称为“manage_subnet1”的 SNMP 管理子网对象。

TopsecOS# **system snmp managesubnet delete name** *manage_subnet1*

system snmp managesubnet show <cr>

命令描述：

显示所有的 SNMP 管理子网对象。

命令示例：

TopsecOS#**system snmp managesubnet show**

system snmp managesubnet clean <cr>

命令描述：

清空所有的 SNMP 管理子网对象。

命令示例：

TopsecOS# **system snmp managesubnet clean**

8.1.5.3 SNMP 陷阱主机

陷阱主机是指接收 TopWAF 发出 SNMP Trap 消息或 SNMP 报警消息的主机，但根据其使用的 SNMP 版本不同，可接收的消息类型有所不同，SNMPv1 和 SNMPv3 的陷阱主机只支持接收 Trap 消息，只有 SNMPv2c 的陷阱主机可同时接收 Trap 消息和 SNMP 报警消息。TopWAF 主动向陷阱主机发送 Trap 消息及报警消息如下所示。

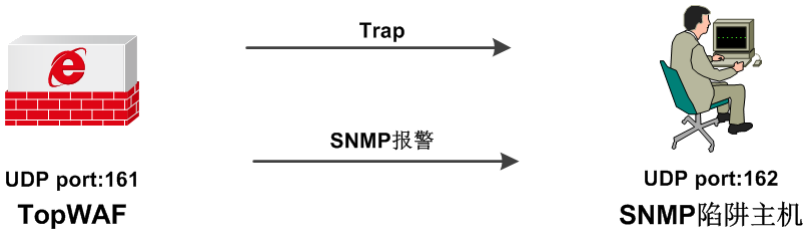


图 8-6 TopWAF 向陷阱主机主动发送 Trap 或报警信息示意图

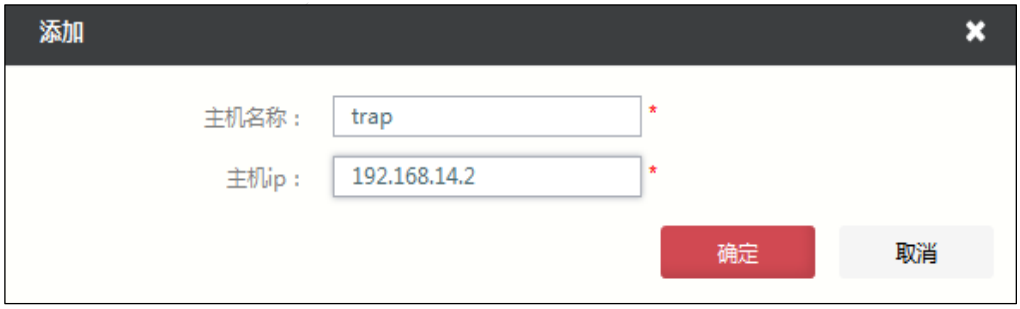
- Trap 消息：TopWAF 主动发送给陷阱主机表明系统出现异常的信息，以提醒网络管理员设备已出现异常。
- 报警消息：通过设备的流量触发报警规则时，TopWAF 自动以 SNMP 报警方式向陷阱主机发送报警信息。

陷阱主机安装 SNMP 管理软件并导入了公有 MIB 库或 TOPSEC MIB 库后，还需要在 TopWAF 上添加陷阱主机信息，网络管理员才可接收 TopWAF 主动发送的 Trap 消息及 SNMP 报警消息，下面介绍如何在 TopWAF 上添加陷阱主机。

WEBUI 方式

步骤1 选择 **系统管理** > **系统设置** > **SNMP**。

步骤2 激活“SNMP 陷阱主机”页签，点击『添加』，如下图所示。



步骤3 配置陷阱主机的名称和 IP 地址。

步骤4 点击【确定】按钮完成陷阱主机对象的添加。

CLI 方式

system snmp traphost add name <*nstring*> **hostip** <*ip*>

命令描述：

增加 SNMP 陷阱主机对象。

参数说明：

参数	说明
name <*nstring*>	必选项，指定需要增加的陷阱主机对象的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
hostip <*ip*>	必选项，指定陷阱主机的 IP 地址。 Ipv4 地址类型，格式为 A.B.C.D。可输入 0 或 0.0.0.0 或 255.255.255.255。

命令示例：

增加一个陷阱主机对象，名称为“trap_host1”，陷阱主机的 IP 地址为“192.168.83.223”。

TopsecOS# **system snmp traphost add name** *trap_host1* **hostip** *192.168.83.223*

system snmp traphost delete name <*nstring*>

命令描述：

删除陷阱主机对象。

参数说明：

参数	说明
name <*nstring*>	必选项，指定需要删除的陷阱主机对象的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。

命令示例：

删除名称为“trap_host1”的陷阱主机对象。

TopsecOS# **system snmp traphost delete name** *trap_host1*

system snmp traphost show <cr>

命令描述：

显示所有的陷阱主机对象。

命令示例：

TopsecOS# **system snmp traphost show**

Name	Host
trap_host1	192.168.83.223

system snmp traphost clean <cr>

命令描述：

清空所有的陷阱主机对象。

命令示例：

TopsecOS# **system snmp traphost clean**

8.1.5.4 SNMPV3 用户

TopWAF 支持 SNMP V3 版本，同时兼容 V1 和 V2 版本。网络管理员使用 SNMP V1、SNMP V2 对 TopWAF 进行查询或配置时，只需在管理主机设置时设置“community”即可，但存在的最大问题是传输的认证和管理数据没有加密、数据的收发缺乏鉴别机制，因此对网络的管理缺乏安全保障。

SNMP V3 版本引入了三个安全级别：1）不需要认证，不提供机密性；2）基于 HMAC-MD5 或 HMAC-SHA 认证，不提供加密；3）不仅提供认证，还提供 CBC-DES 加密算法的加密机制。网络管理员使用 SNMP V3 对 TopWAF 设备进行查询或配置时，不仅可将传送的报文使用 DES 算法进行加密，TopWAF 还通过 SNMPV3 用户的密钥验证网络管理员身份的合法性，因此，进一步提高了对 TopWAF 设备被 SNMP 管理软件管理的安全性。下面介绍如何配置 SNMPv3 用户。

WEBUI 方式

步骤1 选择 **系统管理** > **系统设置** > **SNMP**。

步骤2 激活“SNMPV3 用户”页签，点击『添加』，如下图所示。

在添加 SNMPV3 用户时，各项参数的具体说明如下表所示。

参数	说明
用户名称	必选项，设置网络管理员通过 SNMP 网管软件访问 TopWAF 所使用的用户名。
安全级别	设置是否对 SNMP 认证和管理信息进行加密。可选项：加密，不加密。 说明： 1）当设置加密时，同时使用加密和认证技术，先对数据进行加密，然后进行认证技术的消息摘要计算。 2）设置不加密时，只使用认证技术。
认证密码	必选项，指定管理站通过 SNMPV3 用户账号向 TopWAF 进行身份认证时使用的认证密码。必须为 8 位字符。 说明： 1）TopWAF 支持的 SNMP 认证算法为 MD5。 2）SNMP 认证，可保证只有拥有设备访问权限的用户才可访问该设备。
私有密码	安全级别选择“加密”时，该参数为必选参数。指定消息加密时使用的密码。必须为 8 位字符。 说明： 1）TopWAF 支持的 SNMP 加密算法为 DES。 2）SNMP 加密，使管理主机与被管理设备间的数据以密文方式传输，避免数据被非法用户窃取。

步骤3 点击【确定】按钮完成 SNMPv3 用户的创建。

CLI 方式

system snmp snmpv3user add name <*nstring*> **authpass** <*mstring*> **securitylevel** <authnopriv|authpriv> [**privpass** <*mstring*>]

命令描述：

增加 SNMPV3 用户对象。

参数说明：

参数	说明
name <*nstring*>	必选项，指定需要增加的 SNMPV3 用户对象的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
authpass <*mstring*>	必选项，指定 SNMPV3 用户对象进行认证时使用的密码，加密方式为 MD5。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： 必须为 8 位字符。
securitylevel <authnopriv|authpriv>	必选项，设置安全级别。可选项为：不加密|加密。
privpass <*mstring*>	可选项，在安全级别为加密时，该参数有效。私有密码，指定消息加密时使用的密码，加密方式为 DES。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： 必须为 8 位字符。

命令示例：

增加一个 SNMPV3 用户对象，其中该用户名称为 v3_user1，安全级别为加密，认证密码为 11111111，私有密码为 22222222。

TopsecOS# **system snmp snmpv3user add name** *v3_user1* **authpass** *11111111* **privpass** *22222222* **securitylevel** authpriv

system snmp snmpv3user delete name <*nstring*>

命令描述：

删除 SNMPV3 用户对象。

参数说明：

参数	说明
name	必选项，指定 SNMPV3 用户对象的名称。
nstring	字符串类型，表示要删除的 SNMPV3 用户对象的名称。 说明： 不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。

命令示例：

删除名称为“v3_user1”的 SNMPV3 用户对象。

TopsecOS# **system snmp snmpv3user delete name** *v3_user1*

system snmp snmpv3user show <cr>

命令描述：

显示所有的 SNMPV3 用户对象。

命令示例：

TopsecOS# **system snmp snmpv3user show**

system snmp snmpv3user clean <cr>

命令描述：

清空所有的 SNMPV3 用户对象。

命令示例：

TopsecOS# **system snmp snmpv3user clean**

8.1.6 本机域名解析

TCP/IP 协议使用 IP 地址实现网络的连接和通信，而 IP 地址由点分十进制组成，对用户而言，记住众多网络主机对应的 IP 地址难度非常大。针对此问题，专门设计了域名（一种字符串形式的主机命名机制）以及 DNS（Domain Name System，域名系统），其中，DNS 提供域名与 IP 地址间的查询机制，自动实现域名地址与 IP 地址的映射，用户只需知道某网络服务的域名而无需知道其 IP 地址即可访问该网络服务。

为在 Internet 中通过域名唯一标识某台主机，并为网络服务指定一个有意义的名字，方便用户记忆，域名采用树形结构的命名方案。每个申请 Internet 域名的国家都需向 NIC（Network Information Center，网络信息中心）注册一个顶级域名，NIC 将顶级域名的管理权分配给指定的管理机构，这些管理机构再对其被授权管理的域继续进行划分，以此下去，便形成层次结构的域名体系，域名树形结构如下图所示。

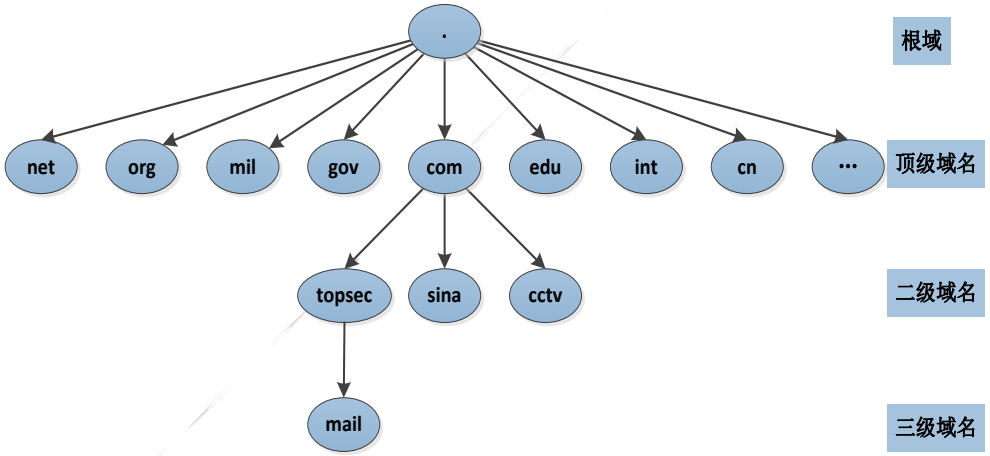


图 8-7 域名层次结构图

域名级别包括根域、顶级域名、二级域名、三级域名等等，不同级别的域名用点号分隔，级别最低的域名写在最左边，级别最高的域名则写在最右边。域名体系的层次结构说明如下：

域名级别	说明
根域	根域用点号（.）表示，以点号结尾的域名为完全合格域名。
顶级域名	包括国际顶级域名和国内顶级域名。 举例： 1）cn：供中国使用；us：供美国使用；jp：供日本使用。 2）net：供网络提供商使用；com：供商业组织使用；edu：供教育机构使用；gov：供政府机构使用；org：供非商业非盈利单位使用；mil：供军事机构使用。

域名级别	说明
二级域名	顶级域名之下的域名。由字母、数字和连接符（-）组成，各级域名之间用实点（.）连接。
……	……

DNS 域名系统采用 C/S 架构，传输层协议为 TCP 或 UDP，服务器端口号 53，DNS 服务器负责域名解析，DNS 客户端提出查询请求。TopWAF 可作为 DNS Client，当其通过域名访问网络资源时，通过向 DNS 服务器发送域名解析请求，获取域名对应的 IP 地址，进而通过 IP 地址访问具体的网络服务。TopWAF 访问 www.topsec.com.cn.时，DNS 域名解析完整过程如下图：

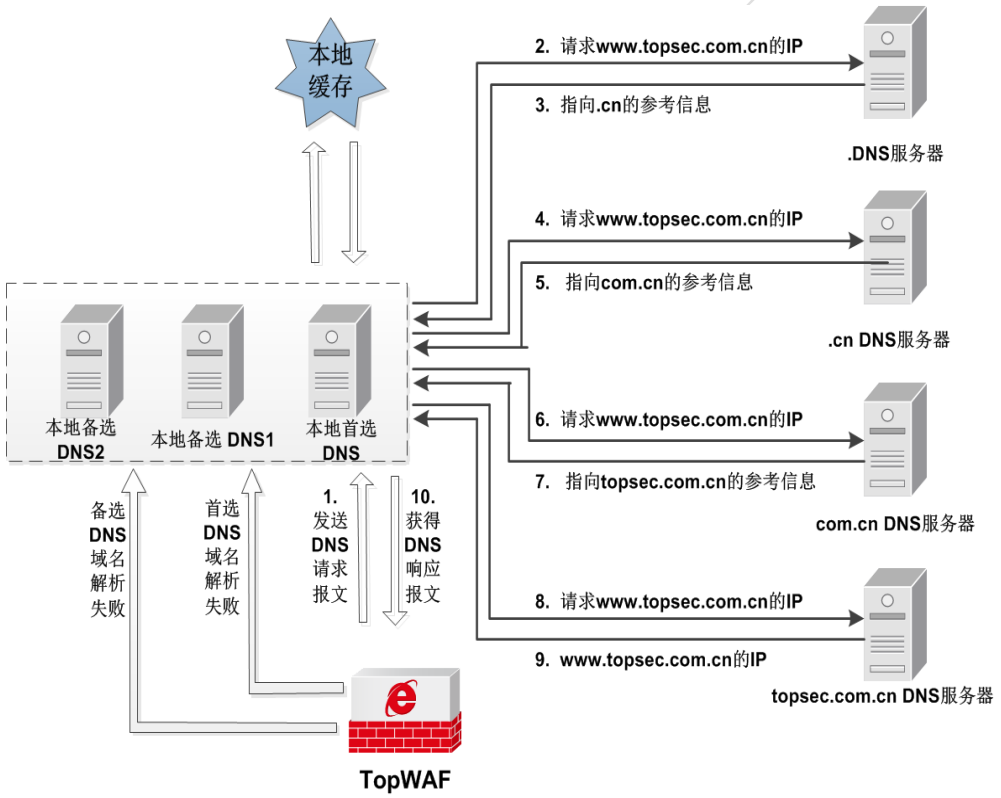


图 8-8 域名解析原理图

TopWAF 首先向本地首选 DNS 服务器发起域名解析请求，如果本地首选 DNS 服务器进行域名解析失败，则向本地备选 DNS 服务器发起域名解析请求。

本地 DNS 服务器接收域名请求后的处理流程如下：

1）本地 DNS 服务器进行域名解析时，首先查询其缓存表，如果查找到域名对应的 IP 地址，本地 DNS 服务器向 TopWAF 返回该域名对应的 IP 地址；否则，向根域服务器发起请求报文。

2）根域服务器查询其映射表项，然后向本地 DNS 服务器返回指向.cn 服务器的 IP 地址；本地 DNS 服务器获取.cn 服务器 IP 地址后，向.cn 服务器发起域名请求。

3）流程同 2）逐级查询，直到查询到最后一个域名服务器 topsec.com.cn，最后一个域名服务器将域名 www.topsec.com.cn 对应的 IP 返回给本地 DNS 服务器。

4）本地 DNS 服务器接收到.topsec.com.cn 服务器解析成功的响应报文，将域名与 IP 地址的映射关系缓存至本地，并将域名解析结果发送给 TopWAF。

下面介绍 TopWAF 作为 DNS 客户端时，如何配置其本地 DNS 服务器。

WEBUI 方式

步骤1 选择 **系统管理** > **系统设置** > **本机域名解析**，如下图所示。

步骤2 配置 DNS 服务器。在“首选 DNS 服务器”文本框中输入优先级最高的 DNS 服务器的 IP 地址；如果有备用的 DNS 服务器，则在“备选 DNS1”/“备选 DNS2”文本框中输入其 IP 地址。

步骤3 点击【应用】按钮完成 DNS 服务器的配置；点击【重置】按钮则恢复系统出厂配置。

✧ TopWAF 支持 IPv4 和 IPv6 域名服务器。

CLI 方式

network dns set dns1 <*hostip*|*ip6*> [**dns2** < *hostip*|*ip6*>] [**dns3** < *hostip*|*ip6*>]

命令描述：

设置域名服务器的地址，最多可设三个 DNS 服务器。

参数说明：

参数	说明
dns1 <*hostip*|*ip6*>	必选项，设置主域名服务器的地址。 hostip：IPv4 主机地址类型，格式：A.B.C.D。第一域值不能是 0、127 或大于 233 的整数，只输入 0 也是非法的。例如：0.12.1.1、127.0.0.1、224.1.1.1 和 0 都是不合法的。 ip6：IPv6 地址类型，没有掩码。
dns2 <*hostip*|*ip6*>	可选项，设置第二备用域名服务器的地址。 hostip：IPv4 主机地址类型，格式：A.B.C.D。第一域值不能是 0、127 或大于 233 的整数，只输入 0 也是非法的。例如：0.12.1.1、127.0.0.1、224.1.1.1 和 0 都是不合法的。 ip6：IPv6 地址类型，没有掩码。
dns3 <*hostip*|*ip6*>	可选项，设置第三备用域名服务器的地址。 hostip：IPv4 主机地址类型，格式：A.B.C.D。第一域值不能是 0、127 或大于 233 的整数，只输入 0 也是非法的。例如：0.12.1.1、127.0.0.1、224.1.1.1 和 0 都是不合法的。 ip6：IPv6 地址类型，没有掩码。

使用说明：

DNS 服务器设置多个时，当主 DNS 服务器失效时，采用第二备用域名服务器，当前两个域名服务器均失效时采用第三备用域名服务器。

network dns reset <cr>

命令描述：

重启 DNS 客户端服务。

network dns show <cr>

命令描述：

查看域名服务器的设置。

命令示例：

TopsecOS# **network dns show**

network dns set dns1 114.114.114.114 dns2 8.8.8.8

8.2 系统维护

TopWAF 为管理员提供了排除系统故障、优化系统性能的功能，包括：配置维护、固件升级、获取健康记录、系统重启、规则库升级、许可证升级、数据库维护和资源监控。

8.2.1 配置维护

TopWAF 的配置信息保存在配置文件中，设备中可同时存在多个配置文件，但是只有一个生效，设备中存在以下配置信息。

- 出厂配置：设备在出厂时，带有基本功能的配置信息。配置文件损坏时，可使用出厂配置正常启动。
- 启动配置：设备在启动时，自动加载的配置文件，如果设备未找到启动配置文件加载出厂配置。
- 当前配置：设备当前正在运行的配置，包括设备的启动配置及管理员新增的配置信息。如果不保存当前配置，设备重启后，会丢失当前配置。

系统支持配置文件的备份、替换和删除等功能，可大大降低管理员批量配置设备的工作量。另外，管理员可通过导入不同配置文件实现设备在不同网络中的配置，自由切换 TopWAF 在网络环境中的功能，并可在设备配置出现问题时帮助管理员轻松将配置恢复到正常状态。

WEBUI 方式

步骤1 选择 **系统管理** > **系统维护** > **配置维护**。

界面中状态栏中图标为“”，表示配置文件是系统当前的运行配置文件；“”表示该配置文件是存储到系统中的备份配置文件。

步骤2 保存配置文件。

点击『保存』，在弹出的确认窗口中，点击【确定】按钮即可将系统中的配置文件保存。

步骤3 备份系统运行配置文件。

点击『另存为』，弹出“配置文件另存为”窗口。输入另存的配置文件文件名和描述信息，点击【确定】按钮即可将系统当前运行配置文件备份到设备中。

步骤4 导出配置文件。

选择系统中存储的配置文件，点击『导出』，在弹出的窗口中，点击【确定】按钮，可将系统中存储的配置文件导出至管理主机中。

步骤5 导入配置文件。

1）点击『导入』，弹出“导入配置文件”窗口。

在导入配置文件时 ，各项参数的具体说明如下表所示。

参数	说明
文件	选择配置文件。点击【选择文件】按钮，在管理主机中选择配置文件。
描述	输入配置文件的必要描述信息。
替换当前的系统配置	如果勾选“替换当前的系统配置”该项表示将该导入的配置文件作为系统的运行配置文件。

2）点击【确定】按钮完成配置文件的导入，点击【取消】按钮撤销本次操作。

步骤6 替换配置文件。

选择一个备份的配置文件，点击其状态栏中的“”，选择的配置将替换为系统当前运行配置文件，配置文件的状态图标转变为“”，表示替换完成。

步骤7 删除备份配置文件。

选择备份的配置文件，点击『删除』，在弹出的提示窗口中，点击【确定】按钮，完成备份配置文件的删除。

✧ 配置文件显示为“”时，不可进行删除操作。

步骤8 恢复设备出厂配置。

点击『恢复默认』，在弹出的提示窗口中，点击【确定】按钮，恢复出厂设置。

CLI 方式

system config reset <cr>

命令描述：

恢复设备的配置文件为出厂设置。

使用说明：

恢复出厂设置会删除设备的配置信息，在恢复出厂设置前，请先导出必要的配置信息。

恢复出厂设置会造成网络中断，请谨慎操作。

system config_file delete <*nstring*>

命令描述：

删除未被使用的系统配置维护文件。

使用说明：

删除系统配置维护文件时，如果文件前显示为“*”，表示该文件当前正在被使用，如果文件前显示为“-”，表示该文件当前没有被使用。

命令示例：

TopsecOS# **system config_file show**

FLAG FILE_NAME SIZE ADMIN_NAME VERSION SAVE_TIME COMMENT

\- config 20010 superman v3.1130.0029.1_topwaf_upt 2014-10-22 07:05:45 default config

* 20151022 24701 superman v3.1130.0032.1_topwaf_upt 2014-11-03 07:02:02 waf

TopsecOS# **system config_file delete** *file2*

```
delete config success!!
TopsecOS# system config_file show
FLAG    FILE_NAME    SIZE    ADMIN_NAME    VERSION    SAVE_TIME    COMMENT
*       20151022     24701   superman      v3.1130.0032.1_topwaf_upt
2014-11-03 07:02:02  waf
```

system config_file load <*nstring*>

命令描述：

下载系统配置维护文件。

参数说明：

参数	说明
load <*nstring*>	字符串类型，系统配置维护文件的名称。 说明： 不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。

命令示例：

```
TopsecOS# system config_file load file1
load config success!!
```

system config_file save_as <*nstring*> [**comment** <*wstring*>]

命令描述：

保存系统配置维护文件。

参数说明：

参数	说明
save_as <*nstring*>	必选项，系统配置维护文件的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
comment <*wstring*>	可选项。设置对该系统配置维护文件的说明。 字符串类型，不包含“<>\\”中任意字符。

命令示例：

TopsecOS # **system config_file save_as** *file1* **comment** *firstfile*

config save as success!

system config_file show <cr>

命令描述：

显示系统配置文件。其中“*”表示当前正在使用的配置文件，“-”表示存储在设备中的备份配置文件。

命令示例：

TopsecOS # **system config_file show**

FLAG FILE_NAME SIZE ADMIN_NAME VERSION SAVE_TIME COMMENT

- config 11049 superman v3.1130.0029.1_topwaf_upt 2015-04-07 15:18:10 default config

* waf-20150120XH9-0319 445741 superman v3.1130.0032.1_topwaf_upt 2015-04-28 12:58:20 waf

8.2.2 固件维护

TopWAF 支持基于 TFTP 服务器、FTP 服务器和本地方式升级设备的系统软件，并支持将升级包备份到设备中，在设备需要升级时进行升级，可方便管理员根据天融信发布的升级包及时对设备的性能和功能进行扩充。系统软件升级前将会首先检查升级包与设备的硬件平台是否匹配，如果不匹配，系统会提示管理员不能进行升级操作。

TFTP 和 FTP 服务器方式通过下载远程服务器的升级包进行升级，而本地方式则通过管理主机中的升级包进行升级，即采用本地方式升级前，需将升级包下载到管理主机中，下面分别予以详细介绍。

在固件维护之前，需要先进行如下步骤：

- 建议管理员在升级前先保存系统的配置。
- 通过本地进行升级时，请尽量退出串口登录。
- 通过 TFTP/FTP 进行升级时，在升级之前需要事先配置好 TFTP/FTP 服务器及其工作目录，并保证升级文件存放在工作目录中。
- 通过 TFTP/FTP 进行升级时，确保 TFTP/FTP 服务器和设备之间有路由可达。

WEBUI 方式

步骤1 选择 **系统管理** > **系统维护** > **固件维护**。

界面中状态栏中图标为“ ”，表示当前运行的系统软件；“ ”表示存储到系统中的备份系统软件。

步骤2 升级系统软件。

➢ TFTP 升级方式

点击『导入』，弹出“导入”窗口，在“升级方式”下拉框中选择“TFTP”。

在采用 TFTP 方式升级固件时，各项参数的具体说明如下表所示。

参数	说明
服务器地址	必选项。输入存放升级包的 TFTP 服务器的 IP 地址。
文件名称	必选项。输入升级包的名称。
描述	输入简单的描述信息。
替换当前的系统固件	勾选“替换当前的系统固件”，TopWAF 会升级固件；否则，TopWAF 并不升级固件，只是将 TFTP 服务器中相应的升级包下载到设备中进行备份。

➢ FTP 服务器方式

点击『导入』，弹出“导入”窗口，在“升级方式”下拉框中选择“FTP”。

在采用 FTP 方式升级固件时，各项参数的具体说明如下表所示。

参数	说明
服务器地址	必选项。输入存放升级包的 FTP 服务器的 IP 地址。
文件名称	必选项。输入升级包的名称。
用户名	FTP 服务器不支持匿名登录时为必选项。输入 FTP 服务器的合法登录账号名称。
密码	FTP 服务器不支持匿名登录时为必选项。输入 FTP 服务器的合法登录

参数	说明
	账号名称对应的密码。
描述	输入简单的描述信息。
替换当前的系统固件	勾选“替换当前的系统固件”，TopWAF 会升级固件；否则，TopWAF 并不升级固件，只是将 FTP 服务器中相应的升级包下载到设备中进行备份。

➢ 本地方式

点击『导入』，弹出“导入”窗口，在“升级方式”下拉框中选择“本地”。

在采用本地方式升级固件时，各项参数的具体说明如下表所示。

参数	说明
描述	输入简单的描述信息。
文件名称	点击【选择文件】按钮，选择管理主机中存放的升级包，然后点击【确定】按钮导入升级包。
替换当前的系统固件	勾选“替换当前的系统固件”，TopWAF 会升级固件；否则，TopWAF 并不升级固件，只是将管理主机中相应的升级包下载到设备中进行备份。

步骤3 升级方式设置完成后，点击【确定】按钮，完成升级包的导入或系统升级，点击【取消】按钮撤销本次操作。

✧ 远程升级时，建议利用 FTP 或 TFTP 服务器进行升级，最好不要选择 WEBUI 方式升级。

✧ 升级系统软件需要一定的时间，升级过程中，请耐心等待，不要在界面中进行任何操作，否则升级可能中断。如系统长时间显示“正在升级，请稍等”窗口，则表明升级不成功，请点击【确定】按钮返回。升级不成功，请重点考虑和检查以下几方面的原因：

1）是否正确配置了 TFTP/FTP 服务器；

2）是否输入了正确的文件名称或选择了正确的升级包。

CLI 方式

system firmware clean <cr>

命令描述：

清空所有未使用的升级文件。

命令示例：

TopsecOS# **system firmware clean**

system firmware delete filename <*string*>

命令描述：

删除指定的未使用升级文件。

命令示例：

TopsecOS# **system firmware delete filename** *topwaf-v1.0.23.2-default_upt*

system firmware import filename <*string*> **get-method** <ftp|tftp> [**ftp-user** <*string*>]

[**ftp-password** <*string*>] **serverip** <*ip*> [**comments** <*string*>]

命令描述：

将升级包导入 TopWAF 系统。该条命令用于非即时升级的情况。此时系统升级在执行该命令后，还需执行 **system firmware load** 加载命令。

参数说明：

参数	说明
filename <*string*>	必选项。升级包文件名。 字符串类型，字符串长度为 1-64 位。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
get-method <ftp|tftp>	必选项。选择对系统进行升级的方式。可选项为：通过 FTP 升级|通过 TFTP 升级
serverip <*ip*>	必选项。远端存放升级包的服务器 IPv4 地址。 IPv4 地址类型，格式为 A.B.C.D。
ftp-user <*string*>	可选项。FTP 服务器上的用户名。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。 说明： 当采用 FTP 方式升级时，该参数才需要填写。
ftp-password <*string*>	可选项。FTP 服务器上的用户密码，与 FTP 用户名对应。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包

参数	说明
	含空格。 说明： 当采用 FTP 方式升级时，该参数才需要填写。
comments <*string*>	可选项。对升级包的说明描述。 字符串类型，长度为 1-256 位。不包含“$\"\\'%<>”中任意字符，也不能包含空格。

命令示例：

TopsecOS# **system firmware import filename** *topwaf-v1.0.23.2-default_upt* **getmethod** *ftp* **serverip** *192.168.91.99* **ftp-user** *superman* **ftp-password** *123456* **comments** *updatefile*

.....

Data pacakge become effective, The device must reboot.

system reboot.....

system firmware load filename <*string*> [**sysdisk** <normal>]

命令描述：

根据文件名加载 TopWAF 设备上的升级包。

参数说明：

参数	说明
filename <*string*>	必选项。升级包文件名。 字符串类型，字符串长度为 1-64 位。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
sysdisk <normal>	可选项，设置升级的系统，可选项为主系统。

命令示例：

TopsecOS# **system firmware load filename** *topwaf-v1.0.23.2-default_upt*

system firmware show <cr>

命令描述：

显示升级包的信息。

命令示例：

TopsecOS# **system firmware show**

system firmware update filename <*string*> **get-method** <ftp|tftp> **serverip** <*ip*> [**ftp-user** <*string*>] [**ftp-password** <*string*>] [**sysdisk** <normal>] [**comments** <*string*>]

命令描述：

设置升级系统软件。该条命令用于即时升级系统的情况。此时系统升级只需执行该命令即可。

参数说明：

参数	说明
filename <*string*>	必选项。升级包文件名。 字符串类型，字符串长度：1-64。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
get-method <ftp|tftp>	必选项。选择对系统进行升级的方式。可选项为：通过 FTP 升级|通过 TFTP 升级。
serverip <*ip*>	必选项。远端存放升级包的服务器 IPv4 地址。 IPv4 地址类型，格式为 A.B.C.D。可输入 0 或 0.0.0.0 或 255.255.255.255。
ftp-user <*string*>	可选项，FTP 服务器上的用户名。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。 说明： 当采用 FTP 方式升级时，该参数才需要填写。
ftp-password <*string*>	可选项，FTP 服务器上的用户密码，与 FTP 用户名对应。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。 说明： 当采用 FTP 方式升级时，该参数才需要填写。
sysdisk <normal>	必选项，选择升级的系统，可选项为主系统。
comments <*string*>	可选项，对升级包的说明描述。 字符串类型，长度：1-256。不包含“$\"\\'%<>”中任意字符，也不能包含空格。

使用说明：

升级过程需要几分钟，请耐心等待。避免对 TopWAF 平台进行任何操作。

命令示例：

TopsecOS# **system firmware update filename** *topwaf-v1.0.23.2-default_upt* **getmethod** *tftp* **serverip** *192.168.1.4* **comments** *updatefile*

8.2.3 健康记录

管理员可以定期备份健康记录并获取历史健康记录，包括设备的配置信息，运行状态等信息，以便当设备出现异常时，可以帮助天融信的技术支持人员快速地定位并解决故障。

WEBUI 方式

步骤1 选择 **系统管理** > **系统维护** > **健康记录**，如下图所示。

在设置定期备份功能时，各项参数的具体说明如下表所示。

参数	说明
启用状态	设置是否启用定期备份功能。
周期	设置定期备份健康记录的周期，可选项为每日、每周。
星期集合	周期设置为“每周”时，该参数才生效，指定每周的周几生成健康记录。
生成时间	设置定期备份健康记录的时间，输入格式为：XX：XX，支持 00:00 至 23:59 的任意时间。
最大保存记录数	设置保存的备份健康记录的数量。取值范围为 5-20。

步骤2 参数设置完成后，点击【应用】按钮保存配置。

步骤3 点击『立即生成』或『下载』可就将健康记录下载到管理主机。

✧ 健康记录已加密，仅供调试人员使用。

8.2.4 系统重启

当系统升级、设备工作不正常或部分新配置需要生效时，需对系统进行重启，管理员可以远程重启系统。

✧ 重启前应保存系统的配置信息，否则，重启后将丢失全部未保存的配置。

✧ 系统重启将会造成业务中断，请谨慎使用。

✧ 系统重启后，管理员需要重新登录。

WEBUI 方式

步骤1 选择 **系统管理** > **系统维护** > **系统重启**。如下图所示。

步骤2 点击【重启系统】按钮，在弹出的窗口中，选择是否保存当前配置信息，点击【确定】按钮保存；点击【取消】按钮放弃保存。

步骤3 在弹出的窗口中，点击【确定】按钮，即可重新启动 TopWAF。

CLI 方式

system reboot <cr>

命令描述：

重新启动 TopWAF 设备。

命令示例：

```
TopsecOS# system reboot
Save system config?[y/n]:y
system config save.....
save config success.
Reboot system [y/n]:y
reboot.....
```

8.2.5 规则库升级

当前网络中入侵手段、病毒类型和应用类型的复杂多变，用户对设备的识别效率和识别能力的需求也在随之增强。为了使设备可以及时的识别新的应用，防御新的攻击和病毒，设备需要及时升级规则文件。

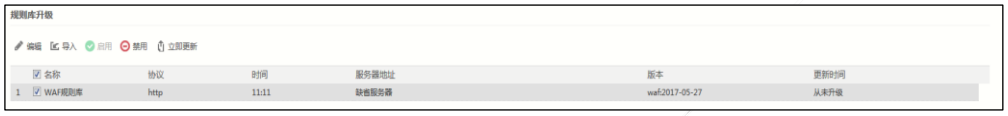
规则库升级功能可以升级规则库，可以提高设备对入侵行为、病毒和应用的识别能力和识别效率。升级规则文件有：自动升级、立即升级和本地升级 3 种方式。管理员可以根据需要选择合适的升级方式。

- 自动升级：自动升级指设备根据管理员设置的时间和目的地址，定期从目的地址处自动下载并更新规则库。

- 立即升级：当管理员发现网络上出现新的攻击方式、病毒或应用，升级中心已发布新的规则库，而此时未到设备的自动升级时间，可立即升级操作，及时升级规则库。立即升级方式与自动升级使用相同的规则库下载地址。
- 本地升级：当 TopWAF 与 Internet 物理隔离，且没有部署升级服务器时，可以采用本地升级方式。升级前将需要升级的规则文件保存到管理主机，再通过 WebUI 登录到 TopWAF 设备，进行选择规则文件进行升级。

WEBUI 方式

步骤1 选择 **系统管理** > **系统维护** > **规则库升级**。



步骤2 自动升级规则库。

1）点击『编辑』，在弹出的“编辑”对话框中，配置自动更新策略。

在配置自动升级规则库时，各项参数的具体说明如下表所示。

参数	说明
名称	显示自动更新规则名称。
服务器	设置规则文件升级的服务器类型。可选项：默认和自定义。 服务器设置为“默认”时，规则库升级服务器地址为“waf.topsec.com.cn”，更新周期为“每周三”。
更新时间	配置自动更新的时间间隔。可选择的更新间隔有：每月、每周、每日和每

参数	说明
	时。并可通过更新间隔下方的参数详细配置更新时间。
服务器地址	设置服务器为自定义时，该项可配置。配置自动更新获取规则文件的服务器地址。 HTTP 方式升级时，服务器地址为字符串类型，最大长度为 63 个字符，支持多个升级服务器地址，可点击右侧『＋』输入多个地址，最多支持 5 个服务器地址。格式为：域名形式或点分十进制形式 X.X.X.X。 FTP 方式升级时字符串类型，最大长度为 63 个字符，支持多个服务器地址，可点击右侧『＋』输入多个地址，最多支持 5 个服务器地址。格式为：域名形式或点分十进制形式 X.X.X.X。 说明： 服务器的地址仅需添加域名或者 IP 地址即可，无需添加“http://”或者“ftp://”，TopWAF 会根据设置的升级方式，自动添加“http://”或者“ftp://”。

2）设置完成后，点击【确定】按钮保存配置，点击『启用』，开启自动升级规则功能，完成自动更新策略配置。点击『立即更新』可立即同步服务器上的规则库文件。

步骤3 本地导入规则库文件。

1）选择规则文件所在行，点击『导入』，弹出“规则文件导入”窗口。

在配置手动更新规则文件时，各项参数的具体说明如下表所示。

参数	说明
名称	显示规则文件名称。
文件名称	点击【选择文件】按钮，选择管理主机上保存的规则文件。

2）参数配置完成后，点击【确定】按钮，完成规则文件升级。

CLI 方式

system rules-update enable waf <cr>

命令描述：

开启规则文件自动升级功能。

可使用 **system rules-update disable waf**<cr>命令关闭规则文件自动升级功能。

system rules-update modify-time waf period-time <*string*>[**period-date** <*string*>|**period-week**

<*num*>]

命令描述：

修改规则文件自动更新策略的更新时间。

参数说明：

参数	说明
period-time <*string*>	自动更新的时间间隔。以每日或者每小时时形式设置。 字符串类型，格式为“小时：分钟”或“分钟”，如 11:12 或 12。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
period-date <*string*>	自动更新的时间间隔。以每月形式设置。 字符串类型，格式为“月-日”或“日”，如 01-01 或者 01。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
period-week <*num*>	自动更新的时间间隔。以每周形式设置。 实数类型，取值范围 0-6，表示星期日-星期六。

system rules-update modify-server waf type ftp serverip <*string*> [**ftpuser** <*string*>] [**ftppass** <*string*>]

命令描述：

修改 FTP 方式升级规则文件的服务器信息。

参数说明：

参数	说明
serverip <*string*>	FTP 服务器 IP 地址。 字符串类型，格式为：域名形式或点分十进制形式 X.X.X.X。
ftpuser <*string*>	FTP 服务器用户名。 字符串类型，长度范围：1-63。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
ftppass <*string*>	FTP 服务器密码。 字符串类型，长度范围：1-63。不包含“$\"\\'%<>”中任意字符，也不能包含空格。

system rules-update modify-server waf type http url <*string*>

命令描述：

修改 HTTP 方式升级规则文件的服务器信息。

参数说明：

参数	说明
url <*string*>	规则库服务器域名。 字符串类型，格式为：域名形式或点分十进制形式 X.X.X.X。不包含“$\"\\'%<>”中任意字符，也不能包含空格。 说明： 最多支持配置5个域名服务器，每个域名的最大长度为63。

system rules-update reset waf <cr>

命令描述：

恢复规则文件升级为出厂配置。TopWAF 出厂时，规则库升级服务器地址为 http://waf.topsec.com.cn，更新周期为“每周三”。

system rules-update show <cr>

命令描述：

查看自动更新策略配置信息。

命令示例：

TopsecOS# **system rules-update show**

Module	UpdateWay	State	Time	Server	User:Passwd
topwaf	http	enable	Wed 01:21	waf.topsec.com.cn	

system rules-update update waf <cr>

命令描述：

立即更新规则库。

配置立即更新规则库前，需要先开启规则文件自动升级功能。

system rules-update version <cr>

命令描述：

查看规则文件版本信息。

命令示例：

TopsecOS# **system rules-update version**

Module	Version	Expire	UpdateTime	RulesNum
topwaf	2016-12-29	2020.12.31	2017-04-28 10:53	688

8.2.6 license 授权

license 用来管理和控制天融信 TopWAF 的部分功能以及服务的使用。对于非所有管理员都有权涉及的受限制模块，license 可授予相关权限。通过 license 授权可修改产品的功能开启状态。客户通过设备码购买相应的授权码，将授权码写入设备进行注册，激活相应的功能。

WEBUI 方式

步骤1 选择 **系统管理** > **系统维护** > **license 授权**，如下图所示。

license 信息中显示了用户信息、开始日期、结束日志及当前 license 的状态，状态包含了未注册、已注册、已过期。

设备码是每台设备都具有的唯一的识别码，根据设备码可以获取到唯一的授权码。

步骤2 输入授权码。

在授权码输入框中输入获取到的授权码。

步骤3 设置完成后，点击【应用】按钮，完成 license 授权。

如果授权码错误将会弹出错误提示信息，若 license 授权成功则会自动重启设备。

8.2.7 数据库维护

数据库维护功能主要是针对系统的日志数据库进行管理和维护。通过选择不同的日志类型，可以导入并查看相应类型的日志，及时查找发现问题。同时可以给日志服务器设置阈值，方便及时清理日志服务器，以免服务器负载过重。

WEBUI 方式

步骤1 选择 **系统管理** > **系统维护** > **数据库维护**，如下图所示。

设置数据库维护策略时，各项参数的具体说明如下表所示。

参数	说明
日志类型	设置日志类型。在下拉列表里选择所要查看的日志类型。

参数	说明
	可选项：流量日志、攻击日志、防篡改日志、DDOS 攻击日志、系统日志、管理员登录日志、调试日志。
导入文件	选择本地存放所选日志的文件，上传至系统数据库。
邮件标题	设置报警邮件标题。当日志数据库达到上限报警时，系统会给用户发送报警邮件。范围：1-127 字符。
邮件策略	设置邮件策略。在下拉列表里选择已有的邮件策略或者选择新建邮件策略。新建邮件策略具体请参见 5.5 邮件策略。
日志告警上限	设置日志告警上限值。单位为：%，取值范围：5-90。

步骤2 设置完成后，点击【应用】按钮，完成数据库维护策略配置。

CLI 方式

system database set mail-policy <*mstring*> **[subject** <*mstring*>**] [percent** <*num*>]

命令描述：

设置 WAF 数据库告警邮件配置。

参数说明：

参数	说明
mail-policy <*mstring*>	可选项。设置邮件策略名。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。
subject <*mstring*>	可选项，设置邮件标题。 字符串类型，长度范围：1-127。不以“\\”结尾且不包含“<script>”字符串。
percent <*num*>	设置告警阈值百分比。 实数类型，长度范围：5-90。

system database show <cr>

命令描述：

显示 WAF 数据库告警邮件配置。

命令示例：

TopsecOS# **system database show**

waf database set mail-policy 123 subject 'alarm' percent 80

system database show [**log_max_count** <*cr*>]

命令描述：

显示各种类型日志的条数上限。

命令示例：

TopsecOS# **system database show log_max_count**

system database show log_max_count

traffic_table: 1000000

audit_table: 1000000

ads_attack: 400000

error_table: 200000

tamper_table: 200000

mgmt_table: 10000

8.2.8 资源监控

管理员通过资源监控功能可以设置 cpu 占用率阈值、内存占用率阈值和磁盘占用率阈值，若其超过所设定的阈值，在设备状态信息的折线图中会显示橙色或红色。查看设备信息折线统计图具体请参见 4.2.4 设备状态。

WEBUI 方式

步骤1 选择 **系统管理** > **系统维护** > **资源监控**，如下图所示。

在配置资源监控时，各项参数的具体说明如下表所示。

参数	说明
cpu 占用率阈值	设置 cpu 占用率阈值。单位为：%，取值范围：0-100。 说明：0 表示关闭监控，如输入值为 80，占用率阈值为 80%。
内存占用率阈值	设置内存占用率阈值。单位为：%，取值范围：0-100。 说明：0 表示关闭监控，如输入值为 80，占用率阈值为 80%。
磁盘占用率阈值	设置磁盘占用率阈值。单位为：%，取值范围：0-100。 说明：0 表示关闭监控，如输入值为 80，占用率阈值为 80%。
资源监控开关	设置资源监控开关。可选项：开启、关闭。

步骤2 配置完成后，点击【应用】按钮，完成资源监控配置。

CLI 方式

system monitor config set cpu_ratio_threshold *<num>*

命令描述：

设置 cpu 占用率阈值。

参数说明：

参数	说明
cpu_ratio_threshold *<num>*	必选项，设置 CPU 占用率的阈值。 数值类型，范围 0-100，0 表示关闭监控。

system monitor config set memory _ratio_threshold *<num>*

命令描述：

设置内存占用率阈值。

参数说明：

参数	说明
memory _ratio_threshold *<num>*	必选项，设置内存占用率的阈值。 数值类型，范围 0-100，0 表示关闭监控。

system monitor config set disk_ratio_threshold *<num>*

命令描述：

设置磁盘占用率阈值。

参数说明：

参数	说明
disk_ratio_threshold <*num*>	必选项，设置磁盘占用率的阈值。 数值类型，范围 0-100，0 表示关闭监控。

system monitor config set resource_monitor_switch <start|stop>

命令描述：

设置资源监控的启动与关闭。

参数说明：

参数	说明
resource_monitor_switch <start|stop>	设置资源监控的启动与关闭。

system monitor **reset**<cr>

命令描述：

将资源监控配置恢复出厂设置。

8.3 系统诊断

TopWAF 支持管理员通过诊断工具和抓包工具对网络的连通性进行探测，以更好地了解网络运行状况并进行相关问题的定位。

8.3.1 诊断工具

根据网络传输的原理，TopWAF 分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括 PING、TRACEROUTE、TCP、HTTP 和 DNS。

- PING：探测 TopWAF 到目的主机的网络层是否可达。
- TRACEROUTE：探测 TopWAF 到达目的主机所经过的路由设备。
- TCP：探测 TopWAF 与目标主机建立三次握手所花费的时间，以诊断网络连通状态。

- HTTP：探测 TopWAF 与使用 HTTP 协议的服务器是否可达。
- DNS：探测 DNS 服务器是否能成功解析某域名。

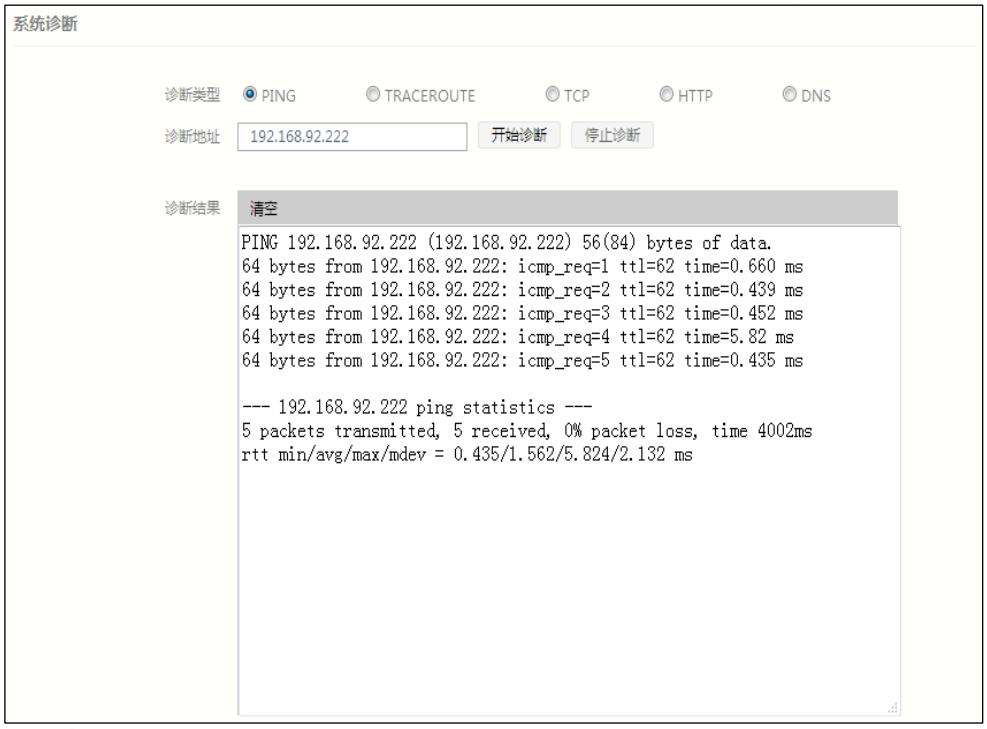
WEBUI 方式

步骤1 选择 **系统管理** > **系统诊断** > **诊断工具**。

步骤2 探测网络连通性主要分为以下三种：

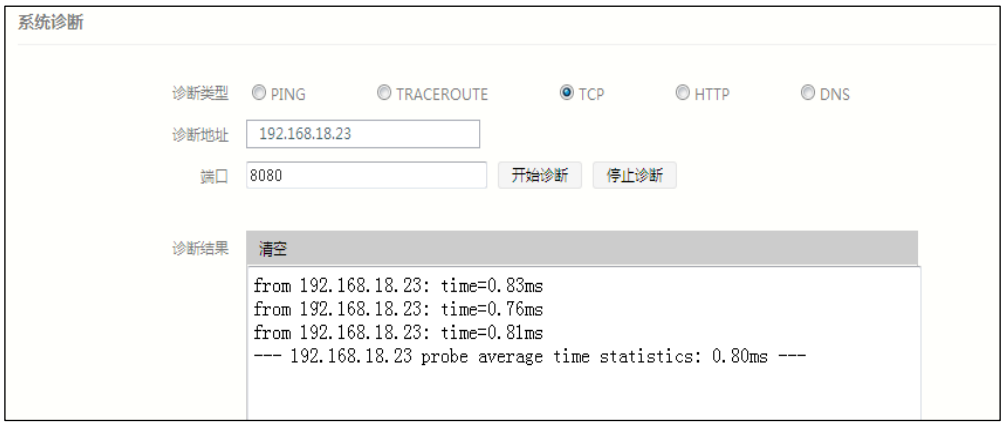
➢ 网络层诊断

选择“PING”或“TRACEROUTE”，然后在“诊断地址”文本框中输入目的 IP 地址，点击【开始诊断】按钮执行目的可达性检测，如下图所示。



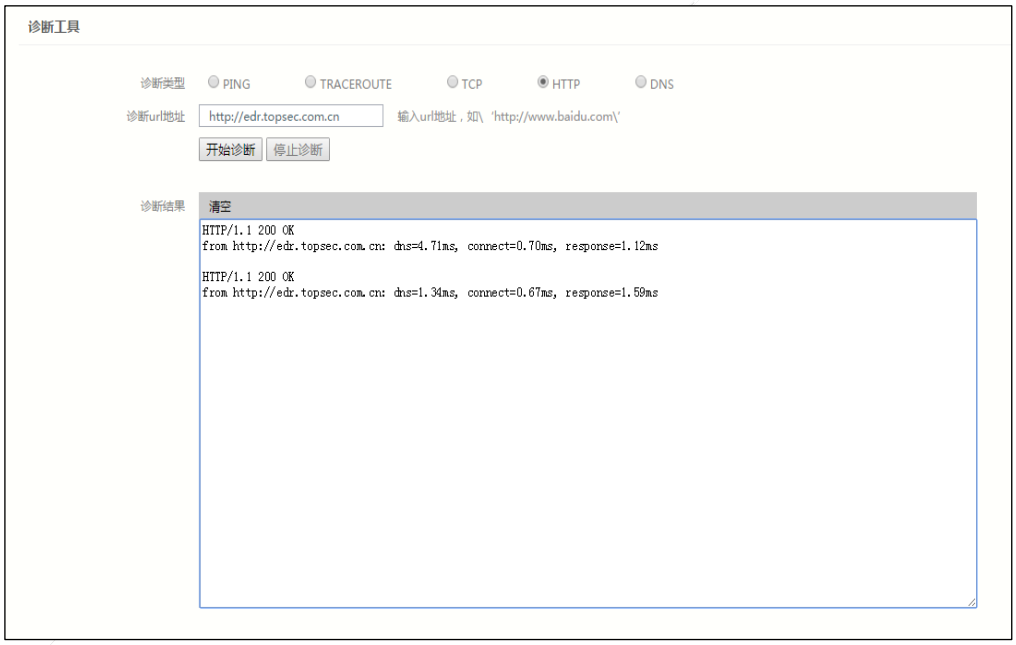
➢ 传输层诊断

选择“TCP”，然后在“诊断地址”文本框中输入目的 IP 地址，“端口”文本框中配置端口号，点击【开始诊断】按钮执行目的可达性检测，如下图所示。



➢ 应用层诊断

选择“HTTP”，在“可用域名”文本框中输入域名，在“端口”文本框中输入端口号，点击【开始诊断】按钮执行目的可达性检测，如下图所示。



步骤3 点击【停止诊断】按钮可以停止命令执行，如点击『清空』可以将命令的执行结果从 WEBUI 界面中删除。（诊断类型为“DNS”时操作类似）

CLI 方式

ping <*string*> [**interface** <*string*>] [**count** <*num*>] [**size** <*num*>]

命令描述：

验证 TopWAF 与 IPv4 主机或网络设备的连接情况。

参数说明：

参数	说明
ping <*string*>	字符串类型，表示 IPv4 地址或者域名。如果为 IPv4 地址字符串，格式为 A.B.C.D。如果为域名，格式为 www.topsec.com.cn。 说明： 不包含“$\"\\'%<>”中任意字符，也不能包含空格。
interface <*string*>	可选项，数据报文传出时通过的接口名称或 IPv4 地址。字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。
count <*num*>	可选项，设定发送 ping 包的次数。 实数类型，单位：次。
size <*num*>	可选项，设定发送 ping 包的字节长度。 实数类型。单位：字节；取值范围：0-65492。

命令示例：

目的 IPv4 地址为 192.168.90.79，出接口 IPv4 地址为 192.168.90.70，数据包大小为 30000 字节，接收包的次数为 100。

TopsecOS# **ping** *192.168.90.79* **interface** *192.168.90.70* **count** *100* **size** *30000*

PING 192.168.90.79(192.168.90.79) 30000(30028) bytes of data

30008 bytes from 192.168.90.79: icmp_req=1 ttl=64 time=0.101 ms

30008 bytes from 192.168.90.79: icmp_req=2 ttl=64 time=0.052 ms

ping6 <*string*> [**interface** <*string*>] [**count** <*num*>] [**size** <*num*>]

命令描述：

验证 TopWAF 与 IPv6 主机或网络设备的连接情况。

参数说明：

参数	说明
ping6 <*string*>	字符串类型，表示 IPv6 地址或者域名。格式为 IPv6 地址字符串或 www.topsec.com.cn。 说明： 不包含“$\"\\'%<>”中任意字符，也不能包含空格。

参数	说明
interface <*string*>	可选项，数据报文传出时通过的接口名称或 IPv6 地址。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。
string2	字符串类型，物理接口名称或 IPv6 地址。 说明： 不包含“$\"\\'%<>”中任意字符，也不能包含空格。
count <*num*>	可选项，设定发送 ping 包的次数。 实数类型，单位：次。
size <*num*>	可选项，设定发送 ping 包的字节长度。 实数类型。单位：字节；取值范围：0-65492。

命令示例：

目的 IPv6 地址为 2200::1。

```
TopsecOS# ping6 2200::1
PING 2200::1(2200::1) 56 data bytes
64 bytes from 2200::1: icmp_seq=1 ttl=64 time=0.059 ms
64 bytes from 2200::1: icmp_seq=2 ttl=64 time=0.100 ms
64 bytes from 2200::1: icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from 2200::1: icmp_seq=4 ttl=64 time=0.067 ms
64 bytes from 2200::1: icmp_seq=5 ttl=64 time=0.045 ms
64 bytes from 2200::1: icmp_seq=6 ttl=64 time=0.037 ms
```

system traceroute <*string*> [**maximum** <*num*>] [**port** <*port*>] [**count** <*num*>] [**wait** <*num*>]

命令描述：

显示路由封包到达目的 IPv4 地址的信息。

参数说明：

参数	说明
traceroute <*string*>	字符串类型，表示目标 IPv4 地址，格式为 A.B.C.D。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
maximum <*num*>	可选项，设置目的可达的最大路由跳数，实数类型。

参数	说明
port <*port*>	可选项，设置 UDP 传输协议的通信端口，取值范围：0-65535。
count <*num*>	可选项，探测包的个数。 实数类型，默认值：3。
wait <*num*>	可选项，设置等待远端主机响应的最大时间，超过该时间还未收到远端主机的响应，则表示该远端主机不可达，实数类型。

命令示例：

目的 IPv4 地址为 192.168.90.70。

TopsecOS# **system traceroute** *192.168.90.70*

traceroute to 192.168.90.70 (192.168.90.70), 30 hops max, 60 byte packets

1 192.168.90.70 (192.168.90.70) 0.353 ms * *

system traceroute6 <*string*> [**maximum** <*num*>] [**port** <*port*>] [**count** <*num*>] [**wait** <*num*>]

命令描述：

显示路由封包到达目的 IPv6 地址的信息。

参数说明：

参数	说明
traceroute6 <*string*>	字符串类型，表示目标 IPv6 地址，格式为 x:x:x:x:x:x:x:x，其中 x 为一个 4 位十六进制整数。不包含“$\"\\'%<>”中任意字符，也不能包含空格。
maximum <*num*>	可选项，设置目的可达的最大路由跳数，实数类型。
port <*port*>	可选项，设置 UDP 传输协议的通信端口。取值范围：0-65536。
count <*num*>	可选项，探测包的个数，实数类型。
wait <*num*>	可选项，设置等待远端主机响应的最大时间，超过该时间还未收到远端主机的响应，则表示该远端主机不可达，实数类型。

命令示例：

目的 IPv6 地址为 2100::1。

TopsecOS# **system traceroute6** 2100::1

traceroute to 2100::1 (2100::1), 30 hops max, 80 byte packets

1 2100::1 (2100::1) 0.031 ms 0.006 ms 0.004 ms

system probe tcp serverip <*ip4ip6*> **port** <*port*> [**count** <*num*>] [**interval** <*num*>]

命令描述：

通过 TCP 协议探测网络状况。

参数说明：

参数	说明
serverip <*ip4ip6*>	必选项，指定目标主机 IP 地址。 Ipv4 或 Ipv6 地址类型，Ipv4 格式为 x.x.x.x，Ipv6 格式不包含掩码。
port <*port*>	必选项，实数类型，设置通信端口。
count <*num*>	可选项，探测包的个数。 实数类型，单位：次；默认值：3。
interval <*num*>	可选项，探测包的间隔。 实数类型，单位：秒；默认值：0。

命令示例：

TopsecOS# **system probe tcp serverip** *192.168.18.23* **port** *8080*

from 192.168.18.23: time=1.29ms

from 192.168.18.23: time=0.77ms

from 192.168.18.23: time=0.84ms

---192.168.18.23 probe average time statistics: 0.97ms ---

system probe http domain <*string*> [**count** <*num*>] [**interval** <*num*>]

命令描述：

通过 http 协议探测网络状况。

参数说明：

参数	说明
domain <*string*>	必选项，指定域名地址。 字符串类型，不能包含“&\”\\’%<>”中任意字符，也不能包含空格。
count <*num*>	可选项，探测包的个数。 实数类型，单位：次；默认值：1。
interval <*num*>	可选项，探测包的间隔。 实数类型，单位：秒；默认值：0。

命令示例：

TopsecOS# **system probe http domain** *http://www.topsec.com.cn*

HTTP/1.1 200 OK

from http://www.topsec.com.cn: dns=2.89ms, connect=3.79ms, response=2.79ms

system probe dns serverip <*ip*> **domain** <*string*> [**count** <*num*>] [**interval** <*num*>]

命令描述：

诊断 DNS 服务器是否可解析某域名。

参数说明：

参数	说明
serverip <*ip*>	必选项，指定域名服务器 IP 地址。 Ipv4 地址类型，可输入 0 或 0.0.0.0 或 255.255.255.255。
domain <*string*>	必选项，指定域名。 字符串类型。不能包含“&\”\\’%<>”中任意字符，也不能包含空格。
count <*num*>	可选项，探测包的个数。 实数类型，单位：次；默认值：3。
interval <*num*>	可选项，探测包的间隔。 实数类型，单位：秒；默认值：0。

命令示例：

探测域名服务器 172.16.1.254 是否可解析 www.topsec.com 的示例：

TopsecOS# **system probe dns serverip** *172.16.1.254* **dns** *www.topsec.com*

48 bytes from 172.16.1.254, www.topsec.com has ipv4 address: 195.218.116.139, dns=6.20ms

48 bytes from 172.16.1.254, www.topsec.com has ipv4 address: 195.218.116.139, dns=4.53ms

48 bytes from 172.16.1.254, www.topsec.com has ipv4 address: 195.218.116.139, dns=1.64ms

--- sum data: 144 bytes, average time statistics: 4.12ms ---

8.3.2 抓包工具

TopWAF 支持在线抓包功能，可帮助管理员通过采样方式进一步分析网络运行状况提供依据，并且为后续管理员制定更切实际和严密的防护策略提供参考。TopWAF 可根据管理员临时制定的抓包规则（如设定需抓取的数据包的协议类型、IP 地址、端口等信息，）对网络上的数据包进行手动截获。

下面介绍制定手动抓包规则，以及查看抓包方式获取的抓包文件。

WEBUI 方式

步骤1 选择 **系统管理 >系统诊断 >抓包工具**。进入抓包条件设置界面，如下图所示。

在设置抓包条件时，各项参数的具体说明如下表所示。

参数	说明
抓包数量	设置捕获的报文总数，当捕获的报文数达到配置值，则自动停止抓包

参数	说明
	功能。
协议类型	设置捕获的报文的协议类型，可选项：udp、tcp、ip、arp。
源 IP	设置捕获的报文的源 IP 地址。IP 地址格式：A.B.C.D。 说明： “源或目的 IP”参数设置后，该参数无效。
源端口	设置捕获的报文的源端口号。端口取值范围：1-65535。 说明： “源或目的端口”参数设置后，该参数无效。
目的 IP	设置捕获的报文的目的 IP 地址。IP 地址格式：A.B.C.D。 说明： “源或目的 IP”参数设置后，该参数无效。
目的端口	设置捕获的报文的目的端口号。端口取值范围：1-65535。 说明： “源或目的端口”参数设置后，该参数无效。
源或目的 IP	设置捕获的报文的源或目的 IP 地址。IP 地址格式：A.B.C.D。 说明： 该参数设置后，“源 IP”和“目的 IP”参数将无效。
源或目的端口	设置捕获的报文的源或目的端口。端口号取值范围：1-65535。 说明： 该参数设置后，“源端口”和“目的端口”参数将无效。
接口	设置进行在线抓包的接口。
高级	是否开启用高级命令设置自动抓包。
system tcpdump -ni	通过命令设置抓包的条件。 说明： 当勾选“高级”时，其余参数的输入框都是不可编辑的。

步骤2 参数设置完成后点击【开始】按钮即可进行抓包操作，抓包完成之后结果会在本页面下方显示。管理员可以下载、删除和清空抓包的结果。

CLI 方式

system tcpdump –ni any

✧ 关于该部分命令的具体语法请参考 tcpdump 的相关命令。

命令描述：

对所有接口的 80 端口进行抓包监听，默认抓 65535 字节的数据，可通过-c 设置抓包的个数。

命令示例：

对所有接口的 80 端口进行抓包监听，抓包的个数为 5。

TopsecOS# **system tcpdump -ni any port** 80 **-c** 5

ngtos_tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on any, link-type EN10MB (Ethernet), capture size 65535 bytes

M-1 [feth0] 14:01:32.833181 IP 192.168.25.212.44323 > 192.168.25.107.80: Flags [S], seq 967138987, win 5840, options [mss 1460,sackOK,TS val 86751661 ecr 0,nop,wscale 7], length 0

X-1 [feth0] 14:01:32.833256 IP 192.168.25.212.44323 > 192.168.25.107.80: Flags [S], seq 967138987, win 5840, options [mss 1460,sackOK,TS val 86751661 ecr 0,nop,wscale 7], length 0

M-0 [feth0] 14:01:33.294719 IP 192.168.25.212.58604 > 192.168.25.220.80: Flags [S], seq 981684255, win 5840, options [mss 1460,sackOK,TS val 86751776 ecr 0,nop,wscale 7], length 0

X-0 [feth0] 14:01:33.294803 IP 192.168.25.212.58604 > 192.168.25.220.80: Flags [S], seq 981684255, win 5840, options [mss 1460,sackOK,TS val 86751776 ecr 0,nop,wscale 7], length 0

R-1 [feth0] 14:01:33.295328 IP 192.168.25.220.80 > 192.168.25.212.58604: Flags [S.], seq 2055027218, ack 981684256, win 8192, options [mss 8960,nop,wscale 8,sackOK,TS val 36434306 ecr 86751776], length 0

5 packets captured

5 packets received by filter

0 packets dropped by kernel

8.4 管理员

管理员是用来登录并对设备进行管理配置的特殊用户，管理员可以通过 CLI、Web 等方式登录设备，对设备进行网络以及安全策略等相关配置，使设备按用户需求工作。每台 TopWAF 设备可以有多个管理员，不同的管理员对设备可以有不同的管理权限。

设备出厂后，第一次启动过程中将初始化预置管理员。按照职能和管理范围的不同，管理员可以分为超级管理员 superman、配置管理员，虚拟系统管理员。所有的管理员不允许重名。

1）超级管理员具有 TopWAF 中所有的管理权限；

2）配置管理员具有查看和设定规则的权限，以及部分 TopWAF 管理权限，但没有分配管理员的权限，只能修改自身的登录密码。

超级管理员可以添加、删除、修改配置管理员并对他们进行相应的授权。

管理员登录方式的具体说明如下表所示。

登录方式	说明
Web	即通过 HTTPS 登录 Web 界面。管理员可利用任意以太网接口，只要登录 PC 与设备路由可达并开放相应的服务即可，一般优先选择管理口进行登录。 说明： 1）设备默认开启 HTTPS 服务。 2）管理员通过 Web 界面对设备进行操作，这种操作方式比命令行方式更直观。
CLI	即通过命令行方式登录，可选项：Console 口、Telnet、SSH。 1）Console 口方式是其他命令行登录方式的基础，同一时刻只允许一个人操作。使用场景有： （a）首次登录设备 CLI 界面； （b）无法远程登录设备时，通过 Console 口进行本地登录； （c）设备无法正常启动时，通过 Console 口进入并加载系统软件。 2）Telnet 方式便于对设备进行远程管理和维护，同一时刻允许多人操作。 3）SSH 方式与 Telnet 方式相比更安全。

8.4.1 密码设置

为降低管理员管理管理员账号的难度，并保障普通管理员账号的安全，TopWAF 支持管理员修改其自身密码。

WEBUI 方式

步骤1 选择 **系统管理** > **系统设置** > **管理员**，激活“管理员”页签。

✧ 在管理员模块的设置界面中配置好密码强度，在此处提示出选择的强度。关于密码强度的设置具体请参见 8.4.4 设置。

在修改管理员自身密码时，各项参数的具体说明如下表所示。

参数	说明
输入原始密码	输入管理员账号当前密码。
输入密码	设置新密码，新密码不能与旧密码相同，密码的复杂度的设置具体请参见 8.4.4 设置。
再次输入	再次输入新密码，需与“输入密码”文本框中输入的密码完全一致。

步骤2 点击【应用】按钮完成密码的修改。

CLI 方式

password old-password <*mstring*> **new-password** <*mstring*> **new-repeat** <*mstring3*>

命令描述：

修改当前管理员的密码。

参数说明：

参数	说明
old-password <*mstring*>	必选项。输入管理员的当前密码。 字符串类型。不以“\\”结尾且不包含“<script>”字符串。
new-password <*mstring*>	必选项，输入管理员新密码。 字符串类型。不以“\\”结尾且不包含“<script>”字符串。
new-repeat <*mstring*>	必选项，重新输入管理员的新密码。 字符串类型。不以“\\”结尾且不包含“<script>”字符串。

命令示例：

TopsecOS# **password old-password** *talent* **new-password** *topsec123* **new-repeat** *topsec123*

8.4.2 管理员

TopWAF 支持预置管理员对其进行管理，也支持新添加的管理员对其进行管理。新添加的管理员的权限由其继承的管理权限模板控制，关于管理权限模板的设置具体请参见 8.4.3 管理权限。

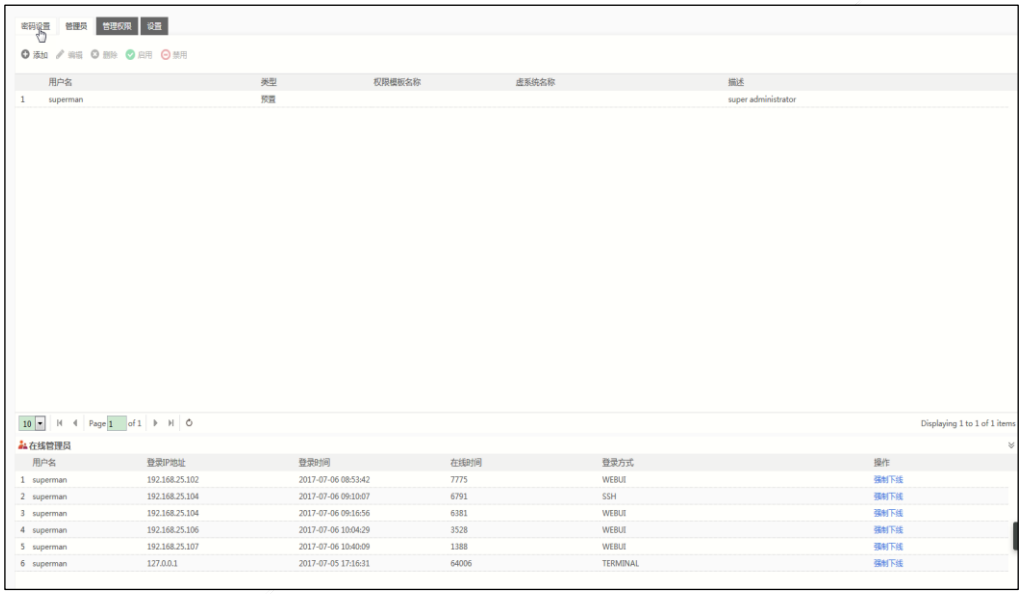
管理员登录成功后，登记在一个在线管理员列表里，在线管理员信息包括：管理员名称、登录 IP 地址、登录时间、在线时间、登录方式。

具备管理员管理权限的管理员可新添不同访问控制类型的管理员，还可远程监控登录 TopWAF 的所有管理员，并可强制在线管理员退出系统。

✧ 预置管理员不能被删除、被修改权限，只限于对预置管理员的操作只限于修改自身密码，预置管理员不能被删除、被修改权限。

WEBUI 方式

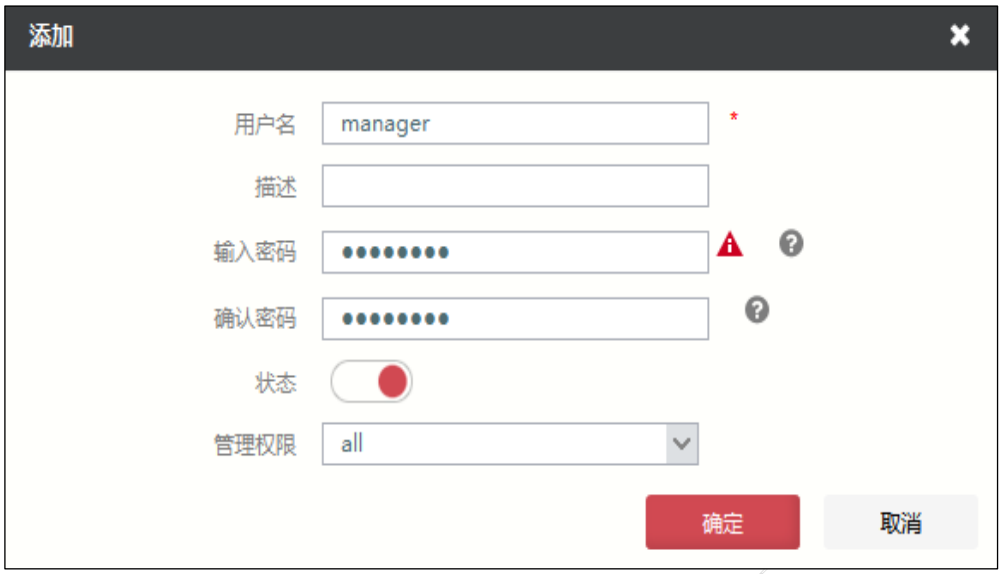
步骤1 选择 **系统管理** > **管理员**，激活“管理员”页签，进入管理员功能界面，如下图所示。



界面中上半部分显示了所有管理员账号信息，包括管理员名称、类型和管理权限等信息。选中已有管理员，点击菜单栏中的『启用』，弹出确定启用当前管理员的提示窗口，然后点击【确定】按钮表示该管理员账号启用；点击菜单栏中的『禁用』，弹出确定禁用当前管理员的提示窗口，然后点击【确定】按钮表示该管理员账号被禁用。界面下半部分显示了目前所有登录 TopWAF 的在线管理员信息，包括名称、登录 IP 地址、最近登录时间、在线累积时间和登录方式。

✧ 管理员列表中，若管理员账号被禁用，则显示为深灰色，如上图红框内所示的策略，非深灰色的管理员账号均处于启用状态。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。



在添加管理员时，各项参数的具体说明如下表所示。

参数	说明
用户名	必选项，设置管理员的用户名称，需为除“!@#$%^&+=|?\"\\'> <`~”以外的字符。
描述	设置管理员的相关描述。
输入密码	必选项，设置管理员名称对应的密码，关于密码的复杂度具体请参见 8.4.4 设置。
确认密码	必选项，再次输入管理员名称对应的密码。
状态	设置管理员的启用状态。默认为“”，表示已开启，点击该按钮将显示“”，表示已关闭。
管理权限	设置管理员具备管理 TopWAF 的权限。关于管理权限的设置具体请参见 8.4.3 管理权限。

点击【确定】按钮完成管理员的添加。

步骤3 选择在线管理员列表中任一管理员，点击相应的『强制下线』，强制管理员下线。

CLI 方式

system admin add name <*nstring*> **passwd** <*mstring*> [**comment** <*wstring*>] [**vsys-name** <*nstring*>]

命令描述：

添加系统管理员。

参数说明：

参数	说明
name <*nstring*>	必选项，设置管理员名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
passwd <*mstring*>	必选项，设置管理员登录密码。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
comment <*wstring*>	可选项，设置对添加的管理员的具体说明。 字符串类型，不包含“<>\\”中任意字符。

命令示例：

添加名称为“zmz”，登录密码为“talent”的管理员。

TopsecOS # **system admin add name** *zmz* **passwd** *talent*

system admin modify-info name <*nstring*> [**passwd** <*mstring*>] [**comment** <*wstring*>]

命令描述：

修改系统管理员基本信息。

参数说明：

参数	说明
name <*nstring*>	必选项，指定管理员名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
passwd <*mstring*>	可选项，设置管理员登录密码。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
comment <*wstring*>	可选项，设置对添加的管理员的具体说明。 字符串类型，不包含“<>\\”中任意字符。

system admin modify-priv admin-name <*nstring*> [**map-name** <*nstring*>]

命令描述：

修改系统管理员权限。

参数说明：

参数	说明
admin-name <*nstring*>	必选项，指定管理员名称。 字符串类型，不包含“!@#$%^&+=|?\” \\’ ><`~”中任意字符，且不能包含空格。
map-name <*nstring*>	可选项，设置管理权限的模板名称。 字符串类型，不包含“!@#$%^&+=|?\” \\’ ><`~”中任意字符，且不能包含空格。

system admin forced-offline session-id <*num*>

命令描述：

强制管理员下线配置。

参数说明：

参数	说明
session-id <*num*>	必选项，实数类型,设置在线管理员的编号。

system admin show <cr>

命令描述：

显示系统管理员。

命令示例：

TopsecOS # **system admin show**

admin-name: superman

admin-type: default

privilege-map:

comment:super administrator

status: valid

system admin online <cr>

命令描述：

显示系统在线管理员。

命令示例：

TopsecOS # **system admin online**

---

session-id: 1 admin-name: superman logon-ip: 192.168.104.11 logon-type: WEBUI

logon-time: 2015-01-30 01:30:52 online-time: 1857

---

session-id: 2 admin-name: superman logon-ip: 192.168.92.6 logon-type: WEBUI

logon-time: 2015-01-30 01:52:34 online-time: 555

session-id: 3 admin-name: superman logon-ip: 192.168.92.3 logon-type: WEBUI

logon-time: 2015-01-30 01:52:44 online-time: 546

---

session-id: 4 admin-name: superman logon-ip: 192.168.92.6 logon-type: TELNET

logon-time: 2015-01-30 01:56:07 online-time: 343

---

session-id: 5 admin-name: superman logon-ip: 192.168.104.11 logon-type: WEBUI

logon-time: 2015-01-30 01:56:58 online-time: 291

8.4.3 管理权限

管理权限指管理员对 TopWAF 各功能模块的操作权限，包括“无”、“只读”和“读写”，“无”指管理员无查看和设置权限；“只读”指管理员具备查看的权限；“读写”指管理员具备设置权限。TopWAF 基于管理权限模板对非预定义的管理员赋予管理权限，关于为管理员赋予管理权限的操作具体请参见 8.4.2 管理员。

✧ 创建管理员账号和为管理员赋权可由相同的管理员完成，也可由不同的管理员完成。例如在一员管理模式下，可由 superman 完成管理员创建及赋权的操作；三员管理模式下，可由 admin 创建管理员账号，grantor 为管理员赋权。

TopWAF 基于管理权限模板对非预置管理员赋予管理权限，管理权限模板可实现划分 TopWAF 的部分功能为不同的访问控制类型，以控制不同管理员的管理权限，进而对管理 TopWAF 进行合理分工。

WEBUI 方式

步骤1 选择 **系统管理** > **管理员**，激活“管理权限”页签。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。

在添加权限模板时，各项参数的具体说明如下表所示。

参数	说明
权限名	必选项，设置权限模板名称。
描述	设置权限模板必要的描述信息。
自定义模块	设置权限模板的访问权限。 说明： 勾选相应模块的复选框，则具有查看及配置该模块相关配置的功能。

步骤3 点击【确定】按钮完成权限模板的添加。

CLI 方式

system privilege show-modules <cr>

命令描述：

显示系统管理权限及其对应的 ID。

命令示例：

TopsecOS# **system privilege show-modules**

63	log	130	ha
131	helpmode	133	dns
134	global	135	snmp
137	memory	138	pf-service
139	local-service	143	config-file
144	stream5	256	alarm
257	show-running	258	show
259	ping	260	network-show
320	define	322	user_manage
324	vsys	325	stat
896	ddos	902	waf

system privilege map create name <*nstring*> [**comment** <*wstring*>] [**r-module** <*mstring*>] [**rw-module** <*mstring*>]

命令描述：

添加管理权限模板。

参数说明：

参数	说明
name <*nstring*>	必选项，设置管理权限模板的名称。 字符串类型，不包含“!@#$%^&+=|?\”\\’><`~”中任意字符，且不能包含空格。
comment <*wstring*>	可选项，设置权限模板必要的描述信息。 字符串类型，不包含“<>\\”中任意字符。
r-module <*mstring*>	可选项，选择只读的功能编号（ID 号），用逗号分隔，例如：256,129,281。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： 可通过 **system privilege show-modules** 命令查看功能对应的 ID 号。
rw-module <*mstring*>	可选项，选择读写的功能编号（ID 号），用逗号分隔，例如：256,129,281。

参数	说明
	字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： 可通过 **system privilege show-modules** 命令查看功能对应的 ID 号。

命令示例：

添加名称为“map1”，包含功能模块“902”的管理权限模板。

TopsecOS# **system privilege map create name** *map1* **rw-module** *281*

system privilege map show-single name <*nstring*>

命令描述：

显示指定的管理权限模板的功能信息。

参数说明：

参数	说明
name <*nstring*>	必选项，指定管理权限模板的名称。 字符串类型，不包含“!@#$%^&+=|?\” \\’ ><`~”中任意字符，且不能包含空格。

命令示例：

添加名称为“map1”，包含功能模块“901”的管理权限模板。

TopsecOS# **system privilege show-single name** log

name: security-policy

type: default

description: 拥有安全引擎以及访问控制策略相关的操作权限

privilege:

id module_mean status

65	管理员管理	none
66	权限管理	none
128	高可用性	none
129	提示语言	none
130	DHCP 服务	none
133	SNMP 服务	none
134	设备维护	none
256	告警配置	none
258	配置维护	rw
259	网络诊断	none
261	网络管理	r
262	设备管理服务	none
263	地址转换	rw
264	本机服务策略	none
265	资源对象	rw
266	访问控制	rw
268	应用代理	rw
273	会话管理	none
274	日志	r
280	WAF 管理	rw
281	DDOS 管理	rw

system privilege map show <cr>

命令描述：

显示所有的功能权限。

命令示例：

TopsecOS# **system privilege map show**

name: security-policy

type: default

description: 拥有安全引擎以及访问控制策略相关的操作权限

privilege:

id	module_name	status
65	管理员管理	none
66	权限管理	none
128	高可用性	none
129	提示语言	none
130	DHCP 服务	none
133	SNMP 服务	none
134	设备维护	none
256	告警配置	none
258	配置维护	rw
259	网络诊断	none
261	网络管理	r
262	设备管理服务	none
263	地址转换	rw
264	本机服务策略	none
265	资源对象	rw
266	访问控制	rw
268	应用代理	rw
273	会话管理	none
274	日志	r
280	WAF 管理	rw
281	DDOS 管理	rw

system privilege map add-module name <*nstring*> [**r-module** <*mstring*>] [**rw-module** <*mstring*>]

命令描述：

添加功能模块到管理权限中。

参数说明：

参数	说明
name <*nstring*>	必选项，设置自定义模板名称。 字符串类型，不包含“!@#$%^&+=|?\” \\’ ><`~”中任意字符，且不能包含空格。
r-module <*mstring*>	可选项，选择只读的功能编号（ID 号），用逗号分隔，例如：256,129,281。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： 可通过 **system privilege show-modules** 命令查看功能对应的 ID 号。
rw-module <*mstring*>	可选项，选择读写的功能编号（ID 号），用逗号分隔，例如：256,129,281。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： 可通过 **system privilege show-modules** 命令查看功能对应的 ID 号。

system privilege map sub-module name <*nstring*> [**module-select** <*mstring*>]

命令描述：

删除指定管理员的功能模块的访问权限。

参数说明：

参数	说明
name <*nstring*>	必选项，指定管理员权限模板。 字符串类型，不包含“!@#$%^&+=|?\” \\’ ><`~”中任意字符，且不能包含空格。
module-select <*mstring*>	可选项，设置要删除的权限模块对应的 ID。 字符串类型，不以“\\”结尾且不包含“<script>”字符串。 说明： 可通过 **system privilege map show-single name** <*string*> 命令查看功能对应的 ID 号。

8.4.4 设置

管理员负责 TopWAF 的管理与配置，因此为保证 TopWAF 的安全性，管理员的登录会话必须设置一定的安全保护机制，以防止非法人员窃取管理员账号。具备管理员模块读写权限的管理员可以通过设置管理员账号的密码复杂度、允许最大登录失败次数、最大在线数，防止管理员账号被暴力破解，提高管理员管理设备的安全性。

WEBUI 方式

步骤1 选择 **系统管理** > **管理员**，激活“设置”页签，进入管理员账号安全设置界面。如下图所示。

在设置管理员账号安全保护机制时，各项参数的具体说明如下表所示。

参数	说明
密码复杂度	为适应管理员密码安全性、易用性的不同需求，TopWAF 提供密码复杂度的设置功能。 设置添加管理员时口令密码的复杂程度。可选项：高、中、低。 说明： “高”表示密码设置要大于 16 个字符，小于等于 128 个字符，必须包含大小写、数字、特殊英文字符“!@#$%^&*_+-=)”，不包含自身信息（用户名、描述）。

参数	说明
	“中”表示密码设置要大于 12 个字符、小于等于 128 个字符，必须包含大小写、数字。 “低”表示密码设置要大于 8 个字符，小于等于 128 个字符。
首次登录是否强制修改密码	为适应管理员密码安全性、易用性的不同需求，TopWAF 提供首次登录强制修改密码的设置功能。 勾选复选框表示开启首次登录强制修改密码功能。
允许最大登录失败次数	设置允许同一管理员连续登录 TopWAF 的最大失败次数。单位：次；取值范围：3-100；默认值：5。 说明： 同一管理员登录失败次数超过最大失败次数后，TopWAF 的登录界面将被锁定一段时间。
账号锁定时间	设置 TopWAF 的 WEBUI 界面因管理员超过最大登录失败次数后仍未成功登录的锁定时间。单位：秒；取值范围：30-3600；默认值：60。
管理员最大在线数	设置允许管理员登录 TopWAF 的最大连接数。单位：个；取值范围：1-5000；默认值：100。
同一个管理员最大在线数	设定使用同一管理员账号同时管理 TopWAF 的最大连接数。单位：个；取值范围：1-5000；默认值：15。
webui 方式登录最大并发管理数	设置管理员使用 WEBUI 界面方式同时管理 TopWAF 的最大连接数。单位：个；取值范围：0-5000，0 表示不限制；默认值：0。
ssh 方式登录最大并发管理数	设置所有管理员使用 SSH 方式同时管理 TopWAF 的最大连接数。单位：个；取值范围：0-5000，0 表示不限制；默认值：0。
telnet 方式登录最大并发管理数	设置管理员使用 Telnet 方式同时管理 TopWAF 的最大连接数。单位：个；取值范围：0-5000，0 表示不限制；默认值：0。
管理员密码修改周期	设置管理员密码修改周期。单位：天。取值范围：0-365 天，0 表示不限制。
认证方式	指定用户的认证方式，可选项为本地认证和外部认证。 勾选“外部认证”时，需输入认证服务器的名称或 IP 地址。

步骤2 参数设置完成后，点击【应用】按钮完成账号安全机制的配置，点击【重置】按钮将管理员账号保护机制的各参数值恢复为出厂配置。

CLI 方式

system admin-auth-policy set [**password-complexity** <high|medium|low>] [**first-login** <yes|no>] [**maxnum-admin-online** <*num*>] [**maxnum-same-admin-online** <*num*>] [**maxnum-auth-fail** <*num*>] [**account-locked-time** <*num*>] [**password-modify-period**<num>]

命令描述：

管理员账号安全设置。

参数说明：

参数	说明
password-complexity <high|medium|low>	可选项，设置添加管理员时口令密码的复杂程度，可选项为：高|中|低。
first-login <yes|no>	可选项，设置是否开启首次登录强制修改密码功能，可选项为是|否。
maxnum-admin-online <*num*>	可选项，设置所有管理员登录 TopWAF 的最大连接数。 实数类型，单位：个；取值范围：1-5000；默认值：100。
maxnum-same-admin-online <*num*>	可选项，设定使用同一管理员账号同时管理 TopWAF 的最大连接数。 实数类型，单位：个；取值范围：1-5000；默认值：5。
maxnum-auth-fail <*num*>	可选项，设置允许同一管理员连续登录 TopWAF 的最大失败次数。 实数类型，单位：次；取值范围：3-100；默认值：5。
account-locked-time <*num*>	可选项，设置 TopWAF 的 WEBUI 界面因管理员超过最大登录失败次数后仍未成功登录的锁定时间。 实数类型，单位：次；取值范围：3-100；默认值：5。
password-modify-period <*num*>	可选项，设置管理员密码修改周期。 实数类型，单位：天；取值范围：0-365。

命令示例：

TopsecOS# **system admin-auth-policy set password-complexity** high **first-login** yes **maxnum-admin-online** *100* **maxnum-same-admin-online** *5* **account-locked-time** *60*

system admin-auth-policy show <cr>

命令描述：

显示管理员账号安全设置信息。

命令示例：

TopsecOS# **system admin-auth-policy show**

password-complexity: high

anti-crack: on

maxnum-auth-fail: 100

account-locked-time: 3000(seconds)

maxnum-admin-online: 200

maxnum-same-admin-online: 200

password-need-change-first-login: yes

online number limit of login type:

webui: 0 ;ssh: 0 ;telnet: 0

password modify period: 7 days

system admin-auth-policy reset <cr>

命令描述：

重置管理员账号安全设置信息。

8.5 系统日志

TopWAF 提供完善的系统日志功能，方便管理员及时跟踪 TopWAF 的工作状态，比如管理员登录、系统事件、出错信息等反映系统当前或一段时间内的运行状况，及时对生成的日志进行综合分析，发现安全隐患，从而提高被保护网络的安全性和设备安全系统的管理成效。

管理员可根据用户的实际需求，在日志配置界面灵活配置 TopWAF 需要记录的日志，并可以从日志查看界面中查看设备上记录的日志。系统日志按时间先后顺序保存至本地缓存中，设备上记录的日志过多会导致系统缓存区容量达到最大，此时当新的日志产生时，系统将删除缓存区中最旧的日志，显示当前最新的日志。如果管理员想要查看历史日志信息，可以利用 TopWAF 提供的日志服务器配置功能，将设备日志上传至配置好的日志服务器中，在日志服务器中进行查看。

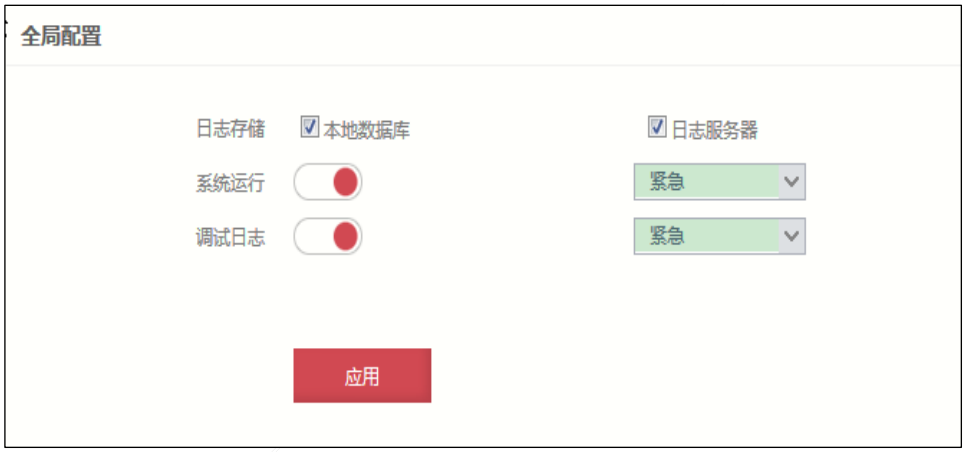
8.5.1 日志配置

TopWAF 日志的功能主要是记录系统运行时的各种信息，如用户登录，系统事件，出错信息等，能够反映系统当前和一段时间内的运行状况。管理员可通过配置系统日志生成条件控制系统日志的数量，以获取定位系统问题时具备参考价值的日志。

WEBUI 方式

在配置日志之前，需要先进行日志服务器的配置，关于日志服务器的介绍具体请参见 8.5.2 日志服务器配置。

步骤1 选择 **系统管理** > **系统日志** > **日志配置**。如下图所示。



在配置系统日志记录条件时，各项参数的具体说明如下表所示。

参数	说明
日志存储	必选项。选择日志的存储方式，包括本地数据库存储和日志服务器存储，可同时勾选。
系统运行	必选项，设置是否记录系统运行日志的开关。
调试日志	必选项，设置是否记录调试日志的开关。
日志级别（下拉框内容）	日志所属级别包括： 紧急：造成严重错误导致系统不可用。 告警：警报信息。 严重：严重错误信息，可能会造成某些功能无法正常工作。 错误：一般错误信息。 警示：所有攻击行为以及非授权访问（除通信日志外）。 通知：非错误信息，但需要管理员特殊处理。 信息：普通事件。

参数	说明
	调试：开发人员调试信息，包括正常的使用信息。 其中，级别为紧急、告警、严重的日志属于高级别的日志，级别为错误、警示、通知的日志属于中级别的日志，级别为信息、调试的日志属于低级别的日志。

✧ 若日志配置发生变化，则系统读取新的参数，建立新的连接，同时关闭与客户端的连接，并通知客户端配置发生了改变。

步骤2 点击【应用】按钮完成日志信息的配置。

CLI 方式

log config type <all|debug|system> **level** <*num*>

命令描述：

设置日志的类型和级别。

参数说明：

参数	说明
type <all|debug|system>	必选项，选择日志类型，可选项为：所有日志|调试日志|系统日志
level <*num*>	必选项，设置日志的级别。系统将会记录所选级别及其以上级别的日志信息。如选择严重，则系统将记录紧急、告警和严重级别的日志信息。值越小表示级别越高。 实数类型，0：紧急，1：告警，2：严重，3：错误，4：警示，5：通知，6：信息，7：调试。 日志级别如下： 紧急：造成严重错误导致系统不可用，该日志被传送到日志服务器； 告警：警报信息，需要通知管理员，该日志被传送到日志服务器； 严重：严重错误信息，可能会造成某些功能无法正常工作； 错误：一般错误信息； 警示：所有攻击行为以及非授权访问（除通信日志外）； 通知：管理员操作； 信息：通事件； 调试：开发人员调试信息。

命令示例：

TopsecOS# **log config type** system **level** *1*

log config show <cr>

命令描述：

显示日志配置信息。

命令示例：

```
TopsecOS# log config show
log config set ipaddr '192.168.1.254' port UDP:514 logtype syslog trans enable t
rans_gather yes log_switch on
log config crypt disable
log config key_set clean
log config set to_console off
log config set to_file off
log config set mode retry off
log config type_set mgmt level_set 8
log config type_set system level_set 3
log config type_set pf level_set 8
log config type_set ha level_set 8
log config type_set debug level_set 0
```

8.5.2 日志服务器配置

日志服务器能够集中负责日志的收集、分析、报告和日志安全管理，可以有效地协助管理员进行系统管理维护、攻击定位，发现安全风险。

TopWAF 可以按照 Welf 或 Syslog 格式来记录日志。系统日志可保存在本地缓存中，当本地存储的日志数量越来越多，本地磁盘大小有限导致设备存储不够时，可考虑通过 TCP 或 UDP 协议将记录的日志传送到日志服务器上，从而实现对设备日志进行统计与分析，并及时发现攻击等安全隐患，提高 TopWAF 的安全管理。

WEBUI 方式

步骤1 选择 **系统管理** > **系统日志** > **日志服务器配置**。如下图所示。

在配置日志服务器时，各项参数的具体说明如下表所示。

参数	说明
服务器地址	必选项，设置日志服务器的 IP 地址，格式：x.x.x.x，默认地址：192.168.1.254。最多可设置 16 个日志服务器。
服务器端口	必选项，设置日志服务器接收日志的服务端口。取值范围：1-65535；默认值：514。 说明： 日志服务器端口必须和设备日志服务器配置页面所指定的端口一致。
传输协议	必选项，设置 TopWAF 传输日志至日志服务器中所使用的协议，可选项：TCP、UDP。
传输类型	必选项，设置 TopWAF 记录日志的格式，可选项：Welf、Syslog。 说明：

参数	说明
	TopWAF 可以按照 Welf 格式或者 Syslog 格式记录日志，并通过 Syslog 协议传送到已设定的日志服务器上，可采用第三方软件来对日志进行统计与分析。
合并传输	必选项。设置是否合并传输日志至所配置的日志服务器中。
传输加密	必选项。设置是否加密传输至日志服务器中的日志。

步骤2 点击【应用】按钮完成日志服务器的配置。

CLI 方式

log config set [**ipaddr** <*mstring*>] [**port** <*string*>] [**logtype** <syslog|welf>] [**console** <on|off>] [**trans** <enable|disable>] [**trans_gather** <yes|no>]

命令描述：

配置日志服务器。

参数说明：

参数	说明
ipaddr <*mstring*>	可选项，设置日志服务器的 IP 地址。 字符串类型，表示 IP 地址，格式为 A.B.C.D。
port <*string*>	可选项，设置日志服务器接收日志的端口号。 字符串类型，格式为 udp:端口号或 tcp:端口号，端口号取值范围：1-65535；默认值：514。
logtype <syslog|welf>	可选项，设置日志服务器传输日志的传输类型，有 2 种：syslog 和 welf。
console <on|off>	可选项，设置是否传输日志到控制台。
trans <enable|disable>	可选项，设置是否传输日志。
trans_gather <yes|no>	可选项，设置是否要合并日志的传输。

命令示例：

TopsecOS# **log config set ipaddr** *192.168.1.25* **logtype** syslog **port** *udp:80* **trans** enable **trans_gather** yes

log config set mode retry <on|off>

命令描述：

设置重试模式。

参数说明：

参数	说明
retry <on|off>	必选项，设置是否开启重试模式。

log config crypt <enable|disable>

命令描述：

设置是否进行日志加密。

参数说明：

参数	说明
crypt <enable|disable>	必选项，设置是否进行日志加密。

命令示例：

TopsecOS# **log config crypt** enable

log config key <*string*>

命令描述：

设置日志的密钥。

参数说明：

参数	说明
key <*string*>	必选项，设置日志的密钥。 字符串类型，8 个字符。不包含“$\"\\'%<>”中任意字符，也不能包含空格。

命令示例：

TopsecOS# **log config key** *11111111*

log config key clean <cr>

命令描述：

清除日志的密钥。

8.6 高可用性

在数据通信过程中，各种软件或硬件错误都可能导致网络连接异常中断，造成数据传输失败或防护网络功能失效。如下图所示，所有的网络流量都从 TopWAF 设备进行转发，如果 TopWAF 设备故障，整条链路的业务将中断。

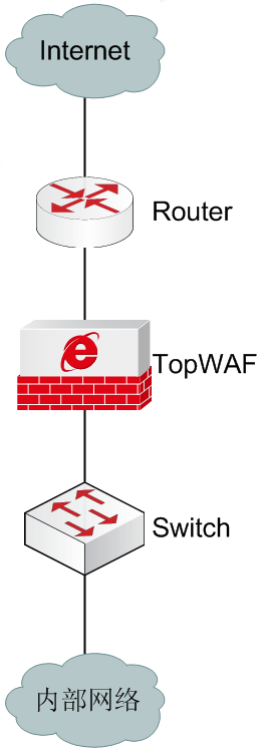


图 8-9 单链路网络示意图

为了保证网络的可靠性，TopWAF 提供了冗余备份功能，以确保在 TopWAF 通信线路或设备故障时，也能保障业务网络数据的正常运转，提高设备的可用性。

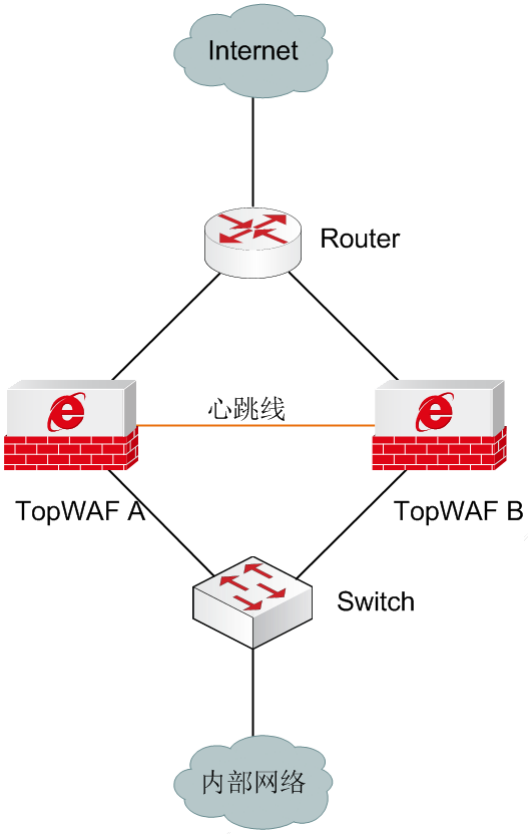


图 8-10 双链路网络示意图

如上图所示，TopWAF A 和 TopWAF B 之间通过心跳口同步状态信息、连接信息和配置信息。

TopWAF 通过配置热备组实现高可用性，同一 TopWAF 设备支持多个热备组，可在不同的热备组中作为主设备或者备设备，如下图所示。如果配置为双机热备工作场景，仅需配置热备组 1 即可，如果配置为负载均衡工作场景，则需要配置热备组 1 和热备组 2。

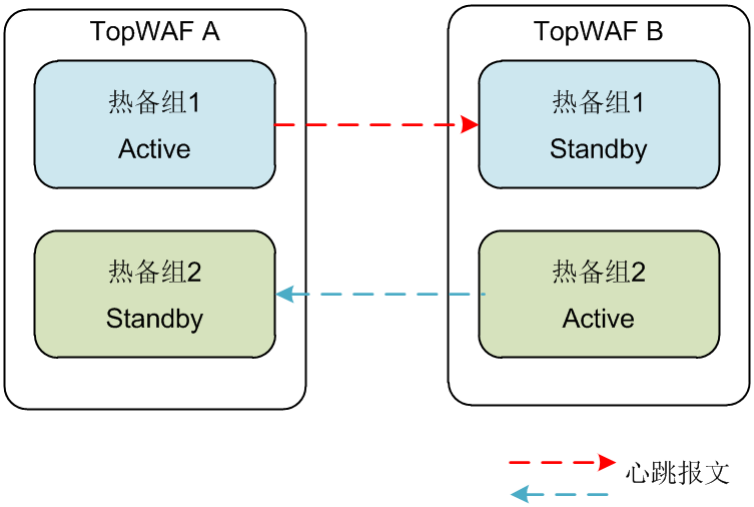


图 8-11 热备组示意图

热备组中的设备有如下 4 种工作状态：

- INIT：初始化状态，热备组未启用。
- ACTIVE：主用状态，当前设备为主用设备。
- STANDBY：备用状态，当前设备为备用设备。
- PREEMPT：抢占状态，当前设备已从故障中恢复，且已启用抢占模式，如果抢占延时时间内，设备正常工作，则设备将抢占为主用状态。

TopWAF 的高可用性支持 3 种工作模式：主备模式（AS，Active-to-Standby）、负载均衡模式（AA，Active-to-Active）、连接保护模式（SP，Session Protect）。

✧ 高可用性中的 TopWAF，必须使用心跳口交换状态监测及探测信息，TopWAF 上的任何以太网接口都可以做为心跳接口。

✧ 利用高可用性进行冗余备份时，两台 TopWAF 型号、软件版本必须一致，否则在其中一台故障时，无法保证将业务正常切换到另外一台设备。

8.6.1 高可用性

- 配置主备模式

TopWAF 以主备模式部署时，由 2 台 TopWAF 设备组成热备组，设备有 2 种工作状态主设备和备设备，有一台主设备处于工作状态，另外一台设备处于备份状态。

如下图所示，主备模式由正常情况到故障情况的工作流量。

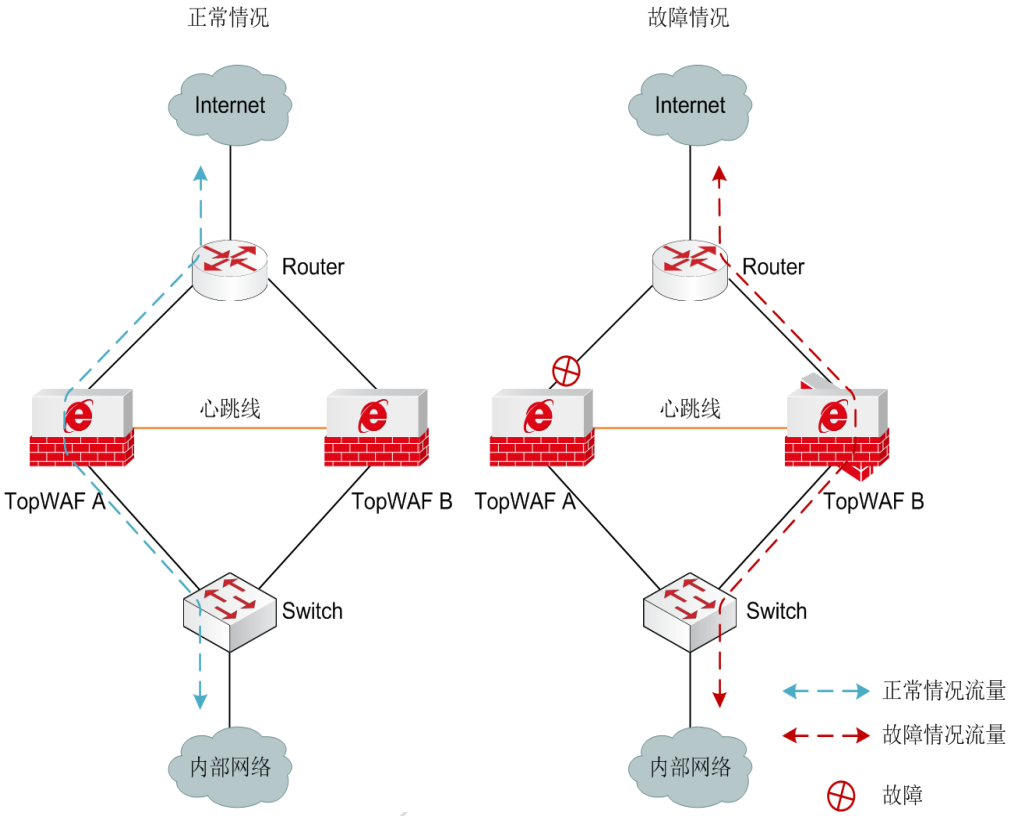


图 8-12 双机热备工作场景示意图

1）正常情况下，主设备承担报文的转发、检测等任务，主设备通过心跳口实时同步处于工作状态的 TopWAF 的状态和配置信息到备设备。

2）当主设备的软件或硬件（不包括心跳口）出现故障时，处于备份状态的 TopWAF 立即对用户完全透明的情况下接替主设备的工作。

3）当主设备故障恢复时，则根据 TopWAF 是否为抢占模式，决定设备是否由备设备切换回主设备。热备组配置为抢占模式时，主设备故障恢复后，恢复原来的主设备为工作状态，为了防止因设备运行不稳定，导致其热备组中设备的角色频繁切换，需要配置适当的延迟时间，主设备工作稳定后再从备设备切换回主设备。

在配置主备模式前，需要先进行如下步骤：

- 配置心跳口属性。所有心跳口的地址必须配置在同一网段，而且接口属性必须要勾选“非同步地址”选项，关于接口属性的配置请参见 7.1 接口，否则心跳口的 IP 地址信息会在主从设备运行状态同步时被对方覆盖。
- 配置双机热备的相关参数，并启用双机热备功能。

WEBUI 方式

步骤1 选择 **系统管理** > **高可用性**。进入高可用性设置基本信息的界面，如下图所示。

在设置基本信息时，各项参数的具体说明如下表所示。

参数	说明
模式	设置为“主备模式”。
本端 IP	设置本端设备心跳口的 IP 地址。IP 地址必须为心跳口上已经配置的 IP 地址。
对端 IP	设置对端设备心跳口的 IP 地址。 说明： 对端 IP 地址和本地 IP 地址必须在同一子网内。
心跳口	设置同步主备设备工作状态的通信接口。
链路探测开关	设置是否开启链路探测功能。
HA 启用状态	是否启用 HA 功能。
配置同步到对端	是否将除 HA 之外的配置数据通过心跳接口同步到对端。

步骤2 参数设置完成后，点击【应用】按钮保存配置。

步骤3 点击“管理组设置”下的『添加』，弹出“添加”窗口。

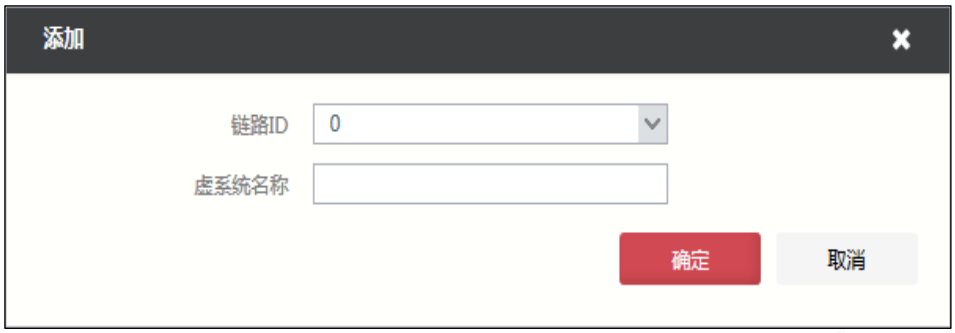
在配置 TopWAF 在热备组中的属性时，各项参数的具体说明如下表所示。

参数	说明
组 ID	设置 TopWAF 通信接口（除心跳口以外）所属热备组的组号，该组号用于确定处于同一热备组的设备，取值范围：1-255。 说明： 1）处于同一热备组的 TopWAF 设备组 ID 需配置相同。 2）热备组的虚拟 MAC 地址由 TopWAF 的组号映射而生成。
配置角色	设置本机在热备组中所处的工作状态，可选项：主、备。 主：管理组处于工作状态 备：管理组处于备份状态
主动抢占	设置是否开启“抢占”模式，即作为主设备的本机出现通信故障时，热备组中的其他设备担任主设备的角色，当本机的故障解除后，是否重新夺回主设备的地位。 说明： 只有当主设备与从设备相比有明显的性能差异时，才需要配置主设备工作在“抢占”模式，否则，当原主设备恢复工作时主从设备的再次切换浪费系统资源。
抢占延迟	设置抢占的推迟时间，以防止本机运行不稳定而导致其热备组中设备的角色频繁切换。单位：秒；取值范围：1-120。
可用接口	从可用接口下拉框中选择接口添加到管理组，并监控其工作状态。

✧ TopWAF 工作在主备模式时，只需添加一个管理组。

步骤4 点击【确定】按钮完成本机在热备组中角色属性的设置。

步骤5 主备模式的相关参数设置完成之后，点击“链路绑定设置”下的『添加』，如下图所示。



步骤6 指定已配置的链路 ID 和虚系统名称，参数设置完成之后点击【确定】按钮完成链路的添加。关于链路探测的设置具体请参见 7.5 链路探测。

CLI 方式

步骤	配置命令	配置说明
1	**ha mode set** as	设置 HA 为主备模式。
2	**ha interface add** <*string*> **local** <*ip*> **remote** <*ip*>	设置 HA 的心跳口，本端 IP 地址及对端 IP 地址。
3	**ha group** <*num*> **mode** <master|backup>	添加热备组，并配置设备在热备组中的角色为主设备/备设备。
4	**ha group** <*num*> **preempt** <enable|disable>	（可选）设置热备组是否启用抢占模式。
5	**network interface** <*string*> **tgid** <*num*>	将接口添加到管理组。
6	**ha group** <*num*> **preempt delay** <*num*>	（可选）设置热备组的抢占延时时间。
7	**ha start** <cr>	启动 HA 功能。
8	**ha sync-config-to-peer** <cr>	HA 同步，同步本端配置到对端。

8.6.1.1 配置负载均衡模式

TopWAF 以负载均衡模式部署时，有 2 种工作状态主设备和备设备。TopWAF 设备组成 2 个热备组，每个热备组中有一台主设备处于工作状态，另外一台设备处于备份状态。

如下图所示，负载均衡工作场景正常情况到故障情况的工作流量。

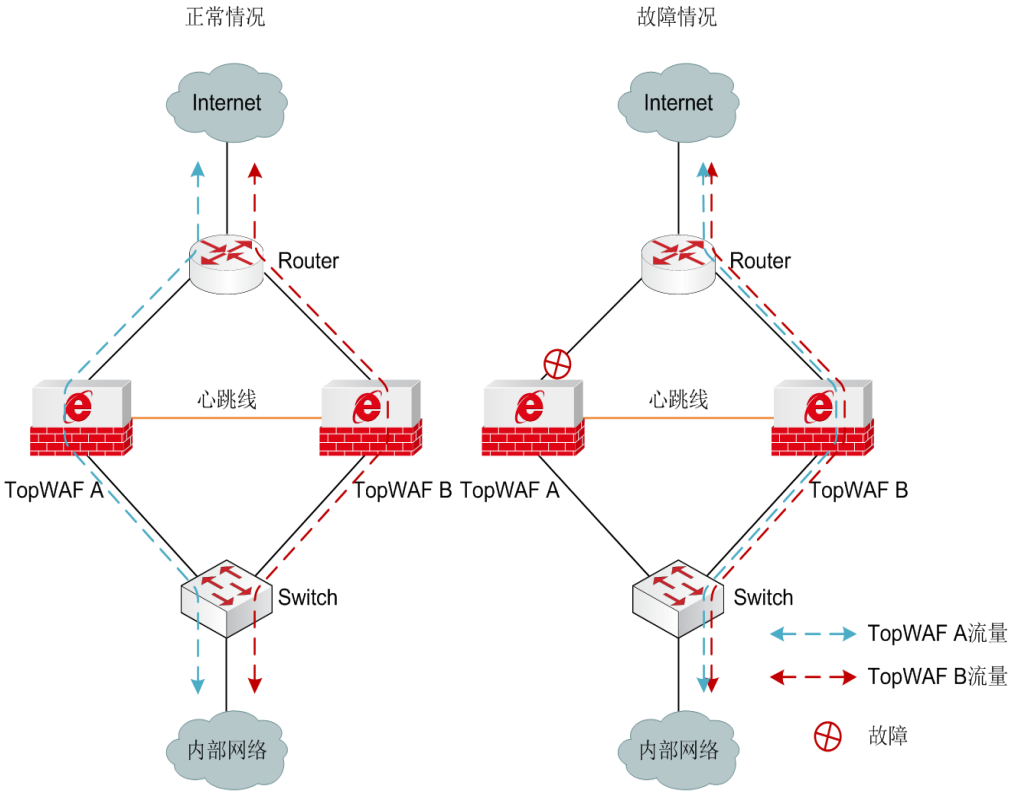


图 8-13 负载均衡工作场景示意图

- 正常情况下，热备组的 2 台设备独立工作，各自承担报文的转发、检测等任务，通过心跳口相互同步对方的状态和配置信息，互为对方的备设备。
- 当其中一台设备的软件或硬件（不包括心跳口）出现故障时，处于同一热备组中的另外一台 TopWAF 立即对用户完全透明的情况下接替故障设备的工作。
- 当主设备故障恢复时，则根据 TopWAF 是否为抢占模式，决定设备是否由备设备切换回主设备。热备组配置为抢占模式时，主设备故障恢复后，恢复原来的主设备为工作状态，为了防止因设备运行不稳定，导致其热备组中设备的角色频繁切换，需要配置适当的延迟时间，主设备工作稳定后再从备设备切换回主设备。

在配置负载均衡模式前，需要先进行如下步骤：

- 配置心跳口属性。
- 配置其他通信接口。互为备份的接口可配置相同的 IP 地址。
- 配置负载均衡的相关参数，并启用负载均衡功能。

WEBUI 方式

步骤1 选择 **系统管理** > **高可用性**。进入高可用性设置基本信息的界面，如下图所示。

步骤2 在配置全局属性时，各项参数的具体说明如下表所示。

参数	说明
模式	设置为“负载均衡”。
本端 IP	设置本端设备心跳口的 IP 地址。
对端 IP	设置对端设备心跳口的 IP 地址。 说明： 对端 IP 地址和本地 IP 地址必须在同一子网内。
心跳口	设置同步主设备工作状态的通信接口。
链路探测开关	设置是否开启链路探测功能。
HA 启用状态	是否启用 HA 功能。
配置同步到对端	是否将除 HA 之外的配置数据通过心跳接口同步到对端。

步骤3 参数设置完成后，点击【应用】按钮保存配置。

步骤4 点击“管理组设置”下的『添加』，弹出“添加”窗口。

在配置 TopWAF 在热备组中的属性时，各项参数的具体说明如下表所示。

参数	说明
组 ID	设置 TopWAF 通信接口（除心跳口以外）所属热备组的组号，该组号用于确定处于同一热备组的设备，取值范围：1-255。 说明： 1）处于同一热备组的 TopWAF 设备组 ID 需配置相同。 2）热备组的虚拟 MAC 地址由 TopWAF 的组号映射而生成。
配置角色	设置本机在热备组中所处的工作状态，可选项：主、备。 主：管理组处于工作状态 备：管理组处于备份状态
主动抢占	设置是否开启“抢占”模式，即作为主设备的本机出现通信故障时，热备组中的其他设备担任主设备的角色，当本机的故障解除后，是

参数	说明
	否重新夺回主设备的地位。 说明： 只有当主设备与从设备相比有明显的性能差异时，才需要配置主设备工作在“抢占”模式，否则，当原主设备恢复工作时主从设备的再次切换浪费系统资源。
抢占延迟	设置抢占的推迟时间，以防止本机运行不稳定而导致其热备组中设备的角色频繁切换。单位：秒；取值范围：1-120。
监控接口	从可用接口中选择接口添加到管理组。

✧ TopWAF 工作在负载均衡模式时，需添加两个管理组。

步骤5 点击【确定】按钮完成本机在热备组中角色属性的设置。

CLI 方式

步骤	配置命令	配置说明
1	**ha mode set** aa	设置 HA 为负载均衡模式。
2	**ha interface add** <*string*> **local** <*ip*> **remote** <*ip*>	设置 HA 的心跳口，本端 IP 地址及对端 IP 地址。
3	**ha group** <*num*> **mode** master	添加热备组，并配置设备在热备组 1 中的角色为主设备。
4	**ha group** <*num*> **mode** backup	添加热备组，并配置设备在热备组 2 中的角色为备设备。
5	**network interface** <*string*> **tgid** <*num*>	将接口添加到管理组。
6	**ha group** <*num*> **preempt** <enable|disable>	（可选）设置热备组是否启用抢占模式。
7	**ha group** <*num*> **preempt delay** <*num*>	（可选）设置热备组的抢占延时时间。
8	**ha start** <cr>	启动 HA 功能。
9	**ha sync-config-to-peer** <cr>	HA 同步，同步本端配置到对端。

8.6.1.2 配置连接保护模式

在连接保护模式下，所有 TopWAF 均处于工作状态并且在网络部署层面相互独立，不区分主备，如下图所示。

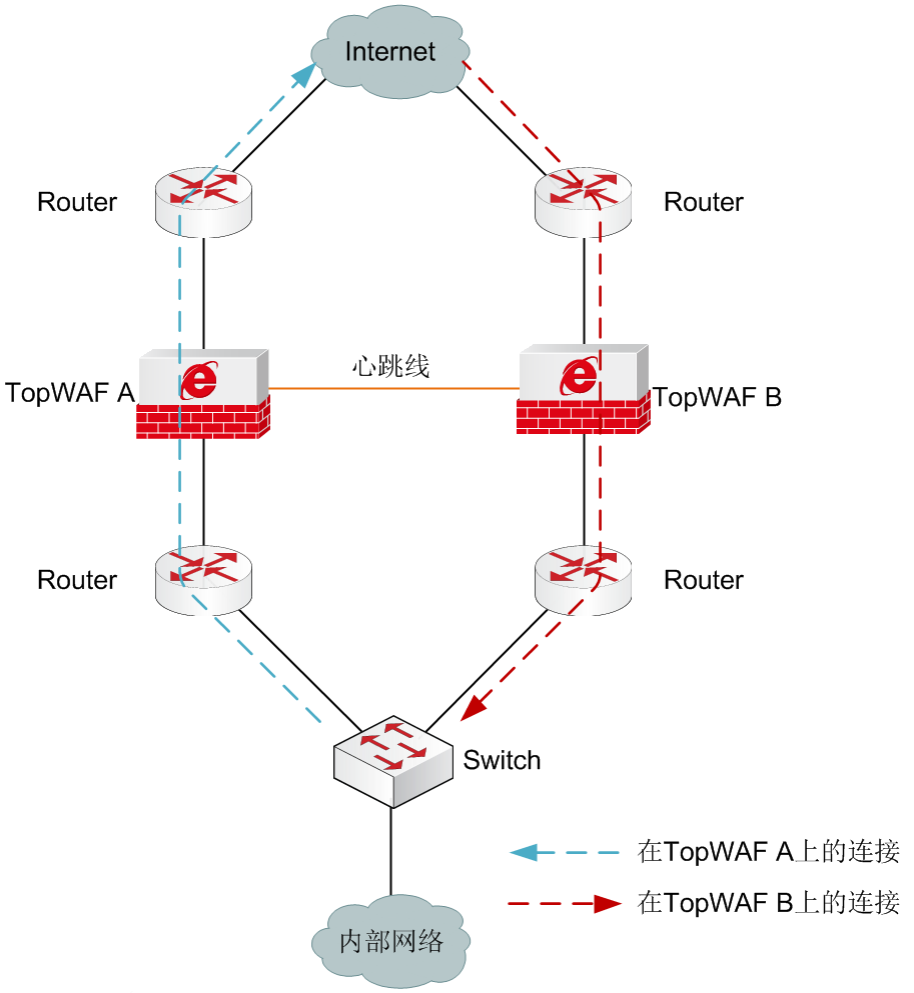


图 8-14 TopWAF 连接保护模式示意图

- 当两台 TopWAF 均正常工作时，由上下游的设备进行选路。如果内部网络在发送数据报文时，选择从 TopWAF A 发送，在 TopWAF A 上将建立数据报文的连接，如果从网络中返回的数据报文选择从 TopWAF B 上返回，在没有开启连接保护模式时，TopWAF B 上没有建立该网络连接，将丢弃该报文；在开启连接保护模式后，TopWAF A 通过心跳口将连接信息同步到 TopWAF B 上，将该连接的报文正常转发到内部网络。
- 当其中一台 TopWAF 发生故障时，上下游设备经过协商后会将其上的数据流通过另外的 TopWAF 转发。

TopWAF 工作在连接保护模式下支持透明和路由模式。连接保护模式下不需要添加热备组，只需配置本地和对端地址即可。

在配置连接保护模式前，需要先进行如下步骤：

- 配置心跳口属性。所有心跳口的地址必须配置在同一网段，否则心跳口的 IP 地址信息会在主从设备运行状态同步时被对方覆盖。
- 配置其他通信接口。互为备份的接口必须配置相同的 IP 地址。
- 配置连接保护的相关参数，并启用连接保护功能。

WEBUI 方式

步骤1 选择 **系统管理** > **高可用性**。进入高可用性设置基本信息的界面，如下图所示。

在配置全局属性时，各项参数的具体说明如下表所示。

参数	说明
模式	设置为“连接保护”。
本端 IP	设置本端设备心跳口的 IP 地址。
对端 IP	设置对端设备心跳口的 IP 地址。
心跳口	设置同步主设备工作状态的通信接口。
链路探测开关	设置是否开启链路探测功能。
HA 启用状态	是否启用 HA 功能。
配置同步到对端	是否将除 HA 之外的配置数据通过心跳接口同步到对端。

步骤2 参数设置完成之后，点击【应用】按钮完成连接保护功能的全局配置。

✧ 连接保护模式不需要添加管理组。

CLI 方式

步骤	配置命令	配置说明
1	**ha mode set** sp	设置 HA 为连接保护模式。
2	**ha interface add** <*string*> **local** <*ip*> **remote** <*ip*>	设置 HA 的心跳口，本端 IP 地址及对端 IP 地址。
3	**ha start** <cr>	启动 HA 功能。
4	**ha sync-config-to-peer** <cr>	HA 同步，同步本端配置到对端。

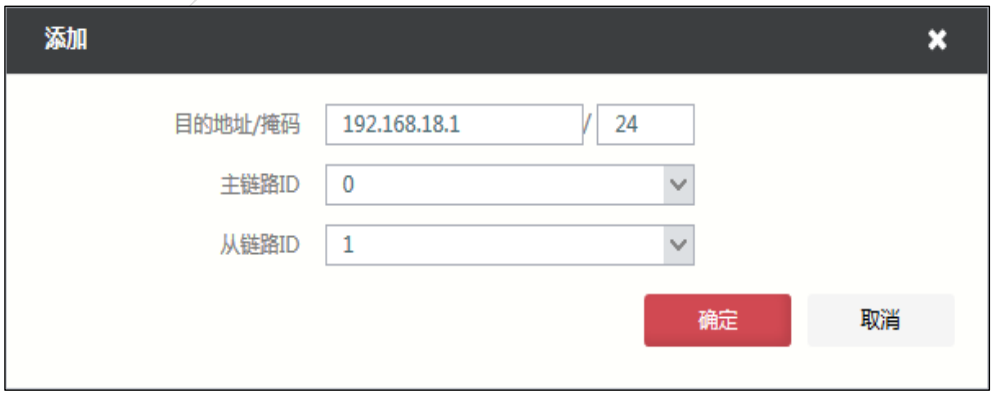
8.6.2 链路备份

在网络设备的整个运行期间，无法保证设备所有接口都能长时间正常运作，或不可避免地会遇到一些可知或不可知因素造成设备某接口无法运行。天融信防火墙提供了“链路备份”功能来实时监视整个链路的工作情况，一旦发现异常，就立即启动“链路备份”功能自动切换到另一条备用链路，以确保网络的正常通信。

WEBUI 配置

步骤1 选择 **系统管理** > **高可用性** > **链路备份**。

步骤2 点击『添加』，弹出“添加”窗口，如下图所示。



在设置链路备份时，各项参数的具体说明如下表所示。

参数	说明
目的地址/网络前缀	必选项。用来标识 IPv4/IPv6 包的目的地址或目的网络。

参数	说明
主链路	必选项。选择已经设置的链路探测 ID，关于链路探测的设置具体请参见 7.5 链路探测。
从链路	必选项。选择已经设置的 IP 探测链路 ID。 说明： 从链路和主链路不能选择同一个链路 ID。关于链路探测的设置具体请参见 7.5 链路探测。

步骤3 参数设置完成后，点击【确定】按钮完成链路备份的设置。

步骤4 选择一条链路备份规则，点击『启用』，启动链路备份功能。

✧ 启动链路备份功能时，会判断当前两条默认路由是否可用，如果不可用，就不启动，并且报错。

CLI 配置

network linkbak set master-id <*num*> **slave-id** <*num*> **dst** <*string*>

命令描述：

链路备份参数设置。

参数说明：

参数	说明
master-id <*num*>	必选项，指定主链路。 数值类型，取值范围：0-9。
slave-id <*num*>	必选项，指定从链路接口。 数值类型，取值范围：0-9。
dst <*string*>	必选项，指定目的 IP 地址，仅当二层协议设置为 IP 协议时需要设置该项。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。

network linkbak show <cr>

命令描述：

查看链路备份的运行信息和状态信息。

network linkbak start <cr>

命令描述：

启动链路备份服务。

network linkbak stop <cr>

命令描述：

停止链路备份服务。

network linkbak clean <cr>

命令描述：

清空链路备份所有设置。

8.6.3 高可用性相关命令

ha clean <cr>

命令描述：

清除 HA 的配置信息。

ha interface add <*string*> **local** <*ip*> **remote** <*ip*>

命令描述：

设置心跳接口。

使用 **ha interface delete** <*string*>命令删除心跳口配置。

参数说明：

参数	说明
add <*string*>	设置接口名称。 字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。
local <*ip*>	本端设备。 IPv4 地址类型，可输入 0 或 0.0.0.0 或 255.255.255.255。
remote <*ip*>	对端设备。 IPv4 地址类型，可输入 0 或 0.0.0.0 或 255.255.255.255。

命令示例：

设置 feth3 为心跳口，本端的 IP 地址为 192.168.1.3，对端的 IP 地址为 192.168.1.6。

TopsecOS# **ha interface add feth3 local 192.168.1.3 remote** 192.168.1.6

ha group <*num*> **delete** <cr>

命令描述：

删除备份组。

参数说明：

参数	说明
group <*num*>	AS 模式下的管理组号，实数类型，取值范围：1-255。

ha group <*num*> **mode** <master|backup>

命令描述：

用于 TopWAF 主备工作状态切换，执行该命令之前需开启 TopWAF 的 HA 功能。

如果 HA 功能已经启用，切换主备工作状态前，需要先停止 HA 功能。

参数说明：

参数	说明
group <*num*>	AS 模式下的管理组号，实数类型，取值范围：1-255。
mode <master|backup>	TopWAF 工作状态设置。主设备|备设备。

ha group <*num*> **preempt** <enable|disable>

命令描述：

配置备份组抢占模式。用户应当首先设定 HA 的工作模式，然后再设置该参数，否则会有错误提示信息。

参数说明：

参数	说明
group <*num*>	设置 ID 号，实数类型，取值范围：1-255。
preempt <enable|disable>	必选项，HA 抢占设置。

命令示例：

设置备份组抢占。

TopsecOS# **ha vrid** *1* **preempt** enable

ha group <*num*> **preempt-delay** <*num*>

命令描述：

设置抢占的延时时间，以防止本机运行不稳定而导致其热备组中设备的角色频繁切换。

参数说明：

参数	说明
group <*num*>	设置 ID 号，实数类型，取值范围：1-255。
preempt-delay <*num*>	必选项，HA 抢占设置。 抢占延时时间，实数类型单位：秒；取值范围：1-120。
number2	抢占延时时间，单位：秒；取值范围：1-120。

命令示例：

设置备份组抢占延时时间为 100s。

TopsecOS# **ha group** *1* **preempt delay** 100

ha mode set <aa|as|sp>

命令描述：

配置 HA 模式。

参数说明：

参数	说明
set <aa|as|sp>	负载均衡模式|双机热备模式|连接保护模式

命令示例：

配置 HA 模式为负载均衡模式。

TopsecOS# **ha mode set** aa

配置 HA 模式为双机热备模式。

TopsecOS# **ha mode set** as

ha show <config|status|session-statistic>

命令描述：

查看 HA 的配置信息。

参数说明：

参数	说明
config	查看当前 HA 的参数配置。
status	查看本设备 HA 的运行状态。

参数	说明
session-statistic	查看备份组会话的统计信息。

命令示例：

查看当前 HA 参数配置。

```
TopsecOS# ha show configuration
ha clean
ha mode set aa
ha group 255 mode master
ha group 255 preempt enable
ha group 255 preempt-delay 10
```

查看当前 HA 参数配置。

```
TopsecOS# ha show status
Group 255
State          Preempt      Priority     Interface
INIT           enable       65000
```

查看备份组的会话统计信息。

```
TopsecOS# ha show session-statistic
ha_statistic_config.ha_HA_get_pktbuff_DP_enter is 0
ha_statistic_config.ha_HA_send_pkt_DP_enter is 0
ha_statistic_config.xmit_error_statistic is 0
ha_statistic_config.ha_HA_COMM_bulidDpMessage_enter is 0
ha_statistic_config.ha_HA_COMM_bulidDpMessage_success is 0
ha_statistic_config.ha_HA_COMM_recvDpMessage_call_session is 0
ha_statistic_config.ha_HA_COMM_recvDpMessage_enter is 0
```

ha_statistic_config.ha_HA_COMM_sendDpMessage_enter is 0

ha_statistic_config.ha_HA_COMM_sendDpMessage_success is 0

ha start <cr>

命令描述：

启动 HA。HA 默认为停止状态，需要手工启动。

可使用 **ha stop** <cr>命令停用 HA。

ha sync-config-to-peer <cr>

命令描述：

HA 同步（从同步配置到对端设备上）。

使用说明：

HA 同步前需要先使用 **ha start** 命令启动 HA 功能。

命令示例：

同步配置到对端机上。

TopsecOS# **ha sync-config-to-peer**

network interface <*string*> **tgid** <*num*>

命令描述：

将接口添加到管理组。

参数说明：

参数	说明
interface <*string*>	查看当前 HA 的参数配置。

参数	说明
	字符串类型，不包含“$\"\\'%<>”中任意字符，也不能包含空格。
tgid <*num*>	必选项，设置高可用性管理组 ID。 实数类型，取值范围：0-255，0 表示取消 tgid。

命令示例：

添加接口到管理组。

TopsecOS# **network interface** *feth11* **tgid** *1*

查看管理组的监视接口。

```
TopsecOS# ha show status
HA-Status: ha disable
Heartbeat-Local IP: 0.0.0.0

Group 1
State       Preempt     Priority    Interface
INIT        enable      65000       feth11
```

声明

1．本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。

2．本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。

3．本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。

4．本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。

RELIABLE NETWORK
SAFE WORLD
TOPSEC