

**Linux抗DDOS流量防火墙使用手册**

****

**HIDDOS研发团队**

**https://gitee.com/httpwaf/**

**版权声明**

本文所有解释权归HTTPWAF研发部所有

Linux抗DDOS流量防火墙（下文简称HIDDOS）版权所有，保留一切权利。

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**开发团队**所有，受到有关产权及版权法保护。未经书面许可不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。

**信息更新**

本文档仅用于为最终用户提供帮助信息，并且随时可由更改或撤回，以最新的文档为准。

**适用版本**

**本文档适用于最新发布版本。**

**免责条款**

根据适用法律的许可范围，按“最新发布版本”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。

**期望读者**

期望了解本产品主要技术特性的用户、研发人员、售前人员、代理商成员等。本文档假设您对下面的知识有一定的了解：

* 进程与防火墙
* Linux基础知识
* 网络安全基础知识
* 文档信息

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** |  | | |
| **扩散范围** | 可扩散任何人 | **文档版本号** | 2.0 |
| **作者** |  | **日期** |  |
| **初审人** |  | **复审人** |  |

* 版本变更记录

|  |  |  |  |
| --- | --- | --- | --- |
| **时间** | **版本** | **说明** | **作者** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[1. 安装前准备 5](#_Toc26412)

[1.1. 系统支持 5](#_Toc30128)

[1.2. 承诺 5](#_Toc29805)

[1.3. 不承诺 5](#_Toc17224)

[2. 安装方式 6](#_Toc22446)

[2.1. 安装步骤 6](#_Toc12550)

[2.2. 运行、停止和卸载 6](#_Toc21779)

[3. WEB管理 7](#_Toc15773)

[3.1. 登录 7](#_Toc5912)

[3.2. 主页 8](#_Toc24014)

[3.3. 进程数据 8](#_Toc10983)

[3.4. 风控分析 10](#_Toc20444)

[3.5. 流量数据 11](#_Toc11379)

[3.6. 白名单进程/IP 11](#_Toc9151)

[3.7. 黑名单进程/IP 11](#_Toc2136)

[3.8. 抗DDOS 12](#_Toc26114)

[3.9. 日志查看 12](#_Toc10706)

[4. 系统管理 13](#_Toc2663)

[4.1. 远程管理 13](#_Toc23878)

[4.2. 恢复出厂设置 14](#_Toc23747)

[4.3. 系统重启 14](#_Toc13358)

[5. 开机启动 14](#_Toc12727)

[6. 开放源码 14](#_Toc23921)

# 安装前准备

## 系统支持

HIDDOS是一款Linux上“DDOS流量防护+进程防火墙”的开源产品，以弥补IPTABLES的不足，大幅降低DDOS防御成本，支持主流CentOS、Ubuntu、Debian等x86-64位系统，管理端口9998**禁止向公网开放**（或设置IP访问白名单）。**免费版本只检测流量，不进行防护阻断IP。**

## 承诺

为了保证服务器安全，我们承诺：

1. 除首次下载安装包，**任何时候绝不联网**，更没有任何后门，不放心的用户可以源码方式部署。
2. 实战测试过主流环境，稳定可靠，默认设置不会影响系统，放心使用。

## 不承诺

免费版不承诺任何环境都有效，不提供任何技术服务，无论任何原因引发的任何问题，都不负任何责任。**请务必在测试环境完美演练后，再谨慎部署到生产环境。**

# 安装方式

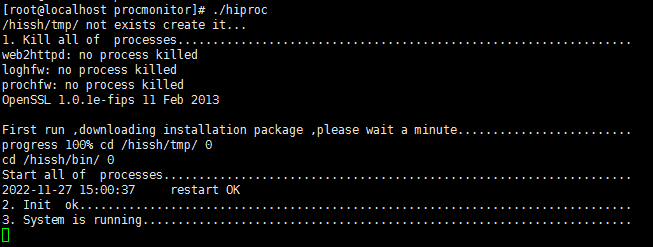
## 安装步骤

**hiddos集安装、启动、状态监控、停止于一体，**保证系统可以联网，并且9998端口没有被占用，硬盘剩余空间大于5G，以root权限，运行下面命令：

chmod +x ./hiddos

./hiddos

首次运行要下载最新版本，大约需要1分钟时间，如果出现下图三个步骤，打印出了 3.System is running.....，代表已经安装成功。



## 运行、停止和卸载

启动运行: ./ hiddos

后台模式运行: ./ hiddos daemon

停止运行: ./ hiddos stop

卸载 : rm /hiproc/ -rf

默认没加开机启动，请自行把hiddos加入服务器开机启动程序。

# WEB管理

## 登录

管理口是9998端口，在浏览器上输入服务器的IP如http://192.168.1.8:9998/即可看到登录页面，用户名是admin 密码默认是admin ，登录进入主页后，请在顶上右边菜单尽快修改密码。

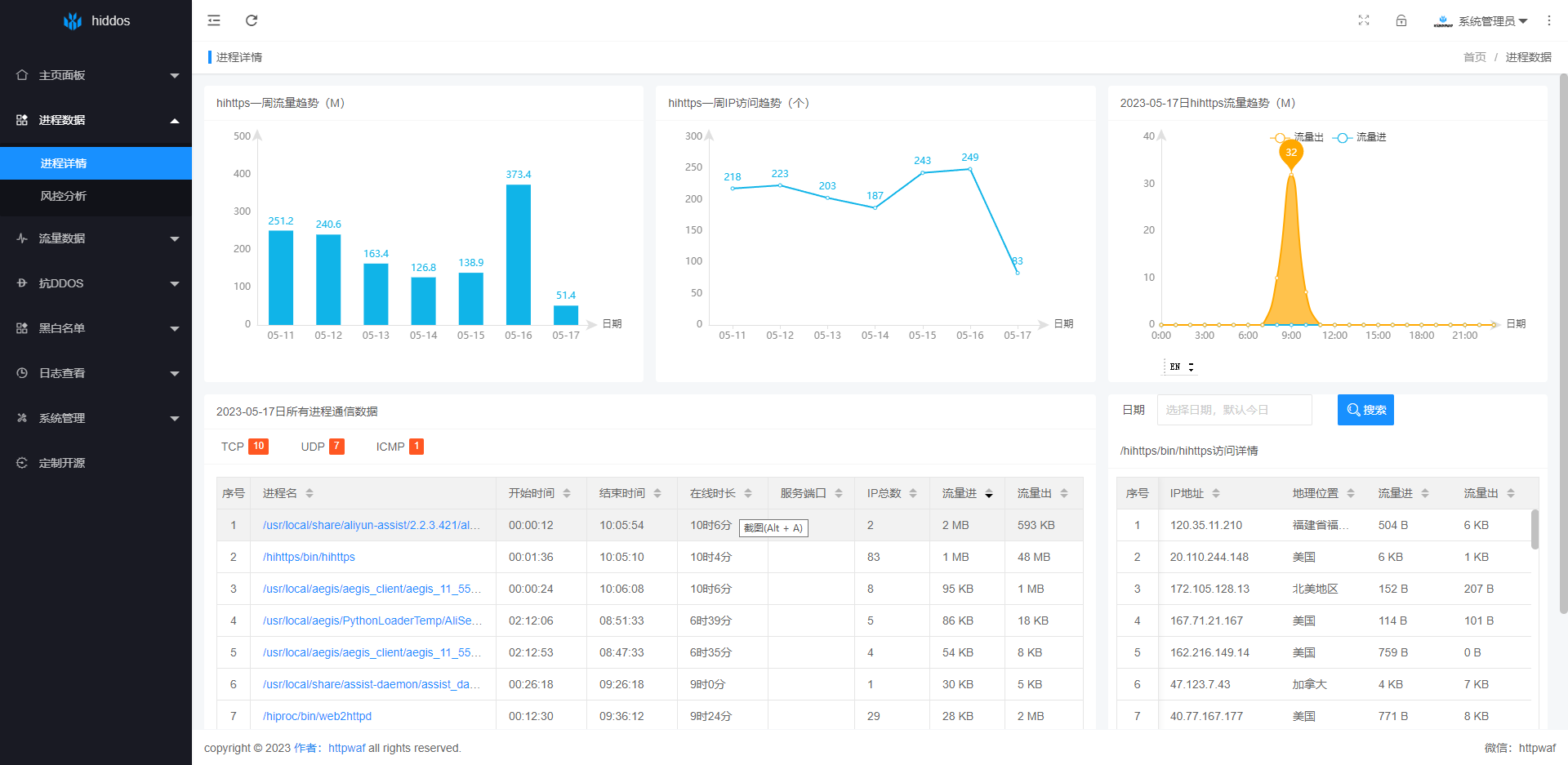


## 主页

登录后进入主页，其中数据是**1分钟更新一次**，理论上安装1分钟内，至少会出现流量、IP地址的数据，说明系统运行正常，否则就和我们技术支持联系。



## 进程数据



点击进程列表数据统计栏，右边可以看到详细的IP地址信息，默认是今天的数据。

点击上面的柱状图和时间，可以切换到任意日期的之前数据，所有进程访问过的IP地址一目了然。

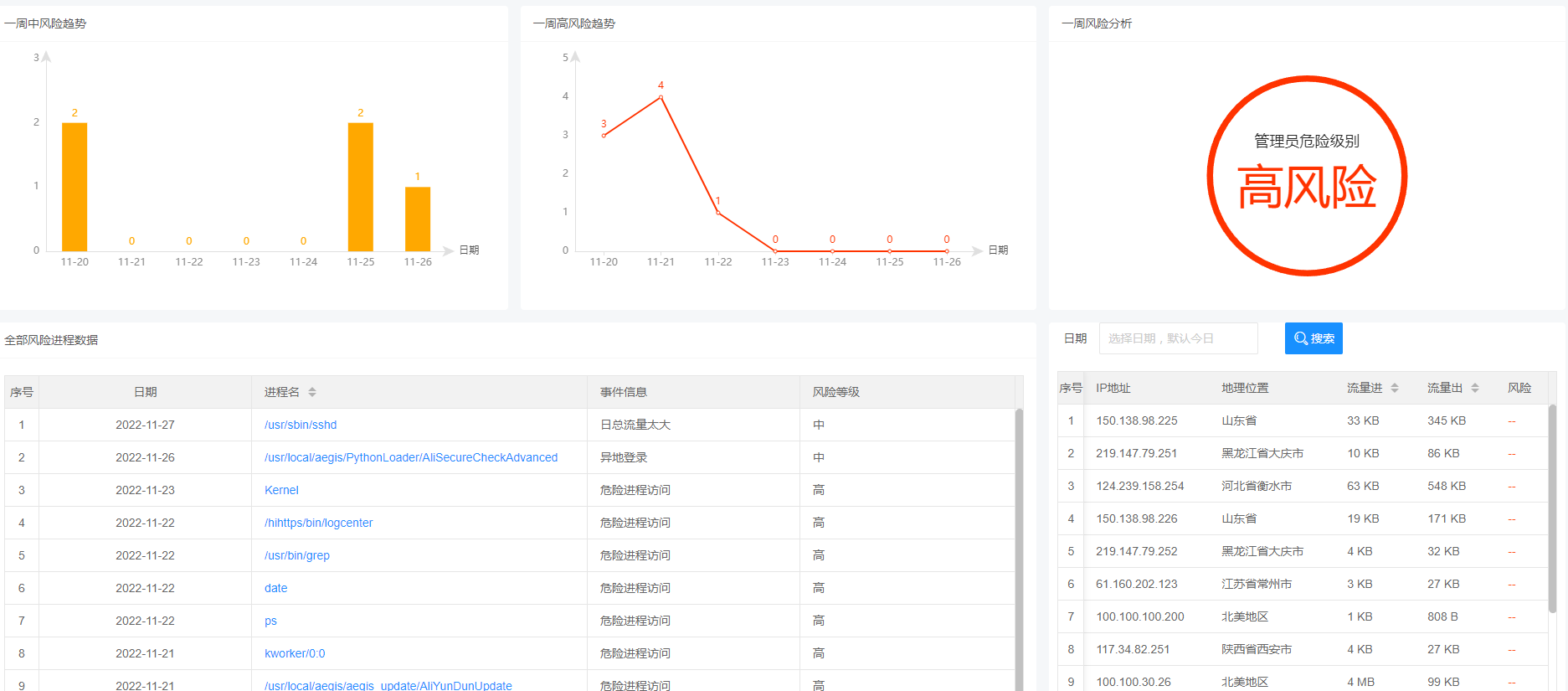
如下图的这台服务器的AliYunDun进程向大量的服务器传送了数据，这种情况就要仔细排查是否服务器被植入了后门，还是本身正常的业务。



## 风控分析

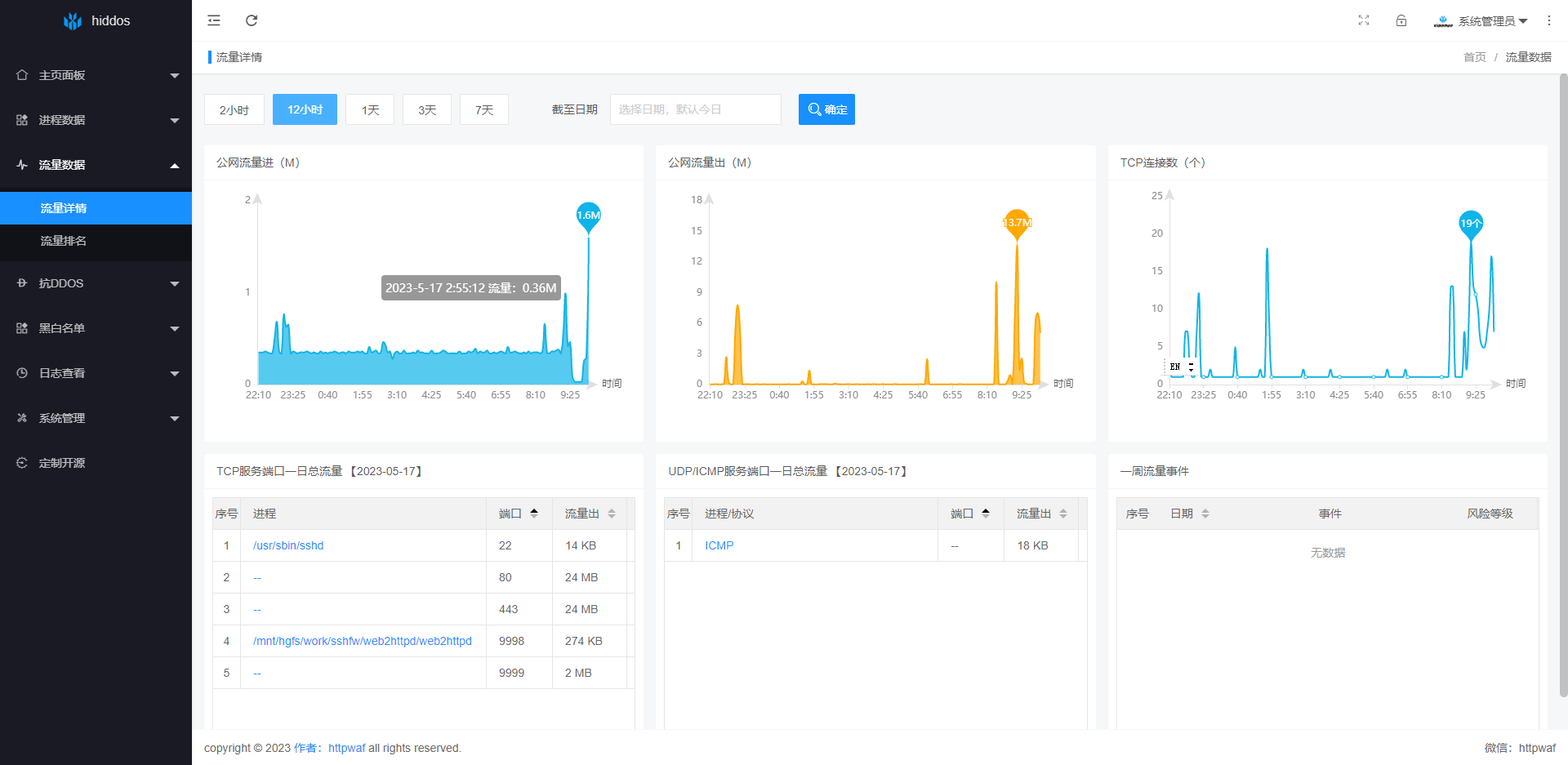
进程风控分析是综合利用机器学习、检测异常等技术检测包括流量异常、IP地址数量异常、IP地址区域异常和危险进程等。**需要至少运行学习7天才有数据**，比如系统在最近一段时间都没运行curl或者wget，一旦其运行，系统将报警高风险。有两种可能：

1. 系统管理员运行了curl或者wget下载，对系统做了高危操作或者配置。
2. 系统其他服务进程有未知漏洞被黑客利用，触发了curl下载黑客程序运行，非常危险。



## 流量数据

流量数据可以灵活根据2小时、12小时、1天、3天、7天等查询任意时段的流量数据，有异常的情况，会自动报警。



## 白名单进程/IP

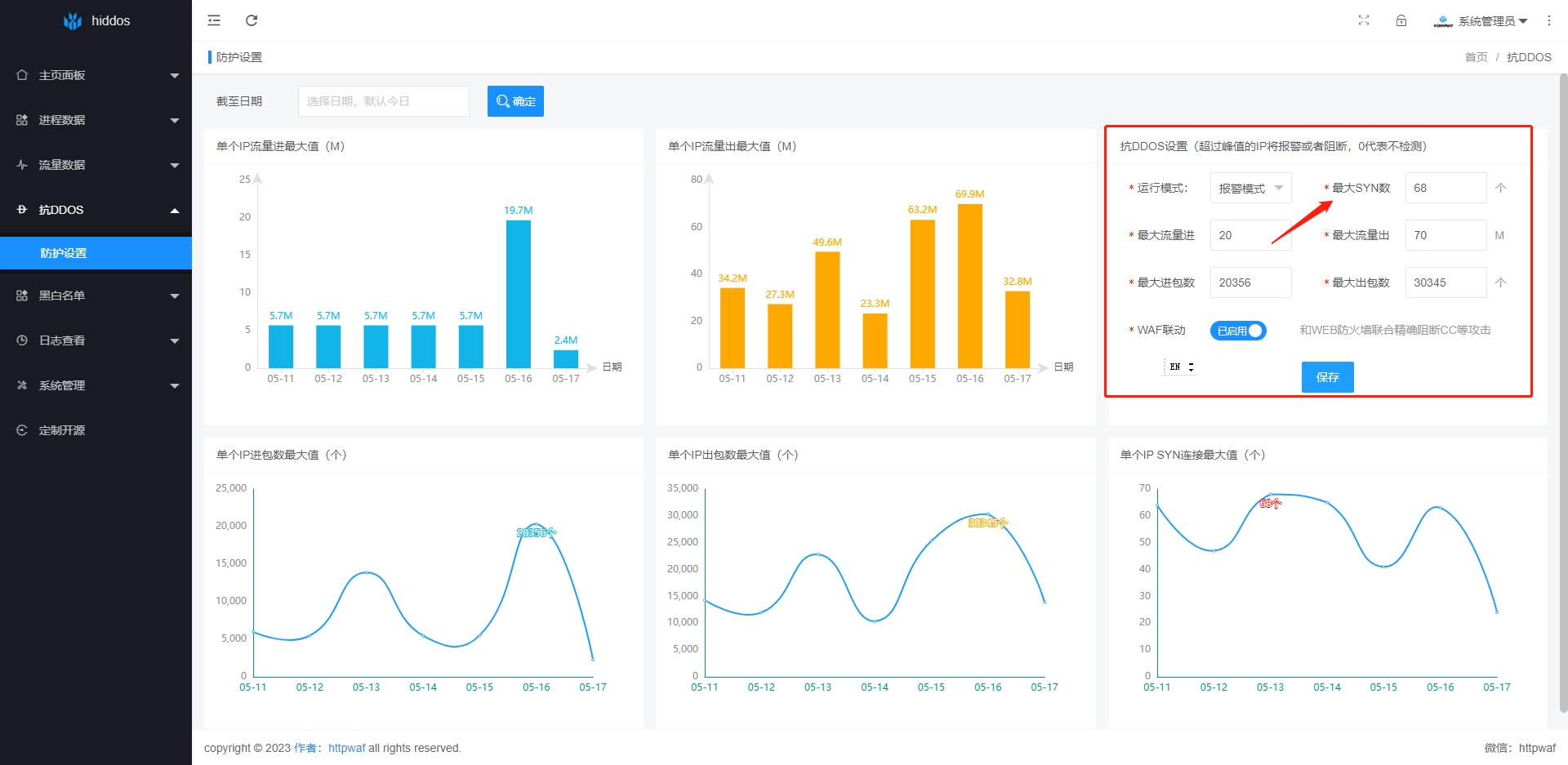
这里可以添加或者编辑仅仅允许运行的白名单进程联网，杜绝木马运行。但特别要注意sshd、web2httpd等系统服务进程要允许运行，必须完整的输入全部路径，精确匹配。

一旦设置错误，服务器将无法访问，后果特别严重，所以我们免费版本不提供这个功能。

## 黑名单进程/IP

黑名单是禁止某些程序联网，如wget等，以免未知漏洞调用。输入进程名称即可，字符串模糊匹配，不要输入路径。免费版本不提供阻断功能。

## 抗DDOS



DDOS防御会统计单个IP根据最近7天的各种峰值，生成各种DDOS防御参数，默认是报警模式，阻断需要人工介入精确设置各种参数。抗DDOS是本系统核心功能，一般来说，需要和上层如WEB应用防火墙联动，更能精确阻断CC或者DDOS。

## 日志查看

显示DDOS防御封杀的IP地址。

# 系统管理

## 远程管理



HIDDOS的9998端口默认允许任意IP访问(0.0.0.0/0)，为了保证安全，禁止向公网用户开放。最好在边界防火墙上配置9998端口的访问范围，如果在这里设置不正确，HIDDOS可能无法访问，会返回“hello word” 的禁止访问提示。

如果万一设置错误，解决方法是重装HIDDOS。

## 恢复出厂设置

如果做了错误的配置，可以用点击这个按钮，恢复到原始安装状态。

## 系统重启

某些情况下，如增加了自定义规则、替换了数字证书等，要重启才能生效。重启过程一般在几秒完成，重启后，务必刷新主页查看运行状态，显示正常代表配置正确。

# 开机启动

开机自启动请自行编写脚本启动hiddos程序，默认不会改动系统任何配置。

/hiproc/bin/hiddos daemon是以后台守护进程的方式启动。

# 开放源码

hiddos是业界极其少有的Linux进程防火墙+DDOS流量防护，可以大量降低DDOS防御费用，源码可以开放，付费和功能定制请加微信号httpwaf。



攻防乃顶级智商对抗，我们努力做最好用的各类应用防火墙，包括WEB应用防火墙、Linux 主机防火墙、数据库防火墙、物联网防火墙等等，**9998管理端口禁止向公网开放，勿谓言之不预也**。