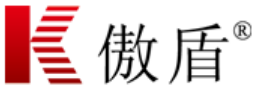
2019

用户手册

傲盾异常流量清洗系统



北京傲盾软件有限责任公司

文档版本　　190308-v5
发布日期　　2019-08-07
注意：
由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用

指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

文档修改记录

文档版本	修改说明	发布时间	作者
09-23	第一次正式发布	2011-09-23	2271
120701-v1	发布新防护插件	2012-07-01	2354
131125-v2	发布新防护平台	2013-11-25	2245
151015-v3	部分修正	2015-10-31	2776
170303-v4	发布新防护平台	2017-03-04	
180302-v5	发布新防护平台	2018-03-02	
190308-v5	发布新防护平台	2019-03-08	

版本说明

本手册适用于北京傲盾 ADC 系列异常流量清洗系统。

内容介绍

本手册主要介绍了北京傲盾 ADC 系列异常流量清洗系统的硬件特性、使用方法方式等。

在使用北京傲盾异常流量清洗系统之前，请仔细阅读本手册。

1 产品概述

1.1 概述

本文档介绍异常流量清洗系统的产品形态、系统架构、功能模块子模块组成、安装调试、需注意事项及系统的测试、运维等。

1.2 读者对象

本文档主要适用于以下读者：

- 期望了解本产品主要技术特性和安装方法的用户
- 系统管理员
- 网络管理员

本文假设读者对下面的知识有一定的了解：

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

1.3 获得帮助

傲盾官网

可以帮助用户获取最新的网络安全信息和傲盾安全产品信息。

网站：http://www.aodun.com.cn

售后服务

提供全国范围内的服务热线，可以帮助用户解决在使用傲盾产品和服务过程中遇到的各种问题和困难。

企业 QQ：3007263945　　企业电话：　010-82728052-880

技术资料

http://www.aodun.com.cn/techsolution_info/techsolu

投诉建议

邮箱：ceo@aodun.com.cn

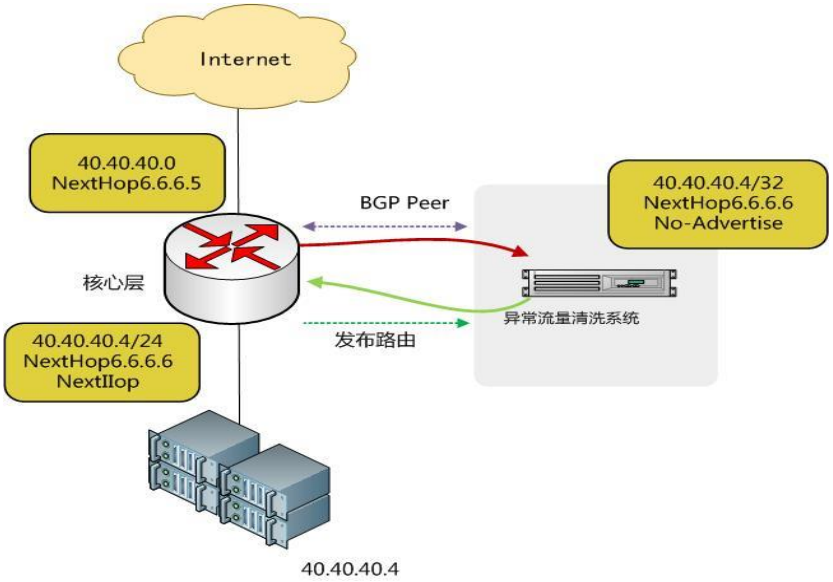
1.4 关于网络安全

随着计算机技术和通讯技术的飞速发展，网络正逐步改变着人们的工作方式和生活方式，成为当今社会发展的一个主题。网络的开放性、互连性、共享性程度的扩大，使网络的重要性和对社会的影响也越来越大。随着网络上电子商务、电子现金、数字货币、网络保险等新兴业务的兴起，网络安全问题变得越来越重要。计算机网络犯罪所造成的经济损失实在令人吃惊。仅在美国每年因计算机犯罪所造成的直接经济损失就达 150 亿美元。

国家计算机网络应急技术处理协调中心 2006 年共收到网络安全事件报告 64686 件，为 2005 年的 5 倍。其中对使用自动化程序与对服务器操作系统主动攻击占绝大多数。网络信息安全已经成为一个关系国家安全、社会稳定、经济安全、民族文化继承和发扬的重大问题。《数字化犯罪》的作者尼尔·巴累特高呼：互联网产生了一个“潘多拉”魔盒——计算机病毒、网络攻击、电子洗钱、网络诈骗等涉及网络的传统型或新型的违法犯罪活动层出不穷，对任何一个国家的网络信息安全都构成极大威胁。

1.5 产品实现概述

北京傲盾异常流量清洗系统可以采用串联部署，这时只需要设置好内外网口即可。当然也可以旁路模式部署在网络环境中，在服务器遭受 DDoS 攻击时，将服务器的流量动态的牵引到流量清洗系统来进行流量清洗。北京傲盾流量清洗系统利用 IBGP 或 EBGP 协议，首先和多个核心设备（直连或者非直连均可）建立 BGP Peer。攻击发生时，流量清洗路由模块通过 BGP 协议会向核心路由器发布 BGP 更新路由通告，更新核心路由器上的路由表项，将流经所有核心设备上的被攻击服务器的流量动态的牵引到流量清洗系统进行清洗。同时流量清洗中心发布的 BGP 路由添加 no-advertise 属性，确保清洗中心发布的路由不会被扩散到骨干网，同时在北京傲盾异常流量清洗系统上通过路由策略不接收核心路由器发布的路由更新。从而严格控制对骨干网络造成的影响。



2 产品特点

2.1 性能

- 系统可靠性

系统开发期间通过安全测试实验室对设备单个接口进行 10G 以上流量压力测试，以及异常流量清洗系统群集测试 50000 小时无故障运行，并支持双机热备，保障系统可 7×24 小时不间断运行。

- 系统安全性

整个系统通过旁路模式部署在网络中，各接口均无法被广域网访问，唯一被访问管理接口采用审核加密访问模式，传输数据均使用加密传输保障传输安全。

2.2 易安装

- 支持透明模式接入网络；
- 系统支持管理端口自定义；
- 系统支持双电源热备份。

2.3 灵活组网

- 通过动态路由旁路模式接入网络，不改变网络原有拓扑结构。
- 支持透明串联接入网络，不增加网络跳数，安装便捷。
- 支持混合组网模式，旁路、串联混合接入网络，适应性强。
- 支持单臂和双单臂旁路接入，为用户节省流量清洗成本。

2.4 操作维护方便

- 支持本地网络登录管理与维护
- 支持 Internet 网登录管理与维护，在有足够权限前提下
- 支持 IE、火狐、谷歌等主流浏览器登录
- 支持横向物理扩展防护能力

2.5 功能

- 数据流指纹检测过滤，防护各种已知与未知的 DDOS 攻击；
- 自定义特征码策略，可进行深层次、智能过滤包过滤；
- 2-7 层访问控制策略，支持下一代网络 Ipv6 协议簇，支持 Ipv6 协议下的 DDOS 攻击防护、深度包内容过滤；
- 路由协议模块，支持 RIPv2、OSPF、ISISv4、BGP4、RIPng、OSPFv3、ISISv6、BGP4+路由协议。多路回注方式支持， 支持原路回注、三层双路回注、策略路由回注、GRE 回注、MPLS 回注、MPLS L3 VPN 回注、双路原口回注、802.1Q VLAN 回注；支持回注 QOS；
- 支持旁路部署、串联部署、单臂部署、双单臂部署、混合部署等多种网络安装方案；
- 支持 DNS 智能防护；
- 数据包分析模块，智能 DATA 分析、TCP 连接分析、HTTP 分析，可以对捕获数据包进行深度挖掘；
- 日志模块,支持 SYSLOG 导出；支持 SNMP 设备监控；支持邮件告警；支持页面声光报警；
- 单 IP 流量监控；
- 实时访问连接监控；
- 权限管理功能，支持一次性口令，Radius 认证支持；
- 支持分布式部署，可以远程管理设备,监控网络；
- 智能防护插件模块，可自动防护 CC 攻击、UDP、ICMP、IP Flood 等攻击；
- 黑洞路由牵引策略功能，对超出定义策略阀值的 IP 实现在上层设备屏蔽；
- 域名过滤模块，支持域名黑、白名单功能；
- 支持 DNS 服务器宕机保护，DNS 域名黑白名单，DNS 随机域名防护，DNS 访问控制，DNS 域名劫持防护，DNS 缓存投毒，DNS 畸形报文访问等多种 DNS 服务器攻击防护手段。

2.6 管理

系统采用 web 来管理，建议使用谷歌或者火狐等优秀的浏览器。系统支持中英文。对于配置上管理 ip 的设备，通常是在本地浏览器中输入 http://IP:16010 就可以登录设备的管理页面。对于安全性需求较高的客户，系统同时支持 https 来登录。以 http 为例，登录方式如：http://192.168.69.199:16010，如下图：

输入初始账号密码 administrator　administrator 就可以登录系统，建议用户在初始上架好设备后及时修改默认密码，以增加系统安全性。在系统右上角位置进行修改，同时也可以编辑系统标志和超时时间。系统标志在浏览器标题栏中显示，通常可以添加单位名称。超时时间是指在用户登录管理平台后，若干时间内没有操作，系统就会自动退出当前管理平台，以增加系统安全性。如下图：

3 首页 – 全局状态

3.1 设备状态

设备状态：显示清洗系统当前实时输入和输出流量，输入和输出包数及清洗系统运行状态。

动态流量图：流量图实时显示当前业务流量大小。默认显示攻击流量和输入流量曲线。在集群环境中默认显示所有设备流量总和。用户可以过滤单台清洗设备所承载流量大小；

设　备：清洗系统群集中用于区分各台设备的 IP 地址与设备名称；

方　向：输入输出以服务器为立足点。输入表示经过该设备服务器接收的流量。输出表示经过该设备服务器向外发送的流量；

拦截前流量：未经清洗系统数据处理前总流量；

拦截后流量：经清洗系统防护完毕后总流量；

包　数：流经清洗系统总包数个数；

系统负载：显示清洗系统 CPU 使用率与系统内存剩余量。

日攻击类型分布图：统计每日攻击类型占百分比

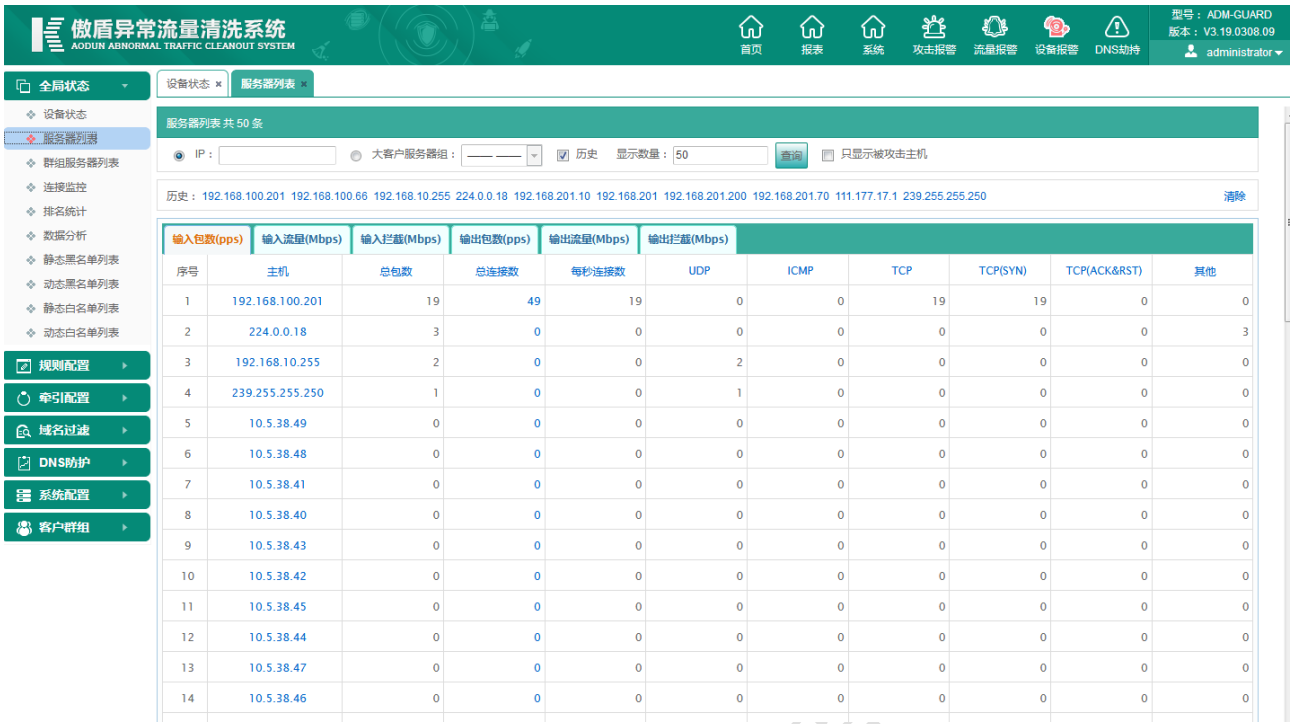
日攻击服务器 TOP 分布图：统计每日服务器攻击次数

攻击告警：当 ip 正被攻击情况下，会提示被攻击 ip、攻击类型、拦截峰值流量

全局信息：能查看设备总静动态黑域名和 ip 黑白名单、域名监控联动开关、以及规则使用激活情况

3.2　服务器列表和群组服务器列表

服务器列表：监控清洗系统下所有的服务器实时状态，可详细监控到清洗系统下所有 IP 的输入包数、输入流量、输出拦截、输入拦截、输出包数、输出流量。支持**顺序排列**，管理员可通过点击主机、总包数、UDP、ICMP、TCP 等，来完成顺序排列，进入服务器列表时，会优先显示被攻击 IP。或者勾选只显示攻击主机，那么设备只会把实时被攻击的 ip 显示统计出来。



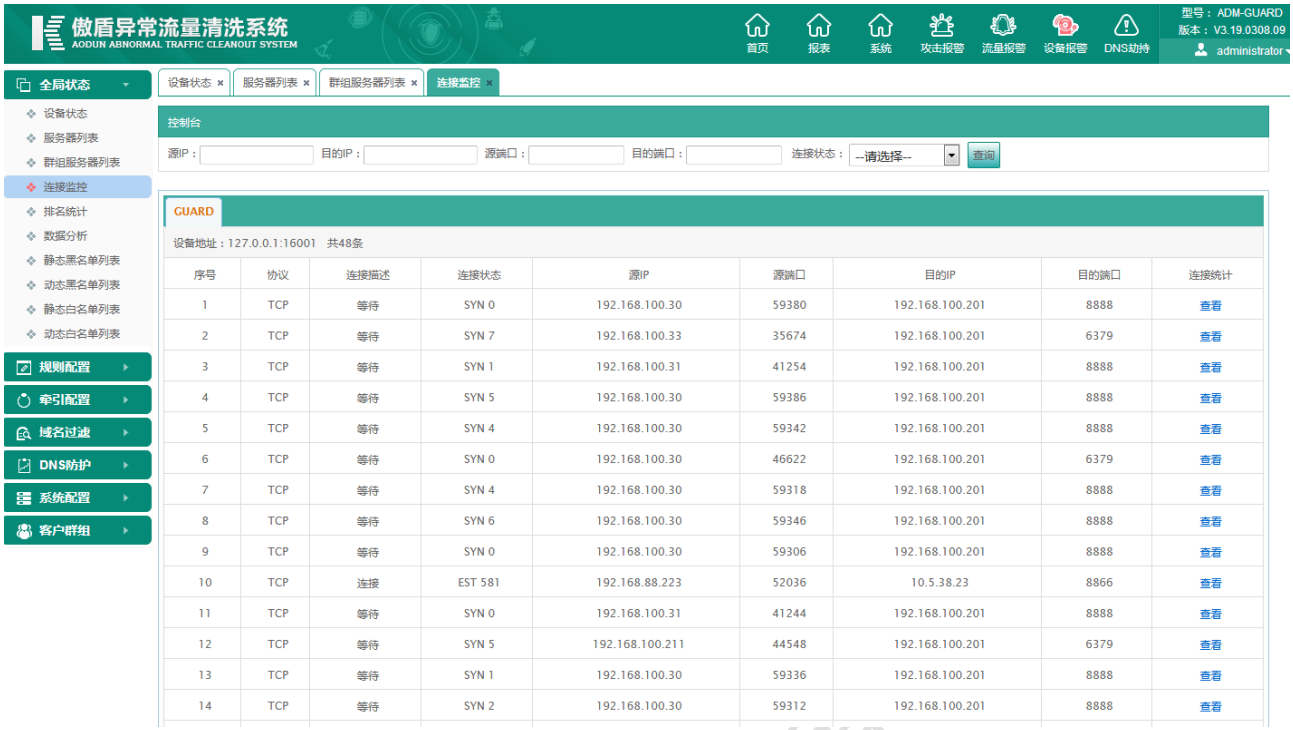
单个或多个 IP 输入包数或输入流量异常增大，可能是此 IP 遭受网络攻击，可对该 IP 抓取数据包分析，设置相应的防护规则实现攻击拦截。

服务器群组列表：通过创建一个群组，把某个大客户的服务器 IP 关联进来，便可以在群组服务器列表中单独显示该用户的所有 IP。

还可以搜索单个 IP，查看此 IP 的输入包数、输入流量、输出拦截、输入拦截、输出包数、输出流量

3.3 连接监控

连接监控：被保护区域内所有 IP 连接实时状态显示。亦可在控制台通过源 IP、目的 IP、源端口、目的端口、连接状态进行条件查询。



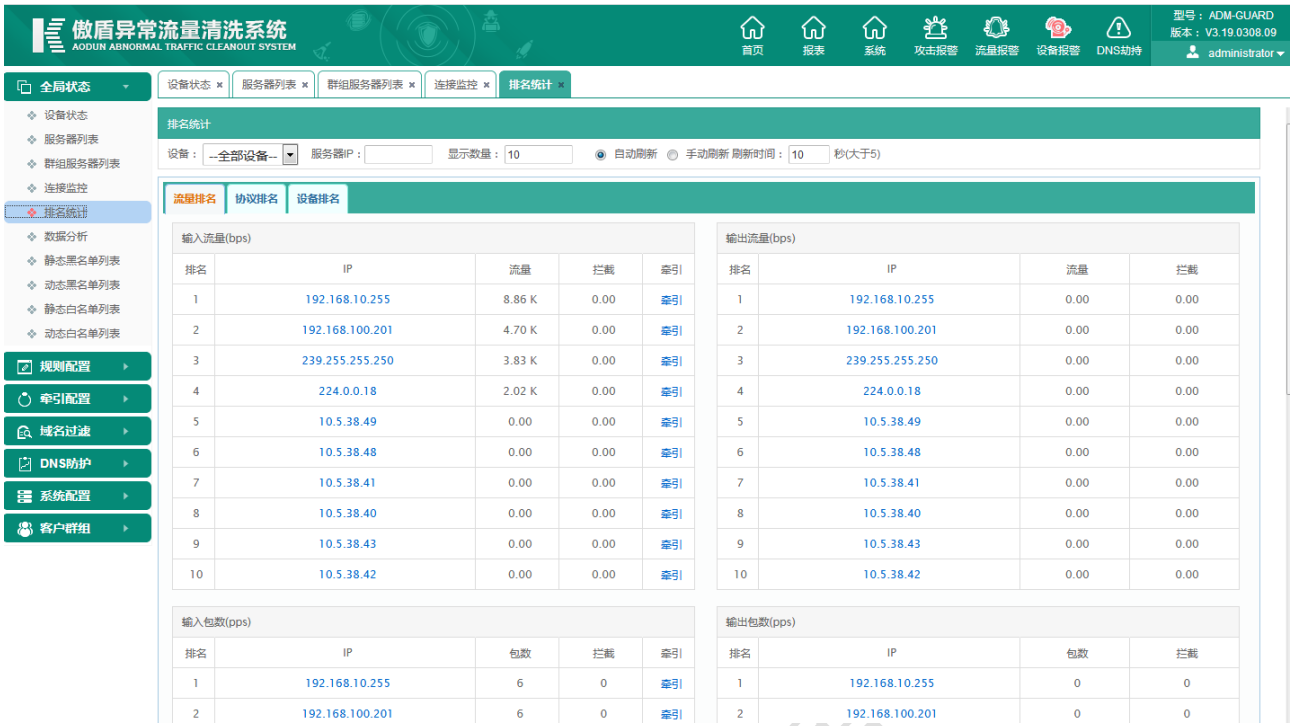
3.4 排名统计

排名统计通过流量排名、数据包排名，快速查询（默认显示前 10 名），并可对异常流量快速牵引导入黑洞路由，避免巨大流量攻击使网络瘫痪。可通过设备、服务器 IP 来精确查询；可调整显示数量（默认为十个 IP）；有自动刷新和手动刷新两种模式；其中，自动刷新可以自定义刷新时间

流量排名：分别按照每 IP 的输入流量和输出流量、输入包数和输出包数、输入连接数和输出连接数的多少进行排名。

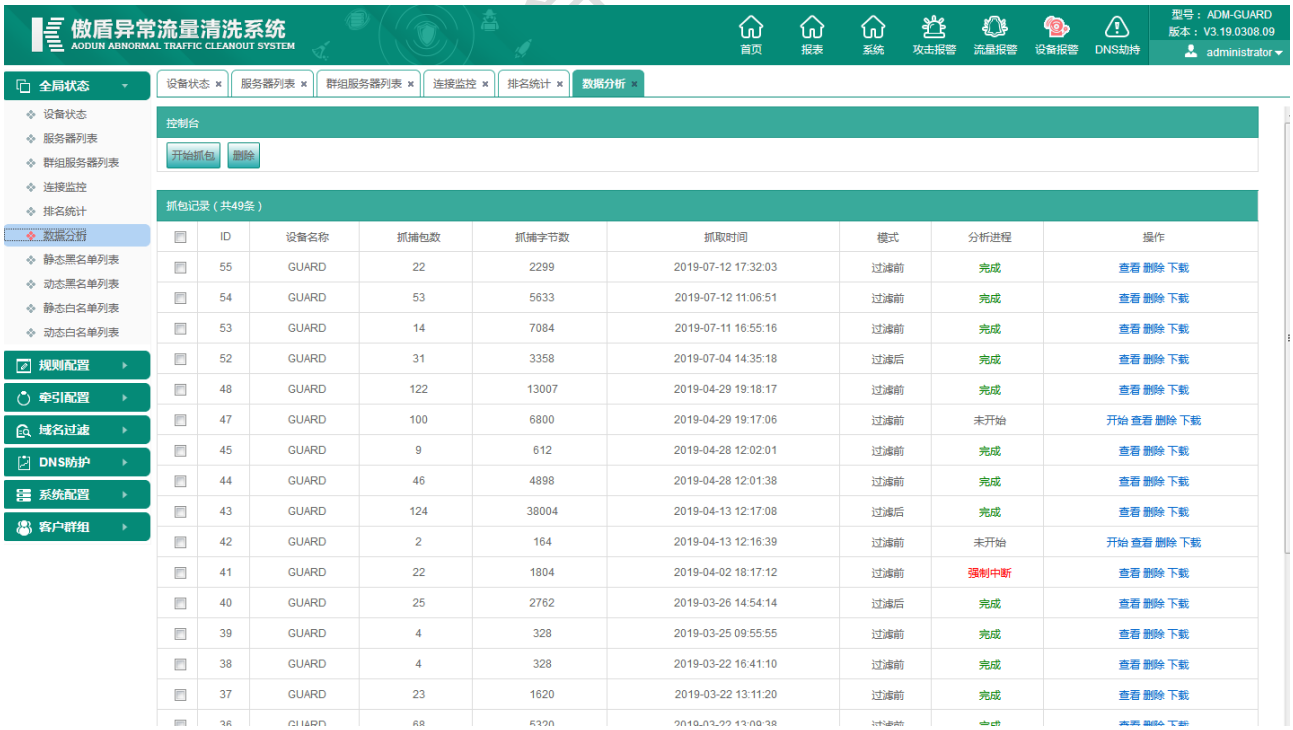
协议排名：可以选择 UDP、ICMP、TCP、TCP（SYN）、TCP(ACK&RST) 、OTHER 几种协议，按照每 IP 的输入流量和输出流量、输入包数和输出包的多少进行排名。

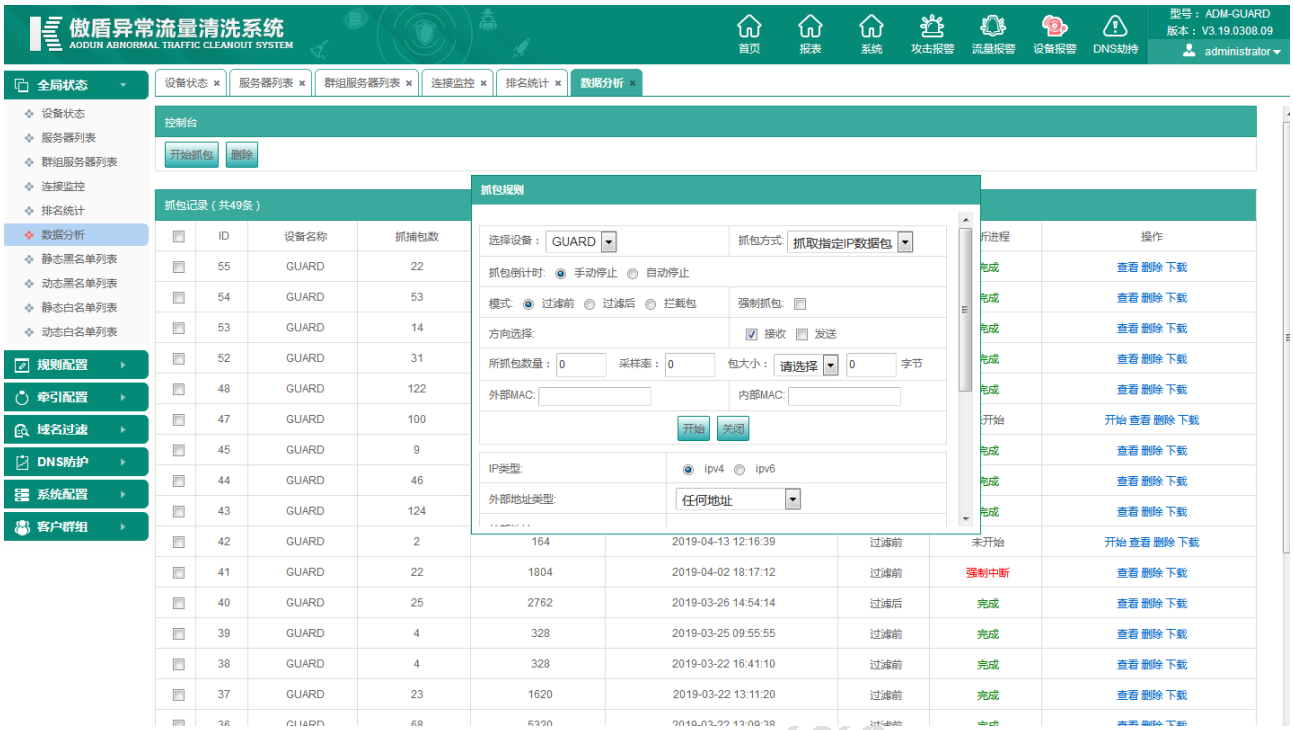
设备排名：分别按照每设备输入流量和输出流量、输入包数和输出包数、输入连接数和输出连接数的多少进行排名。



3.5 数据分析

通过抓包功能，在服务器遭受攻击时抓取攻击流，分析其特征，定制特定的规则来提供定制化的过滤防护。





点击开始抓包，则进入抓包规则设置：

选择设备：用于在集群环境下，在指定设备上抓取攻击流；

抓包方式：抓取指定 IP 数据包表示被保护区域内具体服务器 IP 的数据；抓取所有包表示流经清洗系统所有数据包；

抓包倒计时：分两种，一种默认手动停止，另一种自动停止，填写指定时间自动停止抓包

模　　式：过滤前表示数据流没有经过任何防护模块过滤；过滤后表示经过清洗设备过滤模块清洗的流量；拦截包表示数据流被防护模块拦截后的流量

强制抓包：多人同时抓包时，有可能产生冲突而无法正常抓包，可以勾选强制抓包来抓取；

所抓包数量：采样率、包大小、字节可自定义，抓所需要的数据包

方向选择：默认勾选接收方向，即表示本地服务器输入的方向；发送表示服务器输出的流量；

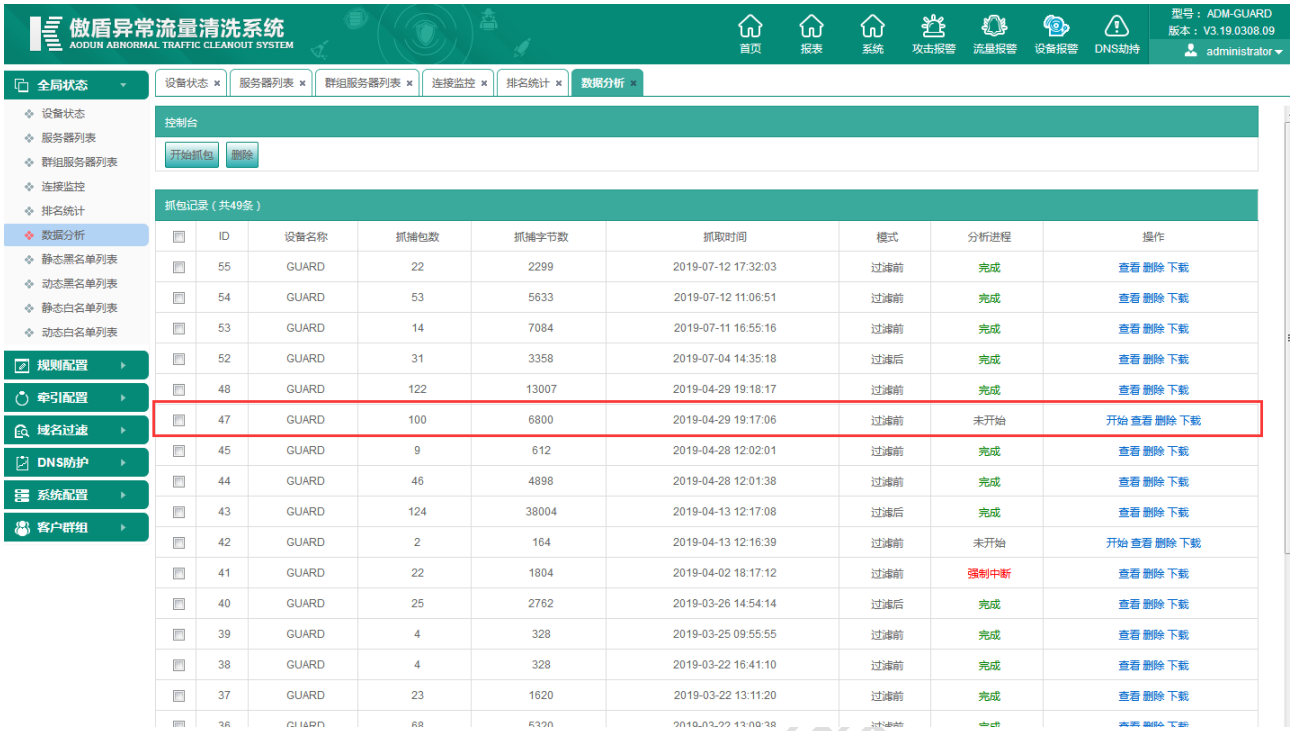
外部地址类型：默认抓取任意外部 IP 发往服务器的流量。支持抓取单个外部地址和范围地址发给服务器的流量；

内部地址类型：本地服务器 IP，支持单个和范围地址；

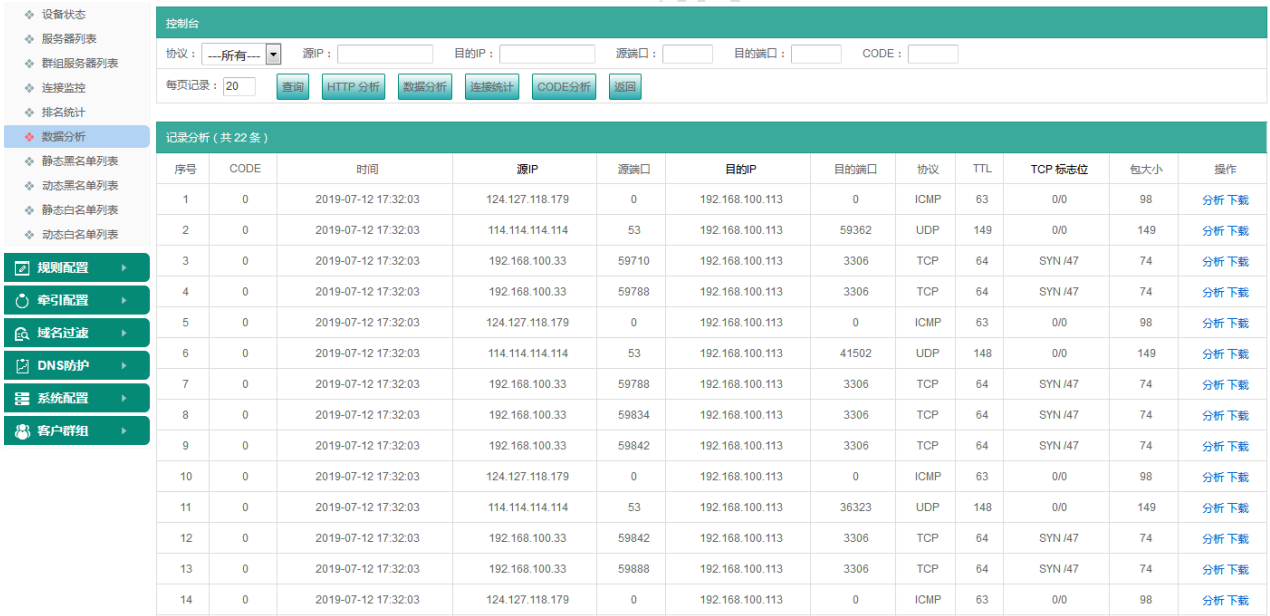
协议类型：IP 表示所有类型的包；另外可细分为 TCP、UDP、ICMP、IGMP 和 other 类型的包。

3.5.1　记录分析

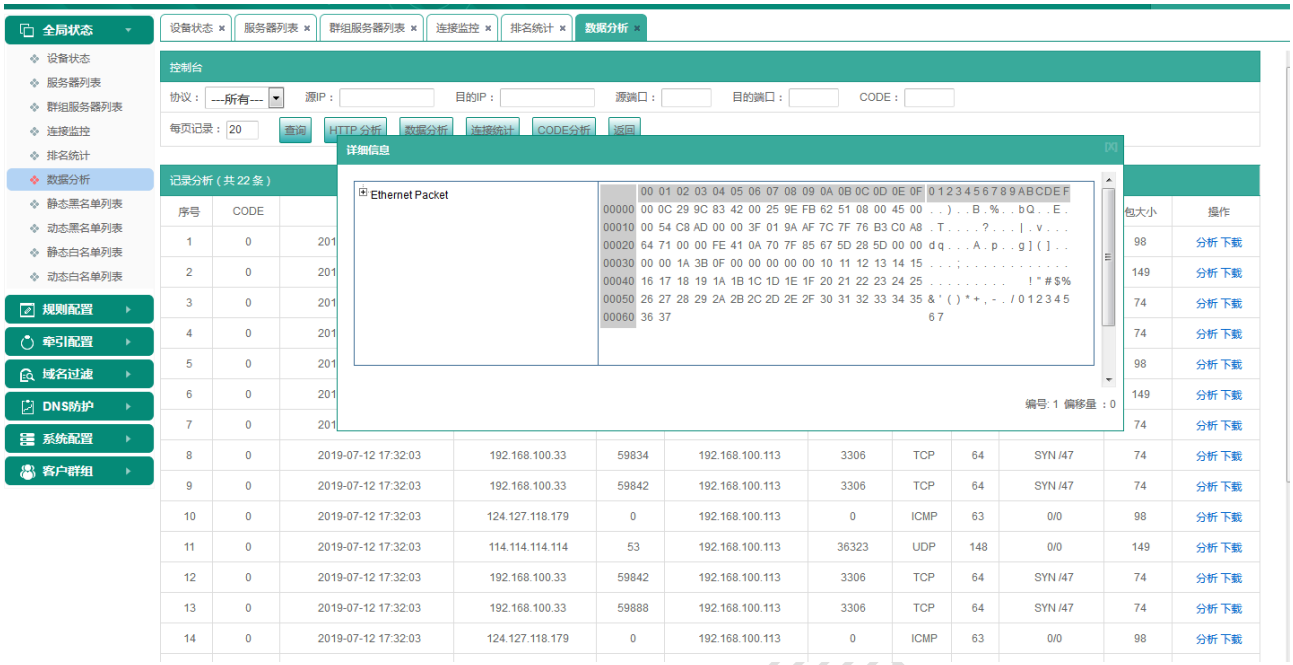
正常的抓完一个包，系统页面上显示的是未开始状态，需要手动点击**开始**按钮进行分析：



开始成功后，点击**查看**就会看到下面的分析结果。默认显示抓取时间、源 IP、源端口、目的 IP、目的端口、协议、TTL、TCP 标志位以及包大小。



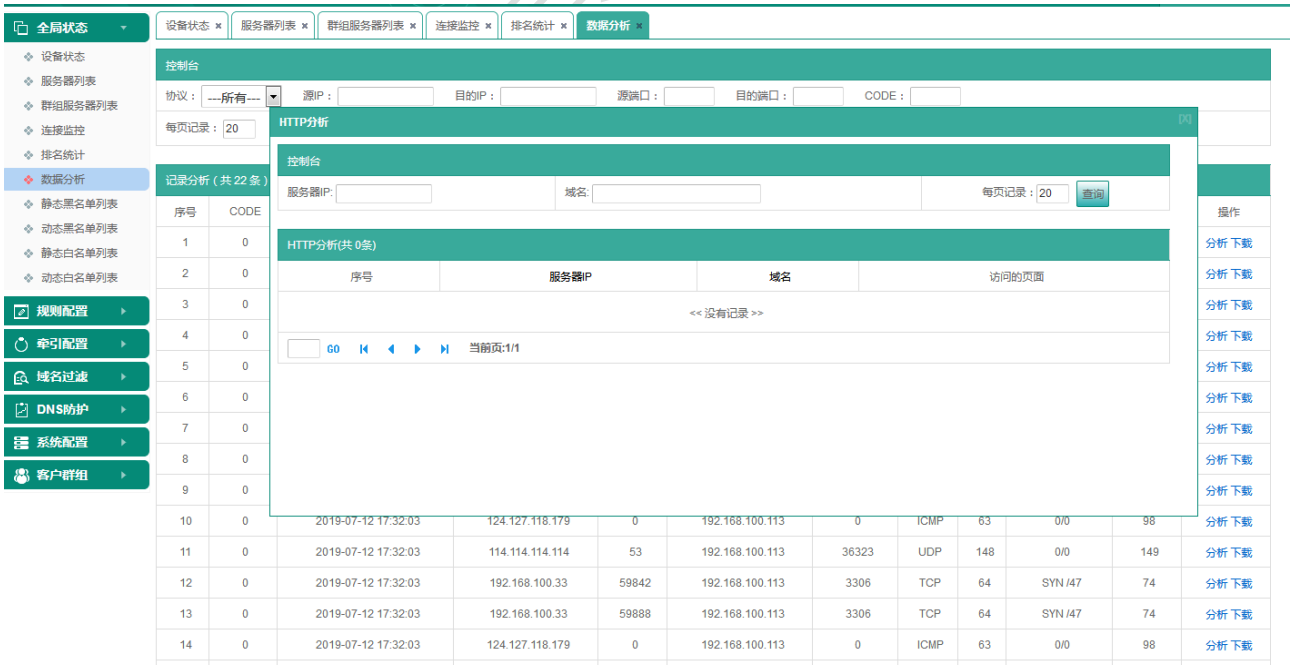
3.5.2 数据包分析



点击图中操作栏【分析】，进入数据包详细信息，进一步查看数据包的内容。

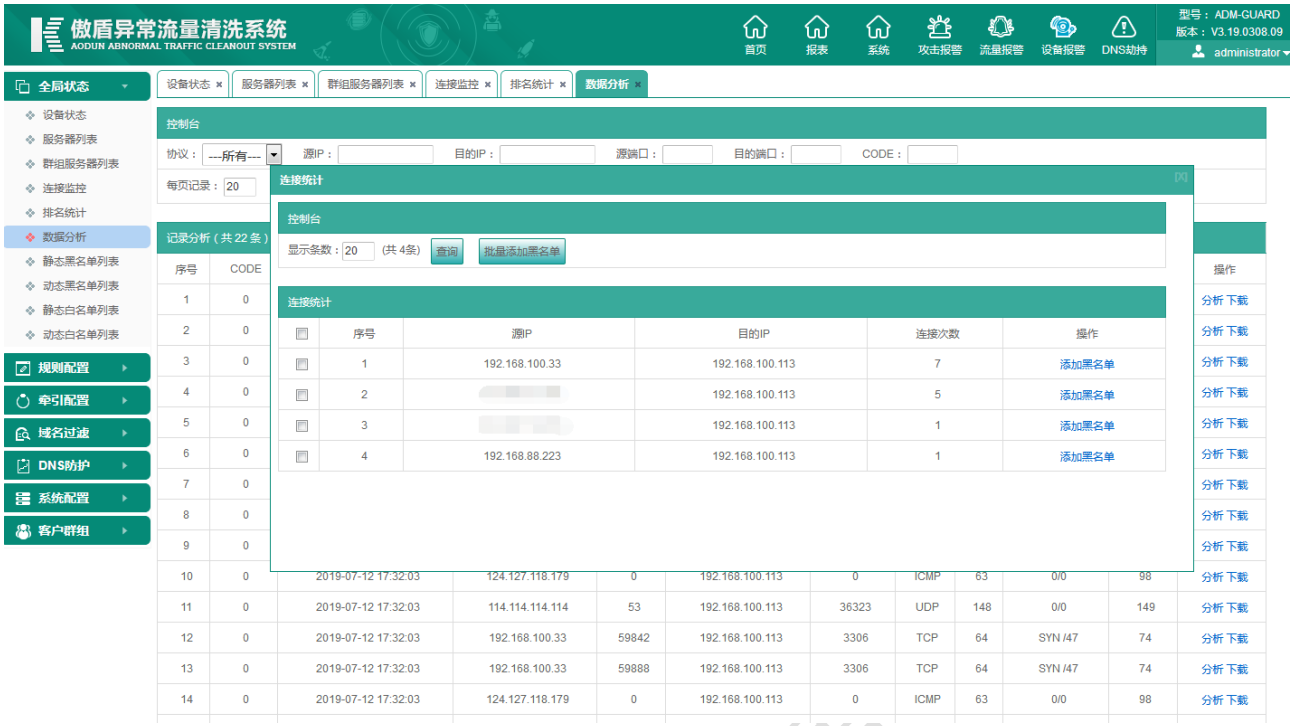
3.5.3 HTTP 分析

HTTP 分析:用于分析客户端所访问的服务器应用层数据，可以查看域名、URL 等处。可以在控制台输入服务器 IP、域名进行条件查询，亦可进行每页记录条数调整。



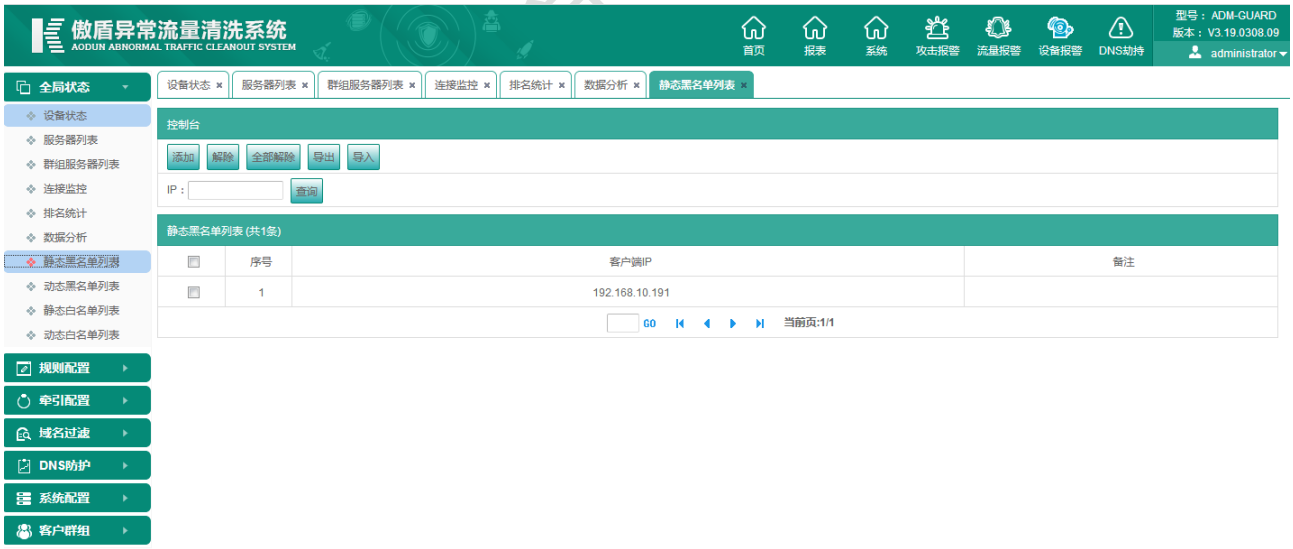
3.5.4 连接统计

连接统计会列出本次抓取数据包中源 IP 连接服务器的次数，可以快速定位到连接形攻击的源地址，并支持把相应源地址中入黑名单中。



3.6 静态黑名单列表

黑名单列表中的 IP 为不受信任的外部客户端 IP 地址，可由管理员手动添加、解除、全部解除、导入、导出。列表中的客户端 IP 防火墙将直接将通信数据丢弃。



3.7 动态黑名单列表

动态黑名单中主要是没有被防火墙规则验证通过的外部 IP，在此列表中的 IP 地址外部无法访问

本地服务器。通常规则中会设置一个拦截时间，该时间值会动态递减到 0，系统会自动释放该外部地址。

通过添加被封 IP、服务器 IP、阻止时间，管理员可以在某个服务器上加黑指定外部 IP，在该时间递减到 0 时，系统会自动释放，支持导入导出。

【按被封 IP 解封】：勾选黑名单列表中相应的外部 IP 条目，可以只解封该外部 IP。

【按服务器解封】：勾选任意一条含有指定服务器 IP 的黑名单记录，可解封所有在此服务器加黑的外部 IP。

【全部解封】：解封掉所有被防火墙拦截的外部 IP。

3.8 静态白名单列表

静态白名单列表中的 IP 为受信任外部客户端 IP 地址，可由管理员手动添加，亦可通过 IP 进行查询。可进行导入导出，导出的文本可以用于导入列表中的客户端 IP 与本地服务器的通信不会被防火墙检查，并且白名单优先级高于黑名单优先级，提醒管理员谨慎添加。

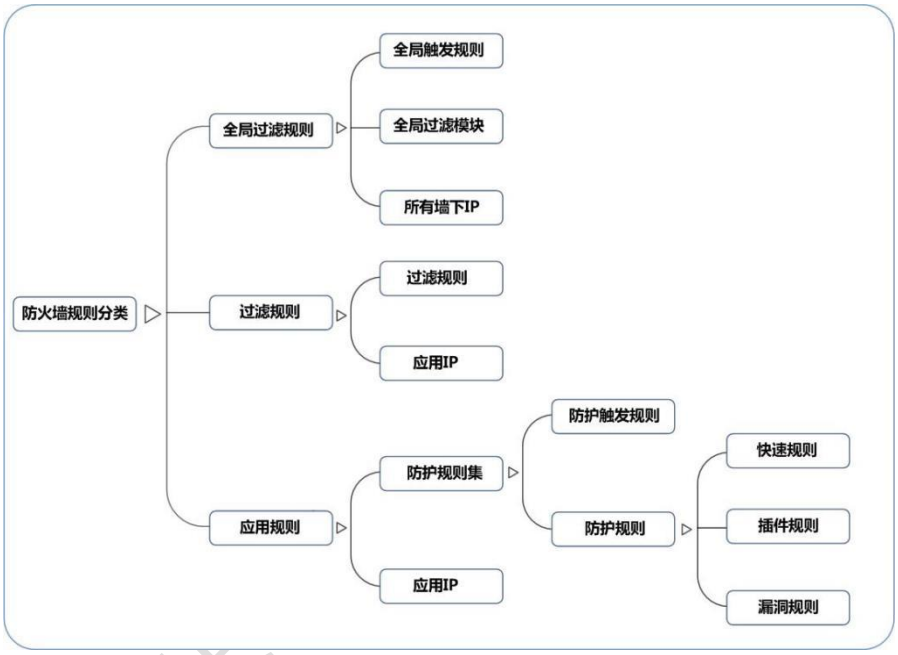
3.9 动态白名单列表

动态白名单中添加的 IP 是由系统的 CC 插件验证添加或者自定义规则添加的。可以导出但是不能导入。当服务器添加 CC 防护后，经过插件验证通过的 IP 会被添加到这里，信任时间会从 10000s 递减。在本次验证通过后，CC 插件将不会对信任的源 IP 进行验证。系统同时又支持按客户端、服务器的解除功能，解除后的客户端在触发 CC 插件后，会进行再次验证。支持按信任 ip 和按服务器列表查询。

4 首页 - 规则配置

清洗系统集成数据流指纹过滤模块，不添加任何防护规则情况可主动防御 SYNFlood、ACKFlood、UDPFlood、ICMPFlood、TCPFlood、No-Standard-ProtocolFlood 等常见的 DDOS 攻击。而本章要介绍的规则配置模块则是傲盾清洗系统的一个特色功能，支持用户自定义防护规则。面对各种变种攻击，管理员可采用自定义规则模块根据业务模型或者攻击特征，针对性的添加规则防护，过滤掉异常的流量，从而保证服务器正常提供服务。

清洗系统规则体系可分为三个类别：全局过滤模块、过滤规则及应用规则。规则分类如下图：

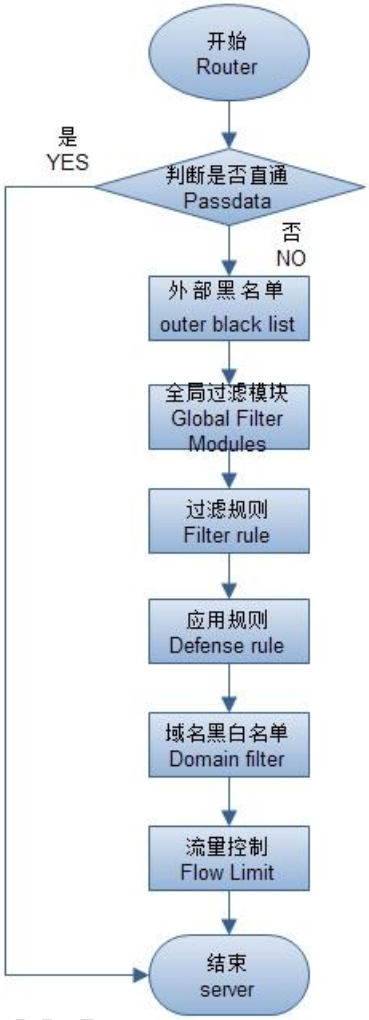


全局过滤模块：由全局触发规则及全局过滤模块组成，默认应用于墙下所有服务器。全局过滤模块在清洗系统出厂时已固化，无需用户单独定义。可以过滤 synflood、ack flood、UDP Flood、ICMP Flood、No-Standard-ProtocolFlood （非标准协义泛洪攻击）等常见 DDOS 攻击。

过滤规则：由过滤规则和应用 IP 组成，类似交换机的 ACL 功能，用以实现简单而直接有效的访问策略。如拦截外部某 IP 对墙下 IP 的访问；拦截服务器某一端口的输入数据；封掉墙下某一服务器某种协议的数据等。

应用规则：由**防护规则集**及本地服务器 IP 组成。**防护规则集**是傲盾清洗系统灵活性体现，它由一条防护触发规则及若干条防护规则组成，可实现功能强大的过滤策略。如数据包内容特征码匹配建模、数据流标记、CC 插件防护、智能 DNS 插件防护等功能强大防护策略。在添加应用规则还可以设置直通功能，设置直通的服务器，防火墙会直接转发该服务器的输入与输出流量，不做任何过滤，而此时添加在该服务器上的规则休也全部失效。

清洗系统数据过滤流程：



数据包进入清洗系统后，清洗系统会首先判断其访问服务器是否设置有直通规则。对于设置直通的服务器，清洗系统直接转发该服务器的入向与出向数据流，不做任何过滤。否则交由外部黑白名单模块处理。如果外部 IP 在黑名单中，清洗系统会拦截其数据流，其余部分流量接着向下转发。如有外部 IP 在白名单中，则直接将此 IP 发送的数据流交给本地服务器。全局过滤模块采用傲盾特有的数据流指纹识别技术对接收的数据包进行过滤，在这里，常见 DDOS 攻击数据将被识别和丢弃。通过全局过滤模块的数据包将被送入过滤规则进行过滤，过滤规则对数据包进行简单有效的过滤。对于放行的数据包则会转入应用规则模块过滤。域名插件主要用于协助管理员对本机房域名进行审查，所有本机房备案与未备案的域名是否能被外网访问，将会在这里得到控制。流量控制模块则会对最终流向服务器的数据流进行最终的流量限制,最后转发至服务器。

4.1 触发规则

触发规则分为全局触发规则和防护触发规则，前者服务于全局过滤模块。防护触发规则主要用于与一条或多条防护规则结合，形成防护规则集，防护触发规则为规则集中防护规则的启用前提条件。可以简单的理解为防护触发规则为防护规则的开关。支持导入导出。

- 全局触发规则

全局触发规则位于**规则配置 →触发规则 →全局触发规则**。是全局过滤模块的触发条件，按协议包数来设置，如果给某一项设置为 0，则表示该协议不会被触发。内容如下图：

每秒 TCP 包数：全局 TCP 过滤模块包触发值，表示单一服务器每秒接收的 TCP 数据包数超过所设置值时，发往该服务器的 TCP 数据将被全局 TCP 过滤模块分析过滤；

每秒 UDP 包数：全局 UDP 过滤模块包触发值，表示当墙下单一服务器每秒接收的 UDP 数据包数超过所设置值，发往该服务器的 UDP 数据将被全局 UDP 过滤模块分析过滤；

每秒 ICMP 包数：全局 ICMP 过滤模块包触发值，表示当墙下单一服务器每秒接收的 ICMP 数据包超过设置值时，发往该服务器的 ICMP 数据将被全局 ICMP 过滤模块分析过滤；

每秒 SYN 包数：全局 SYN 模块的包触发值，表示当墙下单一服务器每秒接收的 SYN 数据包数超过所设置值时，发往该服务器的 SYN 请求将由全局 SYN 过滤模块代理接管；

SYN 防护最大值：清洗系统单台墙 SYN 防护值的上限，超过此数值的 SYN 包将被丢弃；

SYN 严格防护触发数：全局 SYN 模块严格防护模式触发值。置为 50000 表示当每秒全局 SYN 模块代理接管的 SYN 请求数超过此阀值时，处于接管状态的所有服务器所接收的 SYN 数据包将被全局 SYN 模块以严格模式分析过滤；

每秒 ACK&RST 包数：全局 TCP 过滤模块包触发值，置为 10000 表示当墙下单一服务器每秒接收的 ACK&RST 数据包包数超过 10000 个时，发往该服务器的 ACK&RST 数据将被全局 TCP 过滤模块分析过滤；

每秒其它协义包数：以上未定义所有其他协义的全局过滤模块的触发值。

方　　向：触发值对应的数据识别方向，默认选择服务器接收方向。

- 防护触发规则

清洗系统出厂时已经集成部分防护触发规则，可供管理员直接使用。管理员可根据策略需要自行定义新的触发规则。防护触发规则跟全局触发规则稍微不同，如下图。每一项内容的含义跟全局触发规则是相同的。

4.2 防护规则

防护规则包含快速规则、插件规则、漏洞规则以及攻击检测规则。它定义了一系列包过滤的条件。

快速规则是漏洞规则的简化版本。插件规则为傲盾安全实验室开发的封闭规则，管理员无法读取到规则核心内容，调用插件规则时，只需要给该插件传递相应的参数即可。攻击检测规则默认出厂开启，为了在攻击日志中不同攻击情况下自动判断记录是什么攻击，给客户更直观体现出来。

漏洞规则中定义了一系列包内容匹配条件与动作，用户在定义好匹配条件与动作后，数据包在

经过漏洞规则过滤时，就能根据用户定义的条件去筛选报文，对匹配上的报文执行管理员定义好的动作。漏洞规则添加如下：

名　　称：给该规则命名，方便用户在添加规则集的时候查找；

协议类型：表示该规则应用于指定协议类型的数据包。IP 表示所有协议。

子规则组编号：系统会给规则分配一个编号。通常由系统自动分配即可。

添加子规则：漏洞规则中的匹配条件与动作是在子规则中定义的：

名称： 填写本规则的名字

备注： 填写本规则的备注信息

强制同步：抗拒绝服务系统在出现数据没有同步时候一个操作，该功能多用于有多台墙做集群的网络环境

按每连接匹配： 匹配数据按照建立的连接匹配

按每 IP 匹配： 匹配数据按照源 IP 匹配

IP 记录保存时间：访问 IP 分配一个记录来保存这个 IP 的相关数据，设置这个数据保存的时间

接收数据、发送数据： 设置本规则过滤的抗拒绝服务系统接收还是抗拒绝服务系统发送的数据特征码的比较设置如果值为空时不比较直接通过执行下面的逻辑关系比较

逻辑关系值： 匹配包特征码 时用的逻辑关系 = 等于、 <> 不等于、 >大于、 <小于、 >= 大于等于、 <=小于等于 ，注意只有本特征值 匹配时才会判断下面的条件

十六进制、字符：值的类型，十六进制 或字符，十六进制 0 到 F 表示的时候必须两位数字代表一个字节，比如 000F1B 中间不能有空格

从 TCP 数据开始搜索、数据包位置： 这两个参数决定从数据包的什么位置开始搜索，比如选择了从 TCP 数据开始搜索 ，数据包位置 10 抗拒绝服务系统分析数据包的时候就会从 TCP 数据包的数据部分 加上 10 的位置 开始搜索输入的值， 如果不选择从 TCP 数据开始搜索 就从数据包开始部分 加上 10 的位置 开始搜索输入的值

搜索整个包、搜索长度： 这两个参数决定数据包搜索的长度，如果选择搜索整个包，搜索值的时候就会一直搜索到数据包尾，这时搜索长度将不起作用，如果不选择 搜索整个包 就会搜索 指定的搜索长度

判断标志位为真： 与设置标志位、清除标志位、配合使用 比如攻击多特征码，第一个特征码符合的时候设置标志位 ID1 为真第二个特征码符合时 设置标志位 ID2 为真，通过组合 可以完成复杂的规则 刚从黑名单释放 ID8 会设置为真

判断累加器： 与累加器清零、累加器增加 配合使用，记录特征值出现次数或者其他需要累加计数的地方

值出现次数： 按单个数据包时 记录单个数据包里特征值出现的次数 选择按连接则记录整个连接过程值出现的次数，这个功能按每连接匹配 按每 IP 匹配都可以

数据包大小： 与包字节清零、开始累加包字节配合使用通过这个功能可以判断包字节异常的攻击，也可以做限制流量用按单个数据包只是简单的比较单个数据包大小 。特征码比较和逻辑关系比较匹配或者不匹配时执行的针对本数据包的操作

条件匹配： 上面特征码值 和 逻辑关系比较都通过后执行的操作 <通过><拦截><继续子规

则〉继续执行后面的子规则〈跳出本规则〉执行下一个规则

条件不匹配： 特征码值 和逻辑关系比较 只要有一个不匹配则执行 条件不匹配〈跳出本规则>跳出本规则执行下一个规则〈继续后面第几个子规则>继续执行后面的第几个子规则。特征码比较和逻辑关系比较匹配时的操作

加入黑名单： 加入黑名单列表把 IP 封了

加入外网、加入内网： 选择加入外网黑名单 封的是客户端也就是访问服务器的 IP ，如果加入内网黑名单 封的是服务器的 IP

发送 RET 包：针对 TCP 协议使用的，给服务器发送一个 RET 包用来释放连接

只对被封时访问的服务器有效： 如果不选择 被封的 IP 将无法访问抗拒绝服务系统下所有的服务器，如果选择上这个选项 只对被封时访问的服务器拦截；

按客户端 IP 计算：值出现次数、判断累加器按照客户端 IP 计算

按服务器 IP 计算：值出现次数、判断累加器按照服务器 IP 计算

比较值匹配就执行设置操作：选择如果比较的特征码值匹配就会执行下面的设置操作；如果没有选择，必须特征码比较和罗机关系比较都匹配时执行下面的设置操作

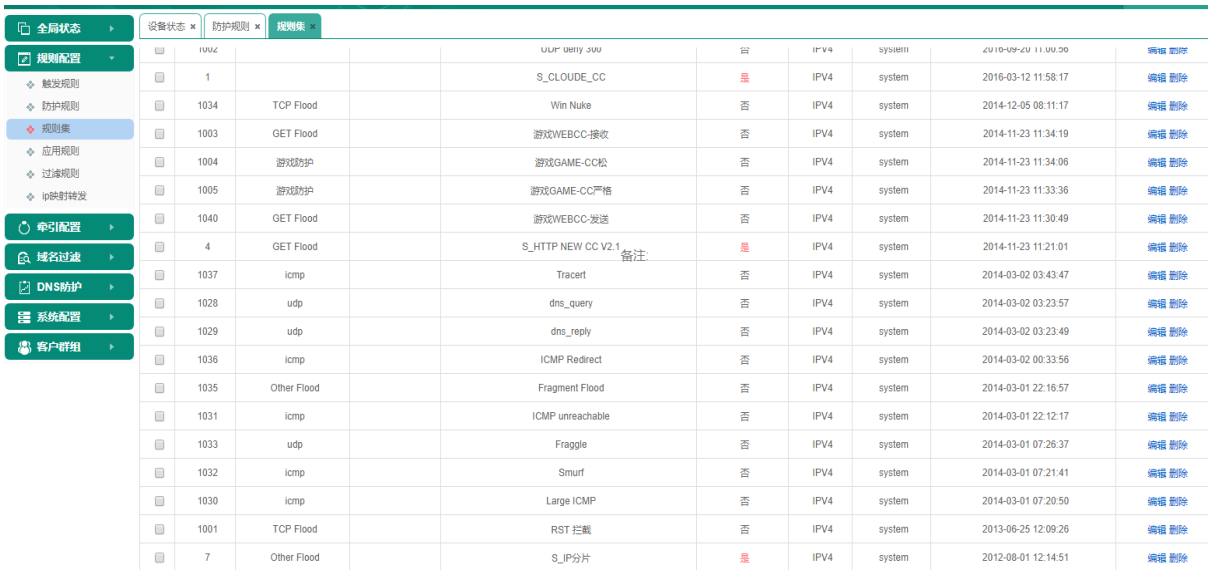
累加器清零、累加器增加： 用来和判断累加器配合使用

设置标志位、清除标志位： 用来和判断标志位配合使用

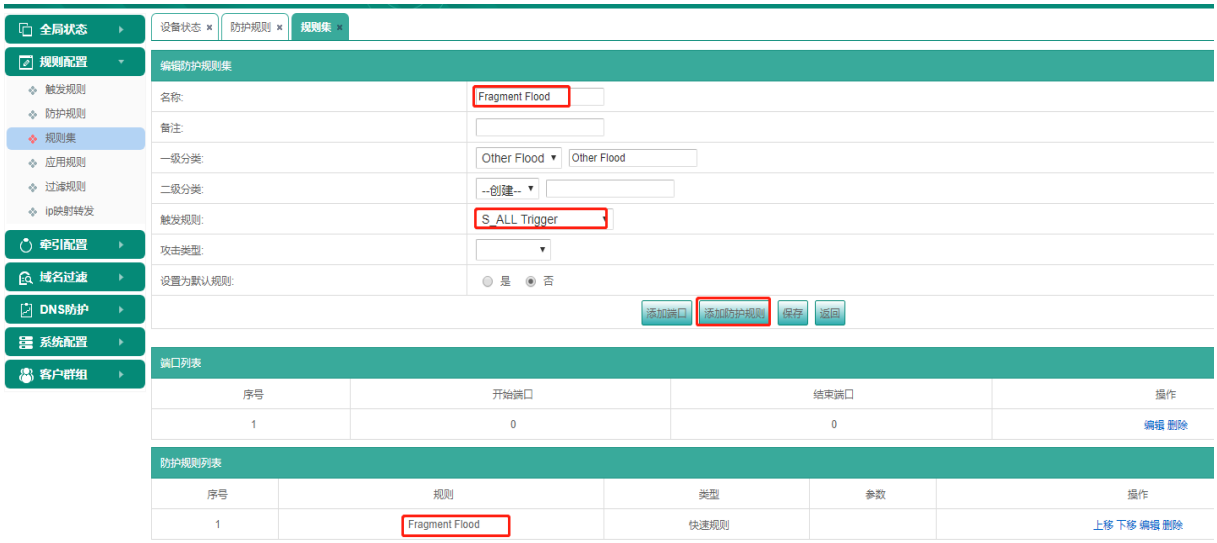
包字节数清零、开始累加包字节： 用来和数据包大小配合使用

4.3 规则集

规则集是由触发规则和防护规则组成。根据特定场景做的规则集，我们把它添加到指定服务器 IP 上，就可以实现在该 IP 上针对特定场景的攻击防护。系统上默认集成了一些常用的规则集，方便直接使用。支持导入导出。



添加规则集，就是把我们所需要的触发规则跟防护规则关联在一起，如下图：



名 称：定义规则的名称。

备 注：对规则添加说明，可选。

一级分类、二级分类：可以对新建的规则集进行分类，可选。

触发规则：选择合适的触发规则进行添加，必选。

攻击类型：给规则集添加攻击类型，如 SYN CC UDP ICMP。可选。

添加端口：设置规则集防护的端口。默认的是起始端口 0 到结束端口 0，表示全部端口生效。

添加防护规则：添加防护规则中的漏洞规则、插件规则、快速过滤规则。在添加插件规则时，可以在这里直接输入插件参数。如下图：

4.4 应用规则

应用规则就是在一个或者多个连续的 IP 上添加防护规则集，过滤异常流量。应用规则的添加有两种方式，第一种是直接在【应用规则】选项中添加。添加完成的策略支持交换编号、禁用/激活、删除。

第二种就是在服务器列表中找到需要添加防护的服务器 IP，过滤出此 IP 后，点击该 IP 会弹出添加规则的对话框，如下图：

点击应用规则处的添加，添加防护规则集：

服务器 IP：需要防护的服务器的 IP 地址，通过服务器列表来添加规则时，此规则只对这个 IP 起防护作用。并且加在单一 IP 上应用规则优先级要大于按范围加的；

是否直通：在该服务器上设置了直通后，清洗系统不会对发向此服务器的任何流量做过滤；

全局触发规则：指得是触发规则—全局触发规则中的触发规则，是系统自带的全局性的触发规则，主要是全局过滤模块的前置条件，一旦达到全局触发的条件，全局过滤模块会智能防护这类攻击；

全局过滤模块：系统自带的全局性过滤防护模块，与上面的全局触发规则配合使用，其中模块勾选则生效，不勾则不生效；

每秒限制输入流量：可以限制特定服务器的每秒输入流量，单位为 Mbps。默认为 0 表示不限制，如果想限制某个 IP 每秒输入流量，可以设置相应的值。例如：填写 500 ，就会限制该 IP 每秒只允许输入 500Mb 的流量，多出的清洗系统将会拦截抛弃；

每秒限制输出流量：可以限制特定服务器的每秒输出流量，单位为 Mbps。默认为 0 表示不限制，如果想限制某个 IP 每秒输出流量，可以设置相应的值。例如：填写 500 ，就会限制该 IP 每秒只允许输出 500Mb 的流量，多出的清洗系统将会拦截丢弃；

系统插件：系统自带的域名过滤插件,主要是指清洗系统的域名管理插件，勾选则解析到 IP 上的域名受清洗系统域名管理模块的过滤限制，不勾选，则不受清洗系统域名管理系统的限制；

添加防护规则集：这里可以为该服务器添加一条或多条相应的防护规则集，就是【规则配置】中的规则集。例如想为服务器加一个防护 cc 攻击的防护规则，可以点击添加防护规则集，然后勾选规则集名称,点击保存即可。如果想取消已经添加上的某个规则集，可以在下方的防护规则集列表下，取消勾选相应的规则集，再保存该应用规则就行。相应就会在应用规则列表中产生一条新的规则条目。可以对该数据进行删除、修改、查询、禁用、激活等操作。

4.5 过滤规则

过滤规则是由过滤规则和应用 IP 组成，用以实现简单的访问策略，类似 ACL 功能，快速而有效。如

拦截某 IP 段对墙下 IP 的访问，拦截对墙下服务器某一端口的访问数据；封掉墙下某一服务器进出数据；封掉墙下某一服务器某种协议的数据通信等。添加完成的策略支持交换编号、禁用/激活、删除。

在应用 IP 上添加的所有过滤规则都会在过滤规则列表中显示，可以针对单条规则或者多条规则进行添加、删除、激活、禁用、查询的操作。过滤规则的添加如下：

名 称：清洗系统过滤规则的名称；

外部地址类型：指外部 IP，可以按任何地址、单一 IP、范围 IP 来选择；

内部地址类型：这个是指本地 IP，有单一 IP 和范围 IP 两种；

协议类型：应用此规则的协议，有 IP、TCP、UDP、ICMP、IGMP、其他六种。当选 IP 协议表示此规则作用于所有协议。选择 TCP 协议和 udp 协议时，还可以选择端口。此外，TCP 还能选择协议标志位：FIN、ACK、SYN、PSH、RST、URG，针对不同的标志进行勾选；

方向选择：这里有接收和发送可选。相对于本地服务器来说，即服务器的接收和发送方向；

行为规则：指触发此规则后数据处理行为，这里有两种行为：通过（直接把流量送达到达服务器）、拦截。

备注：自定义要备注的信息

4.6 IP 映射转发

IP 映射转发功能是一种以傲盾异常流量清洗系统为转发网关的隧道技术，通过该功能的简单配置可帮助用户将多线机房资源，调配给单线机房使用，使单线机房转变为多线机房；也可将异地机房 IP 地址在无需运营商介入的的情况下，移到本地使用，解决用户局部地域因 IP 地址匮乏无法扩展业务问题。

5 首页 - 牵引配置

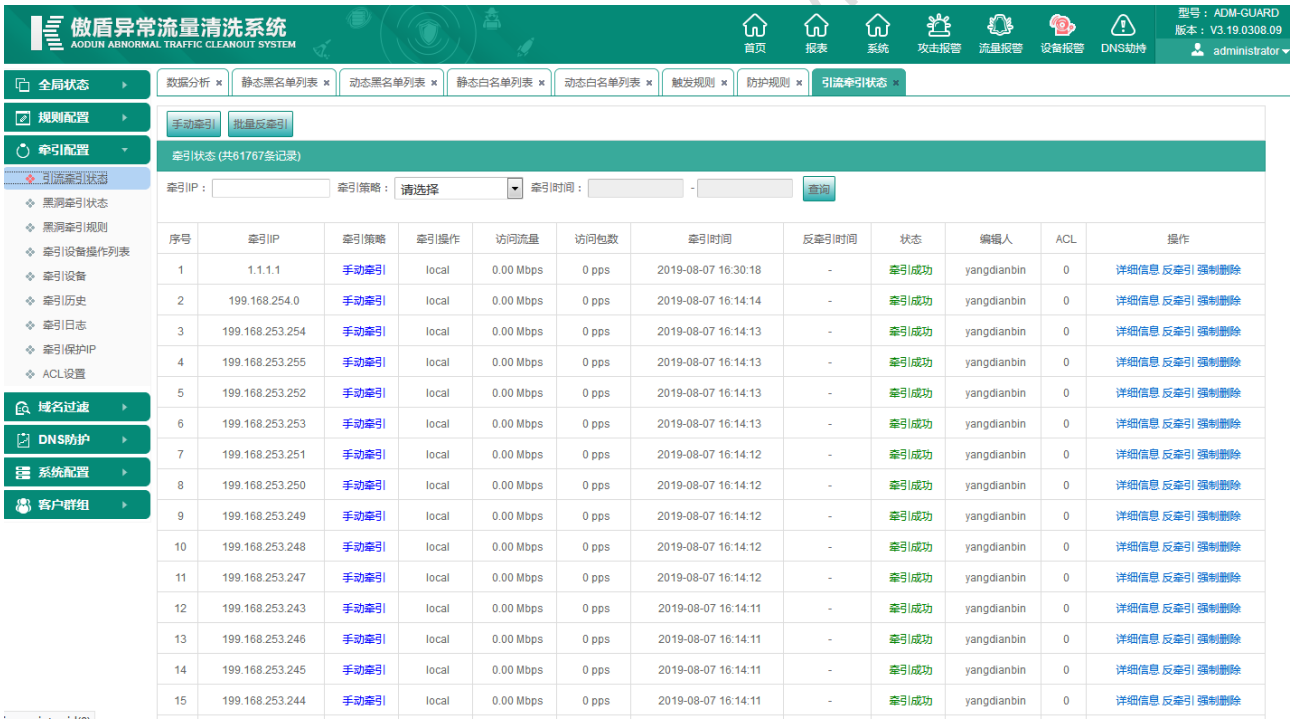
5.1 牵引概述

在牵引配置中，我们可以借助牵引设备，实现引流到清洗设备中，把异常流量清洗过后回注到原链路中，以达到保护服务器业务的功能。还可以借助上层核心交换或者路由来封堵大流量攻击，从而达到保护链路带宽的功能。

牵引配置的逻辑是首先添加相应的牵引设备，根据实际应用场景添加相关联的牵引操作。在策略中直接调用预置的牵引设备操作来引流或者封 IP。

5.2 引流牵引状态

旁路部署模式下，我们需要将本地服务器业务从交换机或者路由器上牵引到傲盾清洗系统中，即所谓引流。引流前先需添加牵引设备，默认协助旁路上架时都会添加好。如牵引条目过多可以通过牵引 ip 来进行查询。



5.3 黑洞牵引状态

被黑洞牵引策略封掉的 IP 会在黑洞牵引状态中列出来。管理员在这里还可以使用手动牵引，将某一个服务器在上层封掉。查询条件客户通过 ip、黑洞牵引策略、牵引时间来查询。

5.4 黑洞牵引规则

管理员可以预置一些策略，监控某些本地服务器，当这些服务器的流量达到某一个值时就在上层封掉此服务器。当前系统支持三种黑洞牵引策略：全局策略、全局本策略、普通策略。三种策略的优先级依次降低。

上图定义了一条全局策略，全局策略监控的是经过当前集群设备所有服务器的流量总和。当总流量达到所设置阈值时，会把流量最大的那个服务器 IP 在上层封掉。直到流量小于所设置的值。各内容如下：

名 称：定义策略名称；

触发策略阀值持续时间：触发流量阀值或包数阀值的时间，达到此值时就会执行左下角关联的

牵引操作。通常这里保持 0 即可，表示立刻执行牵引操作；

牵引持续时间：服务器被牵引的持续时间；

初次牵引时间：第一次达到阈值是的牵引时间；可添加第二次、第三次等时间自定义；

流量阀值：管理员所预置流量阈值，这里只用根据流量大小判断；

包量阀值：管理员所预置包数阈值；

自动反牵引模式：选择模式一，在服务器牵引时间结束后，会立刻反牵引；选择模式二，管理员可以再设置两个参数：流量阈值或者包数阈值。那么在牵引时间结束时，会再次进行该参数的判断，只有小于此阈值，才会执行反牵引。

牵引流量总和：勾选激活选项框，会自动选中全局选项。在本地选项框中可以设置牵引下限，表示在触发了策略阈值时，会判断流量最大的 IP 的流量是否大于此值。只有大于此值才会执行牵引操作。

牵引下限：勾选牵引流量总和时可选，流量低于下限不触发牵引操作。

牵引设备操作：选择触发策略后执行的牵引操作，通常是到上层交换机封 IP。

上图定义了一条全局本策略，管理员可以选择性的监控部分服务器。当这些服务器的流量总和达到了所设置的阈值时，就会封掉 TOP 排名流量第一的服务器。

上图定义了一条普通策略。这里监控的也是管理员添加的部分服务器 IP。与全局策略不同的是，这里的阈值是针对所监控的单个服务器 IP。当某一个服务器 IP 的流量达到此值时，就会执行牵引操作，在上层交换机好把此服务器封掉。

清洗系统集成过滤规则，过滤规则可以用于拦截服务器的输入与输出流量。每一种策略中都会有一个加入路由过滤规则的选项，该功能正是使用清洗系统中的过滤规则来达到拦截服务器的流量的目的。与到上层封 IP 不同的是，流量是在清洗系统中被拦截掉的。

5.5 牵引设备操作列表

无论是到上层封 IP，还是旁路引流，都需要一系列的命令操作。我们把这些命令预置到这里，并且跟相应的牵引设备关联在一起，就是牵引设备操作。无论是定义的策略还是手动牵引，都可以直接调用这些牵引操作，让系统去执行预置在牵引操作中的命令，以达到封 IP 和引流的目的。

5.6 牵引设备

牵引设备是指用于引流的清洗设备或者上层封 IP 的交换机。引流时，牵引设备就是清洗设备本身。在添加时，可以选择 telnet 设备，IP 为每台清洗设备的管理口地址，端口对应清洗设备路由模块所监听的端口 16020。需要在上层封 IP 时，牵引设备就是该交换机对应的地址，系统支持 telnet、ssh 和 webservice 登录。条件好的牵引设备支持导入导出。

5.7 牵引历史

被牵引过的 IP 人工或者自动反牵引后会在牵引历史中列出，管理员可以查看被牵引过的 IP 所触发的策略、被牵引时该服务器的流量值、牵引和反牵引时间。

5.8 牵引日志

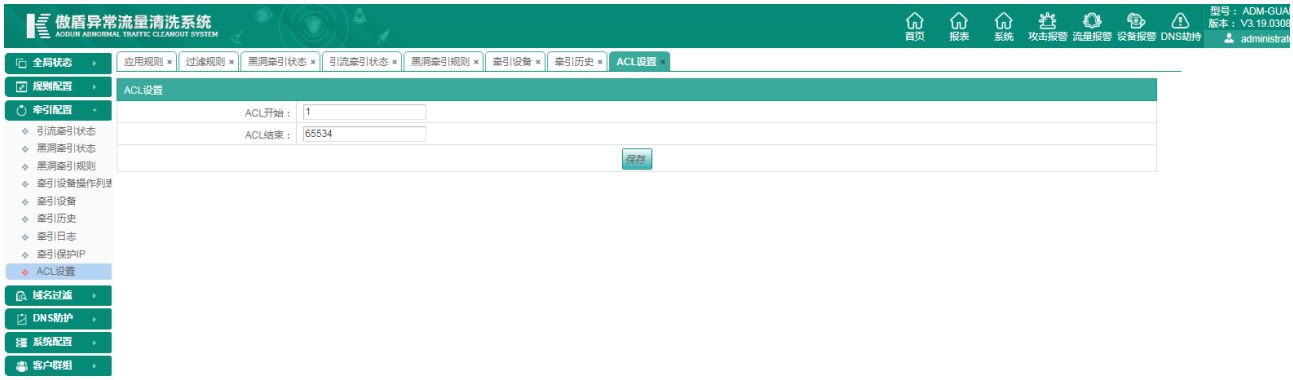
牵引日志用于查询牵引操作的详细执行过程，主要用于管理员对牵引故障的排错。默认牵引 20 条可以根据自己需要自定义查询。

5.9 牵引保护 ip

添加在牵引保护中的服务器地址在所有的策略中将不会被牵引，类似牵引白名单。

5.10 ACL 设置

ACL 默认开始是 1 到结束 65534，这个是在牵引过程中使用到的与交换机 acl 号对应。默认无需修改。



6 首页 – 域名过滤

域名过滤用于对机房内域名进行管控，在工信部严查域名备案的大背景下，有效的服务器域名接入管控显得尤为重要。域名过滤模块的应用，为国内广大的 IDC 用户提供了实用的域名管理手段。

6.1 参数过滤

域名过滤模式：可选择黑名单和白名单模式。或关闭域名过滤模块。开启黑名单模式时，域名黑名单列表中的域名将不能被外网访问；开启白名单时，则只能在域名白名单列表中的域名可以被外网访问。

过滤端口：通常域名监控的是 TCP 的 80 端口。管理员可以根据需要添加多个端口，端口跟端口之间需要用逗号隔开。那么系统就可以配合上白名单或者黑名单域名来协同工作。

使用 IP 直接访问网站：用于控制本地服务器域名是否可以通过 IP 来让外部用户访问。当勾选拦截时，外部用户直接使用 IP 来访问域名时会被系统拦截掉；当勾选忽略时，系统将不过滤使用 IP 访问服务器网站的请求。

与非法信息监控系统联动：如果用户在使用傲盾非法信息监控系统，可以通过此开关来让非法设备过滤到的已备案和未备案域名联动到清洗系统中，不用人工添加。

6.2 域名黑、白名单

当开启白名单模式时，只有在白名单中的域名才能被外部用户访问。如果开启的是黑名单，那么在黑名单列表中的域名将不能被外部用户访问。管理员在添加域名时，只需要添加一级域名就可以。如下图，其中*表示该一级域名下的所有域名。

6.3 过滤提示信息

域名提示信息用于系统在阻断非法域名时，呈现给外部访问用户的一个提示拦截页面。

6.4 联动黑、白名单

联动黑白名单则是从傲盾非法信息监控系统中同步过来的域名。联动黑名单跟域名黑名单功能一致。联动白名单跟域名白名单功能一致。

7 首页 – DNS 防护

傲盾异常流量清洗系统支持 DNS 服务保护功能，DDOS 设备采取 DNS 宕机保护，DNS 访问控制，DNS 动态缓存及随机域名限制等方式保护 DNS 服务器提供正常服务。

7.1 DNS 动态缓存

DNS 模块缓存它的 DNS 的 reply 包，之后再有对该域名的请求的时候，DNS 防护设备直接恢复该域名的 DNS 地址 ，不再透过到 DNS 服务器，防护 DNS 服务器被 DDOS 攻击而受影响。

7.2 DNS 宕机保护

DNS 宕机保护：DNS 防护插件支持对 DNS 服务器状态进行检测，让管理员可以实时的掌握 DNS 服务器是否存活，如果发现有宕机的 DNS 服务器可以及时发现采取措施。

配置 DNS 宕机防护：

DNS 服务器 ip：需保护的 DNS 服务器 IP 地址

域名 1-3：凭借此设置的域名去检测判断服务器是否正常服务

7.3 DNS 黑白名单

DNS 黑白名单设置：DNS 黑白名单支持同时开启，开关为模式转换。**模式一**指在白名单中继续过滤，不在白名单的 IP 则丢弃。**模式二**指在白名单中的 IP 放行，不在白名单继续过滤一下规则。

DNS 黑名单：指触发 DNS 防护插件所设置规则后把攻击 IP 加入黑名单。黑名单一致性校验指的检查界面设置的黑白名单和核心中的黑白名单数据是不是一致，如果检查后提示不一致进行黑名

单同步。针对黑名单列表可以手动添加，批量导入，备份导出，批量删除黑名单列表，既清空及导入删除。

DNS 白名单：指触发 DNS 防护插件所设置规则后把攻击 IP 加入白名单。白名单一致性校验指的检查界面设置的白名单和核心中的白名单数据是不是一致，如果检查后提示不一致进行白名单同步。针对白名单列表可以手动添加，批量导入，备份导出，批量删除白名单列表，既清空及导入删除。

7.4 DNS 域名绑定

DNS 域名绑定：通过客户端访问的域名和该域名对应的 DNS IP 进行绑定,以达到 DNS 服务器为客户端提供正常解析,以防护 DNS 投毒攻击。

DNS 域名绑定一致性校验指的检查界面设置的 DNS 域名和核心中的域名数据是不是一致，如果检查后提示不一致进行 DNS 域名绑定同步。针对 DNS 域名绑定可以手动添加，批量导入，备份导出，批量删除 DNS 域名列表，既清空及导入删除。

配置 DNS 域名绑定：

域名：客户端访问的域名

IP：DNS 服务器 IP

限速单位时间：此设置的单位时间

限速单位时间访问次数：此设置为单位时间内访问的次数

7.5 DNS 访问限制

DNS 访问限制：对客户端请求的 DNS 解析服务进行限速控制，将 DNS 服务器受到 DNS FLOOD 攻击危害降低，对有攻击 IP 进行拦截，保护 DNS 服务器正常提供解析服务。

7.6 DNS 随机域名限制

限制对该 DNS 服务器请求的随机域名，如果是真实的域名一般都会缓存在 DNS 防护设备上，之后再请求，DNS 防护设备就会回应不再透过到 DNS 服务器上，不真实的域名解析请求就被丢弃。

DNS 随机域名限制一致性校验指的检查界面设置的随机域名和核心中的域名数据是不是一致，如果检查后提示不一致进行 DNS 随机域名限制同步。针对随机域名限制手动添加，清空及删除。

7.7 DNS 域名劫持

DNS 域名劫持：是在当有 DNS 请求包投过去，请求到 DNS 回应包中的 DNS 地址和 DNS 缓存中的 DNS 地址 不一致时，就会发生报警来提醒用户 DNS 被攻击存在异常

DNS 域名劫持一致性校验指的检查界面设置的域名和核心中的域名数据是不是一致，如果检查后提示不一致进行 DNS 域名劫持同步。针对域名劫持手动添加，清空及删除。

7.8 DNS IP 地址 TopN

显示 DNS 服务器根据解析的 IP 地址，根据 IP 地址请求的数量进行排名统计

排名： 根据请求数量排序

IP 地址： DNS 服务器 IP

请求数量： DNS 服务器被请求的次数

7.9 DNS 域名 TopN

DNS 解析的域名请求排名统计，设备会将请求的解析域名按从高到低的顺序进行排列。

排名： 根据请求数量排序

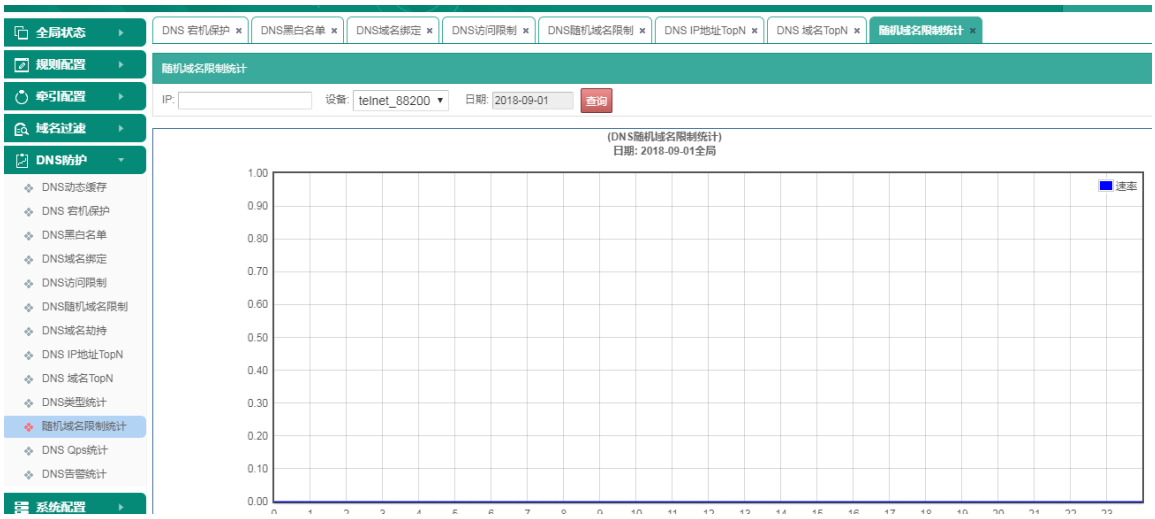
域名： 请求解析的域名

请求数量： DNS 服务器对域名解析的次数

7.10 随机域名限制统计

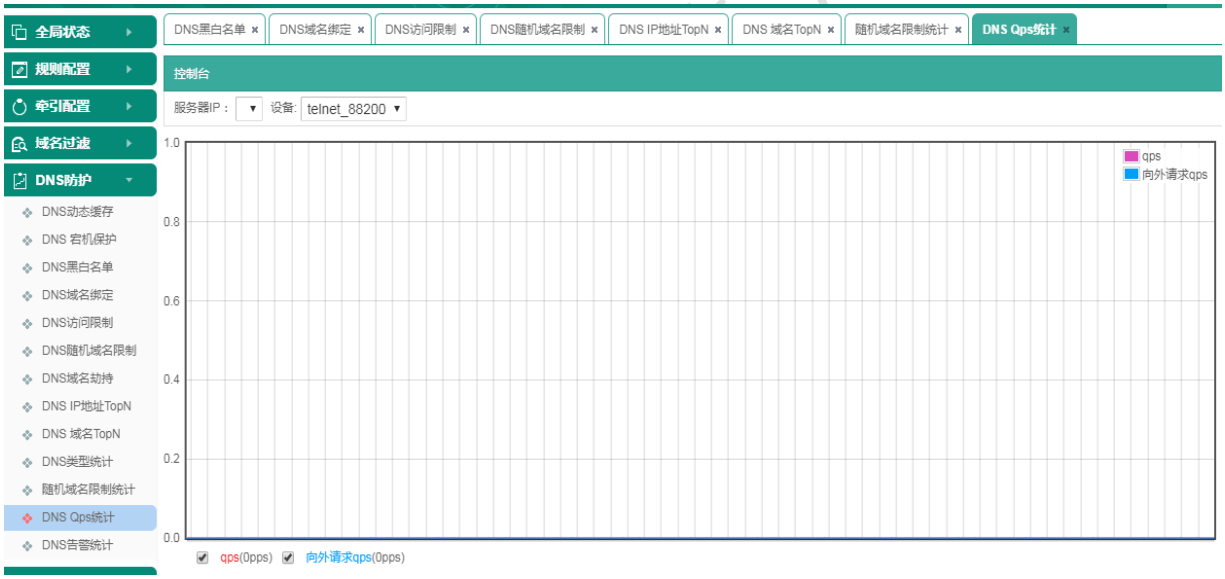
设备对 DNS 随机域名限制进行统计，详细统计被攻击的服务器 IP 地址、攻击次数、频率限制情况，

同时根据攻击频率进行排名统计。



7.11 DNS QPS 统计

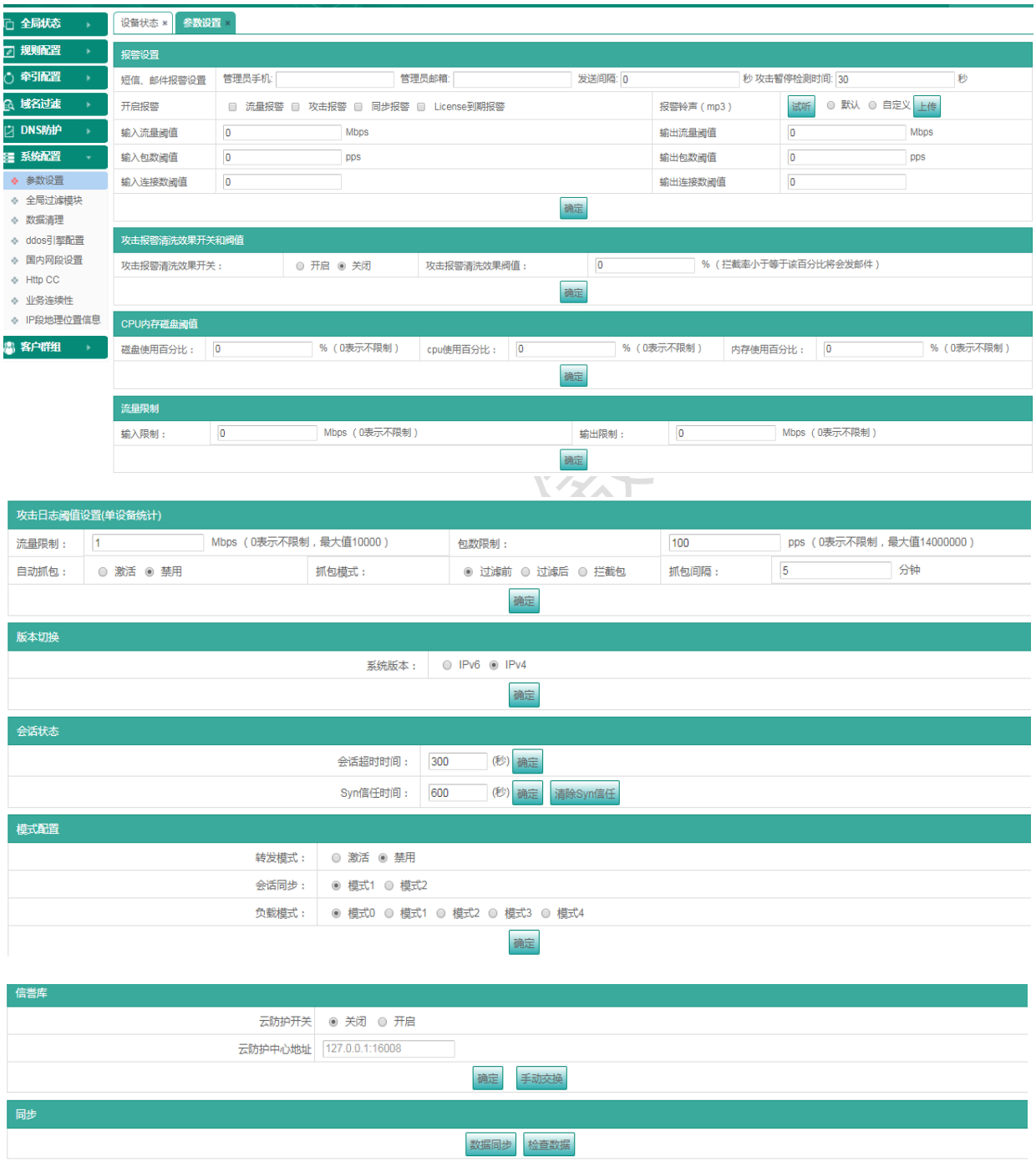
DNS QPS 统计：记录 DNS 服务器接收和回应的数据包信息，通过该功能可以判断 DNS 服务器的性能和了解针对该服务器的攻击拦截情况。



8 首页 – 系统配置

8.1 参数设置

参数设置内部包含报警设置、流量限制、攻击日志设置、会话状态、模式切换等等。



报警设置：针对流入流出清洗设备的流量、包数、连接数进行设置，如果流经清洗设备的流量大于所设置的值，就会在 web 页面上提示告警。在配置好发件邮箱情况下，还可以将报警信息发送给管理员的邮箱；

攻击报警清洗效果开关和阀值：有攻击报警清洗效果开个和攻击报警拦截率邮箱告警

CPU 内存磁盘阈值：默认）%不限制，如果设置了阀值触发后设备报警会进行提示告警。

流量限制：此处的限速是针对全局每台服务器进出流量限制，默认参数是 0，表示不限制。

攻击日志阀值设置：在本地服务器流量达到此值时，被系统检测到含有异常流量，才会生成日志信息。防火墙攻击自动抓包模块，默认禁用，如需使用请选择激活按钮，并设置抓包间隔时间，如有攻击防火墙会自动抓包保存。

版本切换：切换防火墙 IPV4 与 IPV6 的版本，ipv6 支持双协议栈。

会话状态：会话超时表示经过防火墙建立的连接，在没有数据交互时经过相应时间会被释放，可以防止空连接。SYN 信任时间表示触发 SYN 模块并经过 SYN 模块验证认为合法外部 IP 的信任时间，在此时间内 SYN 模块将不会再次验证。

模式配置：防火墙配置为转发模式，数据经过防火墙时会被直接转发到本地防火墙上，不做任何过滤与验证。

同 步：检查数据用于检查当前集群防火墙间是否出现数据不一致的问题；数据同步是把当前管理员在管理机上做的一些数据全量下发到防火墙上。

8.2 全局过滤模块

全局过滤模块包括：syn、udp、icmp、other、drop oversea ip、gamecc、tcp check、attack identify、Sample library filter。全局过滤模块由北京傲盾 DDoS 安全实验室研发中心定制研发，集成傲盾公司二十年来的经验，通过大量的压力测试应用于大量用户实际网络环境中，对于各种常见 Flood 攻击具有良好的过滤拦截效果。并且北京傲盾公司将不断研发新型攻击防御模块，免费为客户更新。

8.3 数据清理

随着系统的使用，设备上会产生大量的日志信息，例如用户操作日志、用户登录错误日志、抓包记

录、牵引历史、牵引日志、攻击日志、流量日志、CPU、内存日志等日志内容。如果不定时清理，管理磁盘有可能会被占满。使用定时清理功能，管理员设置好相关日志的保留时间，清洗系统会自动把该时间以前的日志都删除，从而避免磁盘被占满的可能。

8.4 ddos 引擎设置

DDOS 引擎设置是针对清洗设备核心模块验证的设置，管理员请谨慎操作，如需修改，请在傲盾售后人员的指导下修改。通常用户不需要关心下面的参数，保持默认即可。

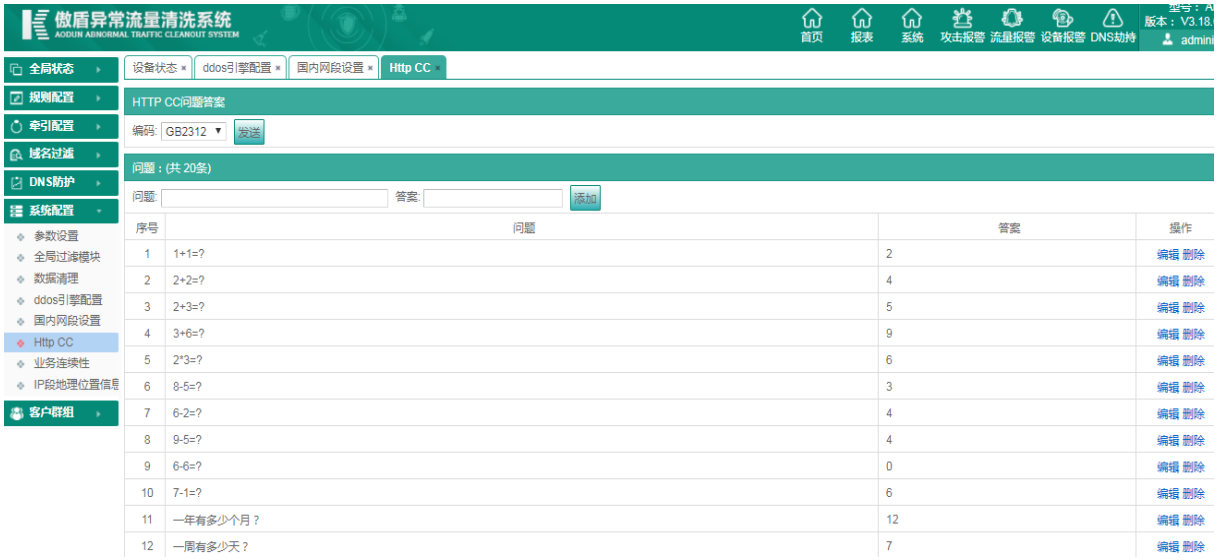
8.5 国内网段设置

打开清洗设备核心模块对国内 IP 设置的支持后，在此处导入国内网段 IP。当在服务器 IP 上添加了应用规则，勾选可信源检测，在此服务器被 DDOS 攻击后，清洗系统核心模块就会将攻击中的国外 IP 过滤掉。

8.6 Http CC

清洗系统集成 CC 插件，CC 插件是被调用在规则集 S_HTTP NEW CC V2.1 中。在实际使用中，是在服务器 IP 上添加应用规则，将此规则集添加上。该插件参数如下：

其中第一个参数 0 用于控制 CC 验证的方式。默认 0 为小尾巴认证；1 为按钮认证；2 为问题认证。当 CC 攻击触发了 CC 插件时，外部用户的访问 GET 行为将被跳转至清洗系统的 CC 模块进行接管，将用户的访问页面跳转至清洗系统的认证页面。如果管理员设置验证方式为问题验证，那么这里的问题将会被呈现给用户，待用户回答正确后跳转回网站首页。



8.7 IP 地址位置信息

如果管理员想在本地服务器上屏蔽属于某一地理位置的外部 IP，需要在系统中导入相应的 IP 地理位置段。那么在引服务器上添加过滤规则，外部地址类型中选择 IP 地址位置，就可以按地理位置来在本地服务器上屏蔽外部 IP 了。

9 首页 - 客户群组

9.1 群组列表

服务器在被攻击或者被牵引时，可以通过群组功能，把该事件通知给用户，以告知用户业务实时情况。管理员可以添加多个群组，为每个群组关联上不同的用户与 IP 段。同时支持选择发送邮件或者短信的时间点。如果设置了流量或者包数报警阈值，那么在服务器被攻击的时候，只有流量大于该值才会发送邮件或者短信。如果勾选了发送给管理员，那么不但会发送邮件给所设置的群组邮件，还会发送邮件通知管理员。　管理员邮件是在系统配置中参数设置那里添加。另外一个控制邮件发送的地方也就是参数设置中的发送间隔，是指在服务器被持续攻击较长时间时，发送第二封邮件的间隔时长。最短为 30 秒，如果置 0，邮件则无法正常发送。短信告警需用户与第三方短信平台对接使用。

9.2 发消息设置

系统要想发送邮件通知群组用户，还需要设置上发件箱。添加好后，使用发送测试邮件来测试该功能是否正常。

9.3 报警白名单

在群组中添加 IP 时，可以按一个范围来填写。如果其中有某些 IP 在攻击或者被牵引时，不需要发送邮件告知用户。可以把这些 IP 添加到报警白名单中。

9.4 告警自定义设置

在给群组用户发送告警邮件时，管理员可以通过自定义设置来选择发送的内容，如：防护方式、服务器峰值流量、拦截峰值流量、峰值包数、拦截包数、持续时间等，还可以根据贵公司的需求在发告警邮件是传输自定义 logo 来进行发送。

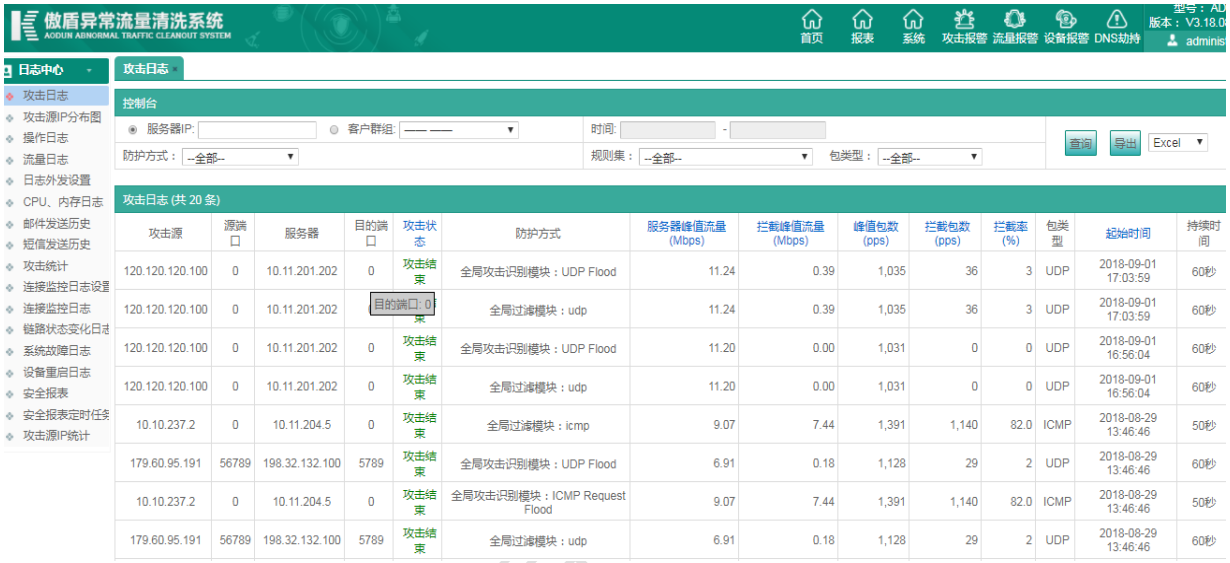
9.5 设置流量告警阀值

可根据之前添加的大客户群组定义流量告警阀值，超出后执行黑洞牵引规则来进行黑洞流量牵引。

10 报表

10.1 攻击日志

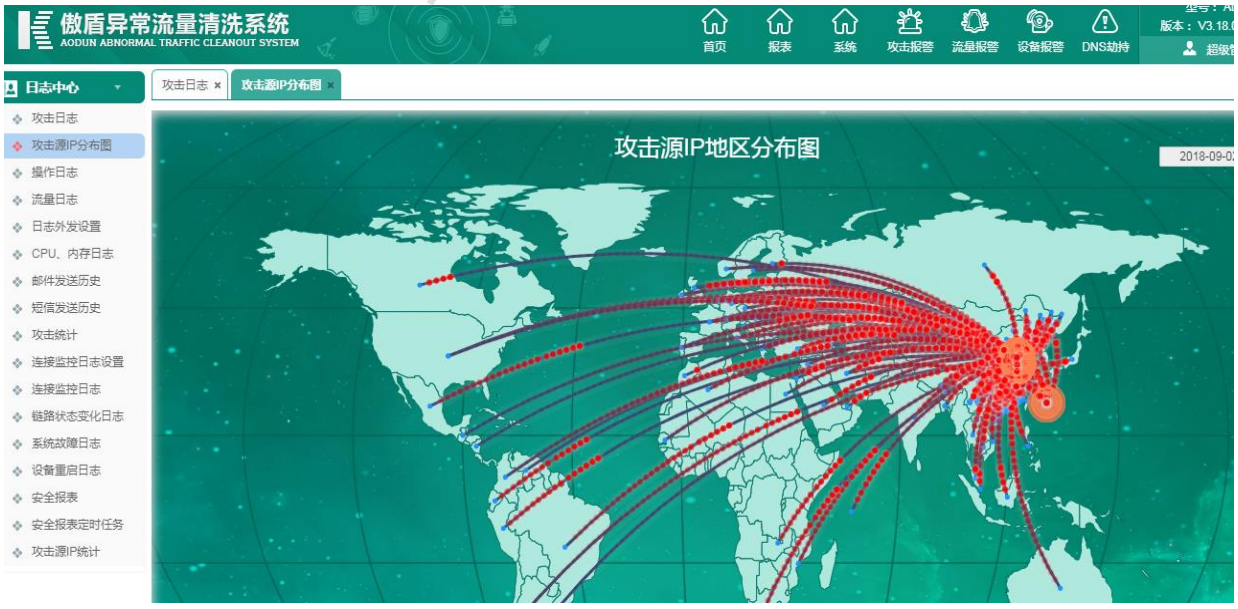
如果有服务器流量触发了清洗系统的过滤模块或者规则集等防护模块，并且有拦截流量产生，系统就会生成一条攻击日志。其中包括攻击源 ip、源端口、目的 ip、目的端口、攻击状态、防护方式、服务器峰值流量、包数、拦截峰值流量、包数等信息。当本次攻击还没有结束时，系统会以红色字体显示“正在攻击”，提醒管理员攻击正在发生。并且日志支持导出到 excel、pdf、html、xml、word 功能。



攻击源	源端口	服务器	目的端口	攻击状态	防护方式	服务器峰值流量 (Mbps)	拦截峰值流量 (Mbps)	峰值包数 (pps)	拦截包数 (pps)	拦截率 (%)	包类型	起始时间	持续时间
120.120.120.100	0	10.11.201.202	0	攻击结束	全局攻击识别模块：UDP Flood	11.24	0.39	1,035	36	3	UDP	2018-09-01 17:03:59	60秒
120.120.120.100	0	10.11.201.202	目的端口: 0	攻击结束	全局过滤模块：udp	11.24	0.39	1,035	36	3	UDP	2018-09-01 17:03:59	60秒
120.120.120.100	0	10.11.201.202	0	攻击结束	全局攻击识别模块：UDP Flood	11.20	0.00	1,031	0	0	UDP	2018-09-01 16:56:04	60秒
120.120.120.100	0	10.11.201.202	0	攻击结束	全局过滤模块：udp	11.20	0.00	1,031	0	0	UDP	2018-09-01 16:56:04	60秒
10.10.237.2	0	10.11.204.5	0	攻击结束	全局过滤模块：icmp	9.07	7.44	1,391	1,140	82.0	ICMP	2018-08-29 13:46:46	50秒
179.60.95.191	56789	198.32.132.100	5789	攻击结束	全局攻击识别模块：UDP Flood	6.91	0.18	1,128	29	2	UDP	2018-08-29 13:46:46	60秒
10.10.237.2	0	10.11.204.5	0	攻击结束	全局攻击识别模块：ICMP Request Flood	9.07	7.44	1,391	1,140	82.0	ICMP	2018-08-29 13:46:46	50秒
179.60.95.191	56789	198.32.132.100	5789	攻击结束	全局过滤模块：udp	6.91	0.18	1,128	29	2	UDP	2018-08-29 13:46:46	60秒

10.2 攻击源 ip 分布图

在这里动态显示本地服务器接收的异常流量的地理位置分布。



10.3 操作日志

记录所有用户操作日志、异常日志以及审计日志。可以根据查询条件开始时间、介绍时间、操作者、详细信息、级别查询。展示的日志有；包括用户登录时间、操作日志类型、操作详细信息、登录 ip 地址、操作用户等。

10.4 流量日志

流量日志主要协助管理员查询本地服务器的流量。系统提供主机、设备、时间多种选项来协调查询。添加上主机地址时，查询的则的该主机的流量。在集群环境下选择了一台设备，查询的是该主机经过该设备的流量。查询单 ip 按日期查询最多查询一个月。

10.5 日志外发设置

日志外发设置，主要用于把当前系统上产生的一些日志，以 syslog 的形式发送到外部日志服务

器上。用于追溯异常情况，以便分析问题的原因。

发送类型：支持 syslog、mail、ftp 三种方式推送，每种按照正常方式配置即可。

10.6 CPU、内存日志

这里主要是供管理员查询防火墙集群中单台防火墙的 CPU、内存使用情况，也可以通过选择日期来查询防火墙的历史系统负载状况。

10.7 邮件发送历史

邮件发送历史主要是为了让管理员能够查询当前系统发送的邮件历史情况。

10.8 短信发送历史

短信发送历史主要是为了让管理员能够查询当前系统发送的短信历史信息。

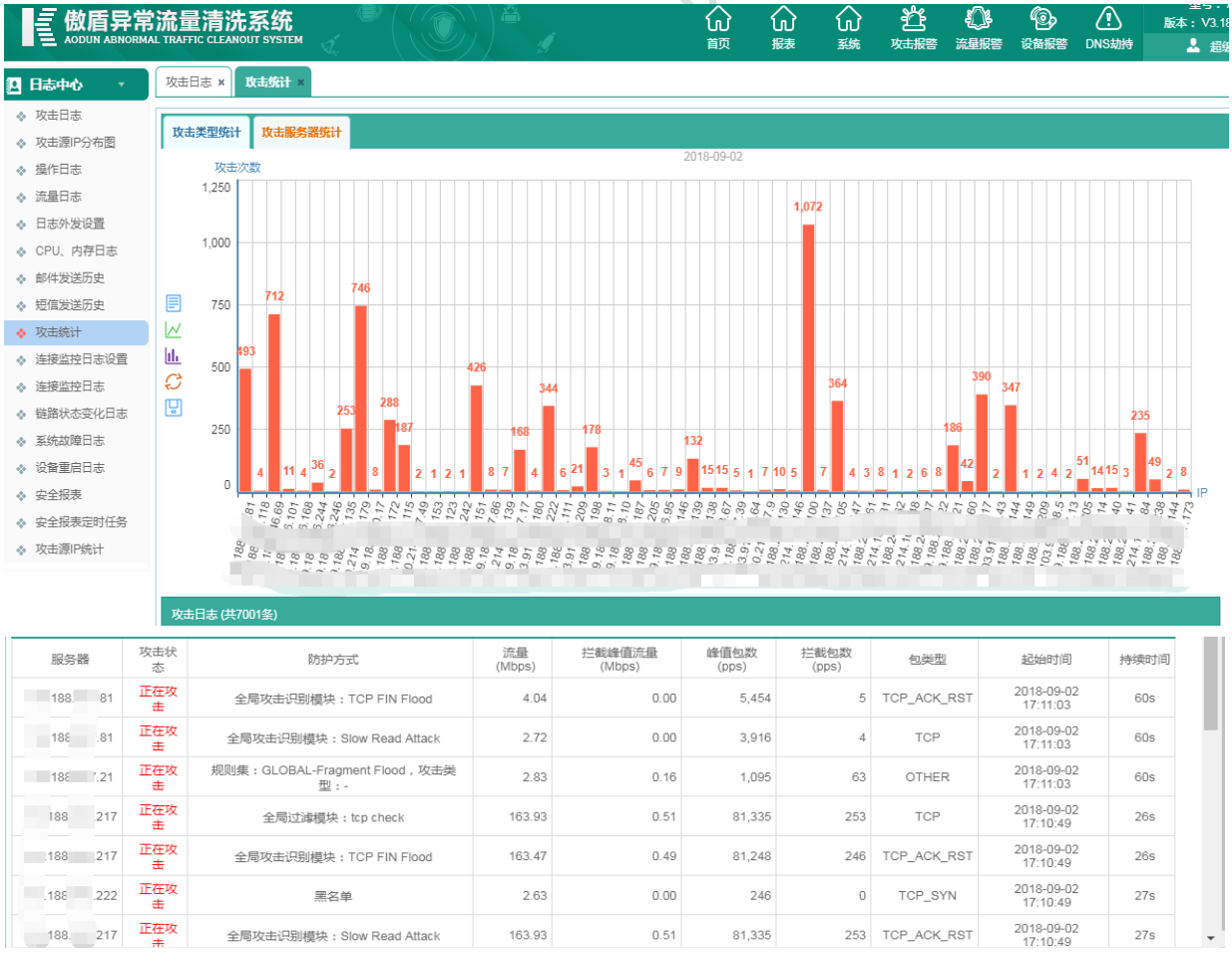
10.9 攻击统计

10.9.1 攻击类型统计

系统通过对当日所遭受攻击的类型、次数和时间段进行统计，并形成攻击趋势图，帮助管理员更好的分析机房的被攻击情况，从而更好的调整机房网络的使用和机房业务的分布。条件查询，可通过服务器 ip 或者 ip 段、时间进行查询。支持 PDF 格式导出。

10.9.2 攻击服务器统计

系统提供被攻击服务器的按时间段统计结果。通过查看一天中的服务器被攻击趋势，和对历史统计结果的对比，帮助管理员更好的分析出机房业务中最易受攻击的业务分布，从而更好的对所接入业务进行调整和网络安全改造。件查询，可通过服务器 ip 或者 ip 段、时间、拦截封流量等进行查询。支持 PDF 格式导出。



10.9.3 攻击源统计

可根据被攻击 ip 时间来查攻击源，top 次数排名，默认排前十名，此报告支持 PDF 和 Excel 格式导出。

10.10 连接监控日志与设置

系统通过设置连接监控 IP 段，去监控该 IP 段的连接情况。显示包括源目的 ip、源目的端口、协议类型、连接状态、连接描述、时间等。要先在连接监控日志设置那里打开此功能，并且添加相应的地址段信息。

10.11 链路状态变化日志

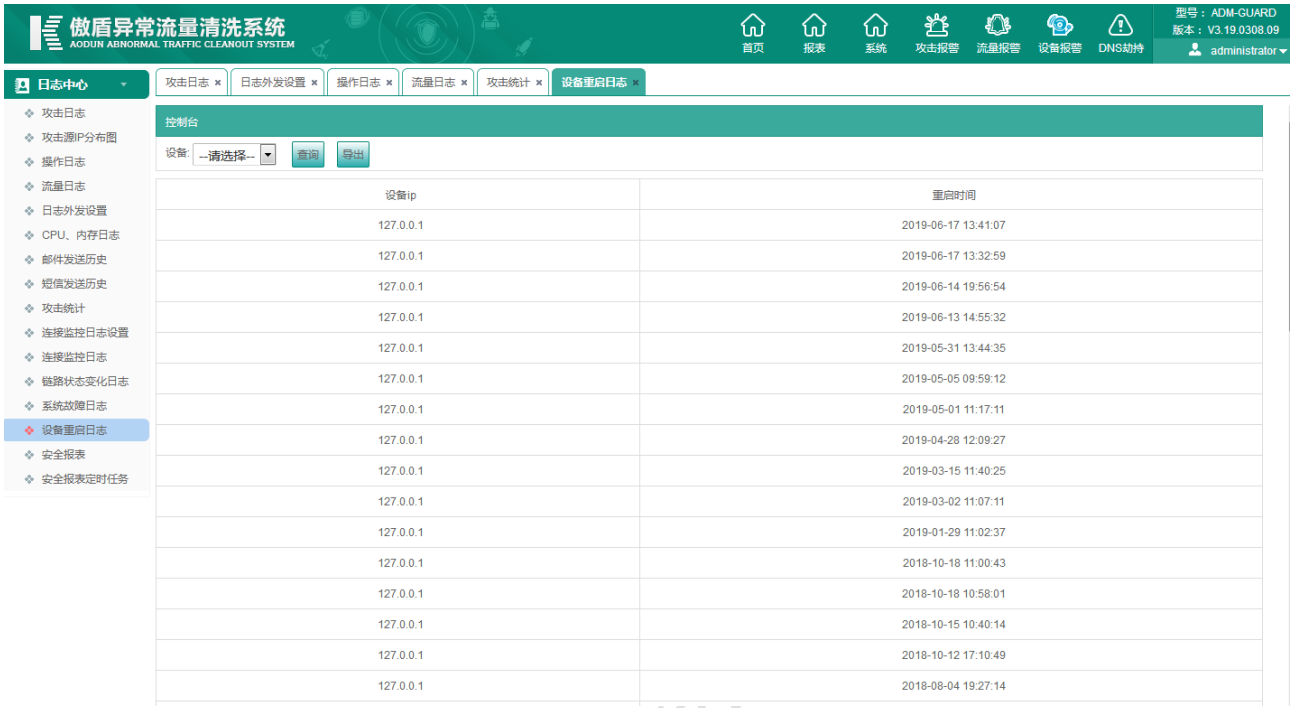
链路状态变化日志对每台设备网卡开启、关闭状态进行日志记录。

10.12 系统故障日志

系统故障日志记录设备异常事故，记录详情信息及出现故障时间。可以针对 CPU、管理端、内存和设备的核心进行监控。

10.13 设备重启日志

设备重启日志记录每台设备的重启记录，记录时间。方便查询系统重启情况。



10.14 安全报表与定时任务

安全报表定时任务用于按计划，针对某 IP 段生成安全统计报告，报告中可以显示用户在一段时间内的流量情况，攻击情况，网络运行情况等，还可以通过饼状图、柱状图、曲线图等直观的进行显示。目前报告支持邮件推送和 PDF 导出。


傲盾异常流量清洗系统
AODUN ABNORMAL TRAFFIC CLEANOUT SYSTEM
日志中心
攻击日志
攻击源IP分布图
操作日志
流量日志
日志外发设置
CPU、内存日志
邮件发送历史
短信发送历史
攻击统计
连接监控日志设置
连接监控日志
链路状态变化日志
系统故障日志
设备重启日志
安全报表
安全报表定时任务
攻击源IP统计
攻击日志 × CPU、内存日志 × 连接监控日志 × 链路状态变化日志 × 系统故障日志 × 安全报表 × 安全报表定时任务 ×
添加报表定时任务
任务名称：
报表生成周期：
月报
周报
日报
IP范围:
-
邮件开关:
保存
返回

11 系统 – 设备

11.1 设备管理

设备列表中列出当前管理机所管理的清洗设备。地址为清洗设备的管理地址，端口为 16001。状态为开启，表示管理机与该设备间通信正常。禁用此设备，管理机将不会向此设备下发配置。如果需要对单台设备进行配置，可以点【配置】项。进入对该设备的配置。

11.1.1 设备配置

11.1.1.1 设备状态

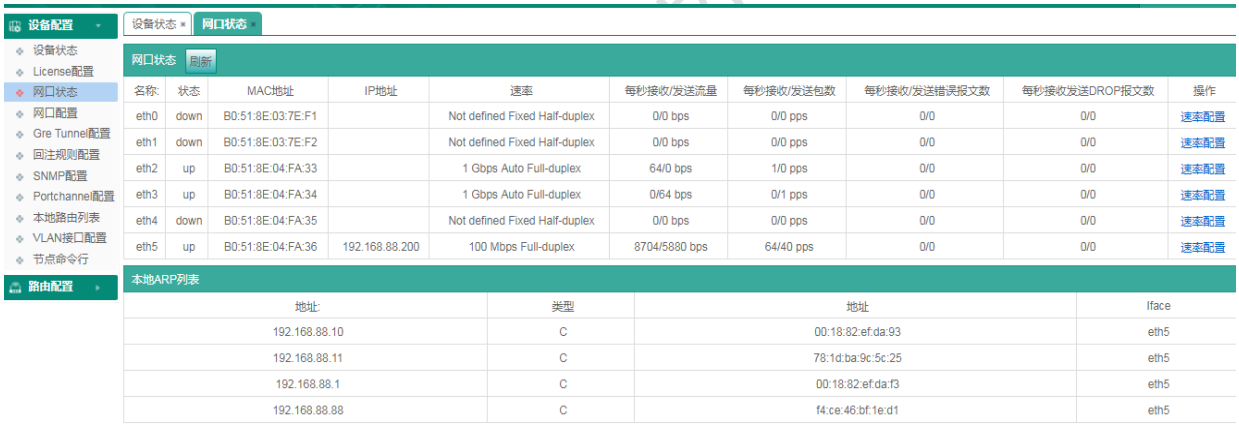
点击设备列表中左侧的【操作】栏中的【配置】，就可以对设备进行管理，如下图。首先进来，看到的就是设备状态，这里用于显示设备状态与服务状态。服务状态中指出当前该设备路由模块是否开启。模块版本表示当前设备的核心版本号。能显示模块版本这块则认设备管理设备正常。

11.1.1.2 License 设置

License 用于对清洗设备使用服务的限制。其中会列出当前设备的型号、硬件平台、防护能力。

11.1.1.3 网口状态

网口状态显示该清洗设备网口的状态信息。



11.1.1.4 网口配置

不同型号的清洗设备出厂网口数量不同。网口配置主要用于设备在上架时，根据部署模式来设置业务网口的角色。除非需要更换部署模式，设备一旦上架并接入业务，就不需要再重新配置网口。配置完网卡 ip 需要进行应用配置下发，否则配置不生效。

11.1.1.5 GRE Tunnel 配置

参数设置内包含名称、GRE tunnel IP、本地地址、远端地址。配置好以上设置后点击应用配置后生效。

11.1.1.6 回注规则配置

参数设置包含被保护的 IP、子网掩码、tos、802.1q 的优先级、Vlan id、GRE Tunnel 标签分发、mpls、vpn 标签。配置好以上设置后点击应用配置后生效。

被保护的 IP：添加需要被保护 IP 地址或网段。

子网掩码：添加需要被保护 IP 的子网掩码。

TOS：添加回注规则的 TOS。

802.1q 的优先级：设置 vlan 的优先级.

Vlan id：设置 Vlan 的 id,大于 0 表示启用了 Vlan.

GRE Tunnel：选择已经设置好的 GRE Tunnel 为当前的回注规则。

标签分发：自动（先启动 ldp 路由器才能自动分发 mpls 的标签 ）。手动（用户指定 mpls 标签）。

Mpls：以上标签分发选择手动后生效，添加 mpls 的标签号（0 表示不启用 mpls）。

Vpn 标签：添加 vpn 的标签号（0 表示不启用 mpls）。

11.1.1.7 SNMP 配置

11.1.1.8 Portchannel 配置

清洗设备支持多端口捆绑，通常在旁路部署时，把多个接口绑定在一起，与交换机建立互联关系。可以为交换机节省 IP 资源。在 portchannel 配置处添加成员接口，最后在应用配置。应用时需要勾选相应的模式。其中模式一为静态绑定，如果需要动态协商，需要选择模式五。配置成功后，在网口配置处就会看到创建成功的捆绑接口，再此接口上做进一步接口配置。

11.1.1.9 本地路由表

旁路模式时，可以查询本地清洗设备的路由表信息。

11.1.1.10 Vlan 接口配置

给对网口绑定 Vlan

ip：配置 vlan ip 地址。

子网掩码：配置子网掩码。

Vlan ID：配置 Vlan id 号。

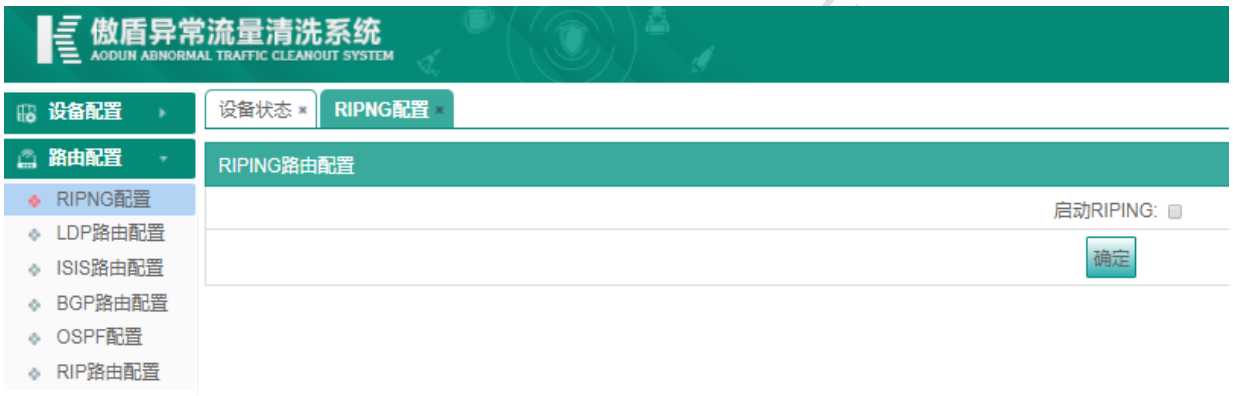
绑定接口：把相应接口加入 Vlan。

远端 IP：配置对端通信 ip。

11.1.2 路由配置

11.1.2.1 RIPNG 路由配置

RIPNG 协议 RIP 协议的 IPv6 版本。



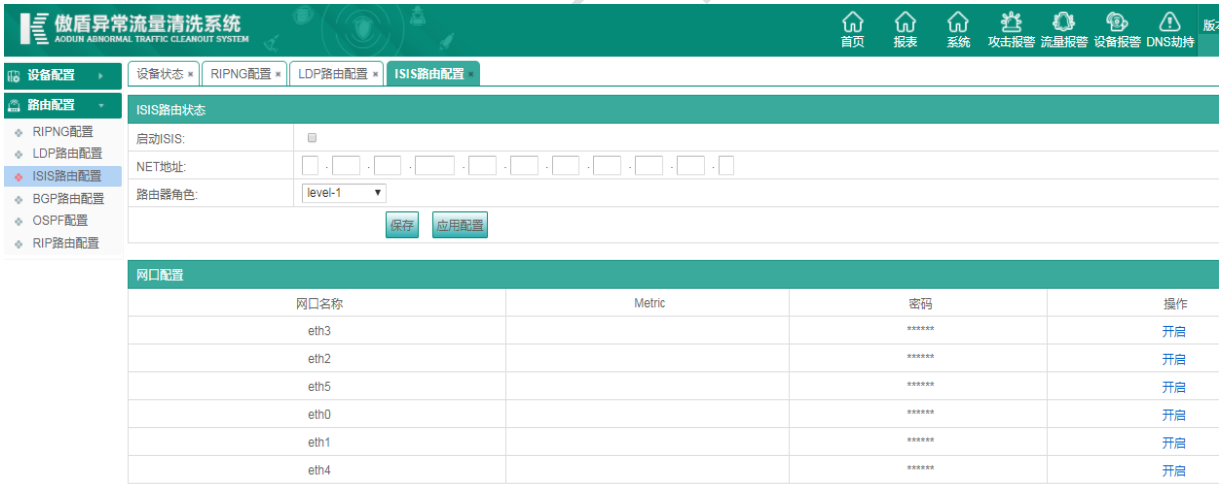
参数设置:只要选择启动 RIP 后再点击应用配置既生效。

11.1.2.2 LDP 路由配置

LDP 指标签分发协议。参数设置内部包含启动 LDP、会话端口，配置好以上设置后需点击应用配置后生效。勾选表示使能 LDP 功能，否则，相反。激活运行 LDP 的接口。

11.1.2.3 ISIS 路由配置

ISIS 指的是中间系统到中间系统，并且是为 ISO 无连接网络协议（ISO's Connectionless Network Protocol,CLNP）设计的路由选择协议。参数设置内部包含启动 ISIS、NET 地址、路由器角色、网口配置，配置好以上设置后需点击应用配置后生效。



11.1.2.4 BGP 路由配置

BGP 常用于旁路部署时，清洗设备中交换机建立 BGP 邻居关系，清洗设备发布主机路由。将业务流从交换机牵引进清洗设备，清洗设备把异常流量过滤后的流量回注给交换机。交换机再次向下转发。在配置网口好后，在清洗设备本端只需要激活 BGP 模块，并配置 AS 号。另外就是需要把对端 IP 地址和 AS 号添加进来。就完成清洗设备上所有 BGP 的配置。

11.1.2.5 OSPF 路由配置

OSPF 协议是 IETF 组织建议使用的内部网关协议（IGP）。同时是一个链路状态协议，它使用 Dijkstra 的最短路径优先算法。新版本支持 IPV6 版

参数设置内部包含启动 OSPF、Area、Cost、Metric、Type、认证方式，Auth、Key-id、Encrypt 配置好以上设置后需点击应用配置后生效。

启动 OSPF：打钩表示使能 OSPF 功能，否则，相反。

Area：添加 OSPF 区域号。

Cost：添加 OSPF 的代价。

Metric：添加 OSPF 的度量。

Type：重分发进 OSPF 里的路由的路径类型。

认证方式：可选择不加密、明文口令、加密口令。

Auth：认证方式为明文口令时的口令。

Key-id：认证方式为加密口令时加密的 key id。

Encrypt:认证方式为加密口令时口令。

11.1.2.6 RIP 路由配置

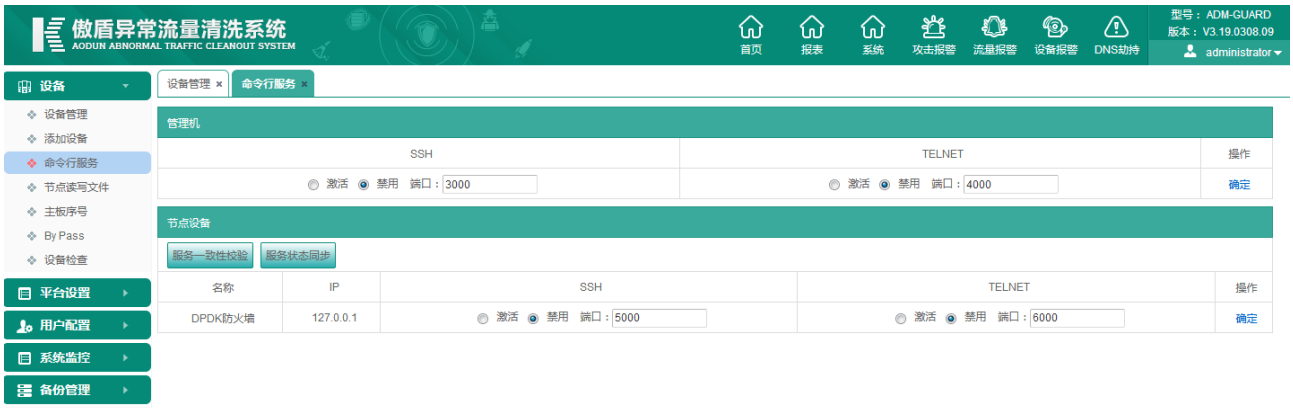
RIP 协议是最早的距离矢量型 IP 路由选择协议。当前存在两个版本，本节配置的是 RIPv1,它是应用于 IPv4 的。只要选择启动 RIP 后再点击应用配置既生效。

11.2 添加设备

如在实际环境中需添加集群设备可通过该模块添加。选择被添加产品的类型;(如异常流量清洗系统、异常流量检测系统)，设备名称自定义，IP 地址为清洗系统管理 IP 地址。

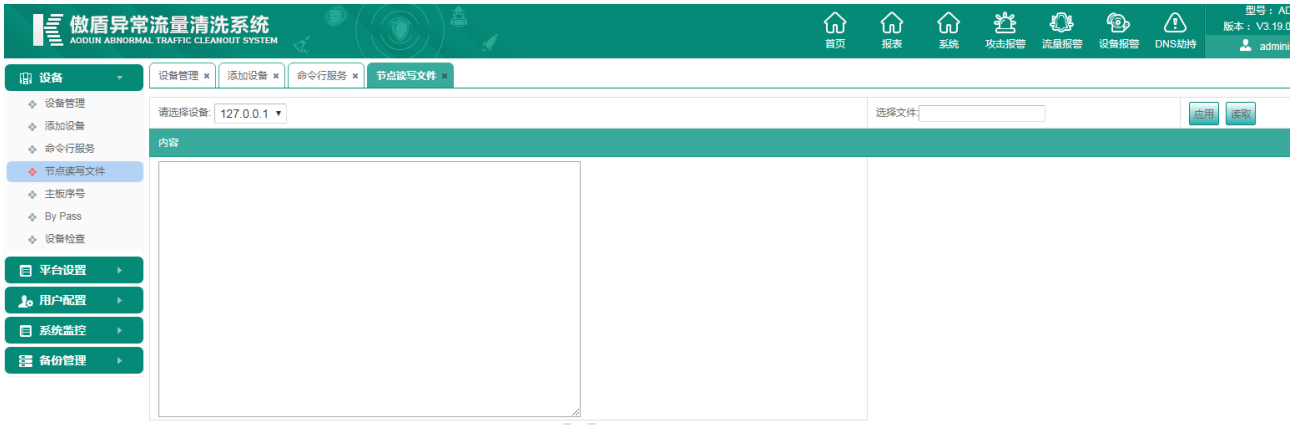
11.3 命令行服务

针对管理端、节点端设备开启 ssh 与 telnet 命令行功能，可根据实际自定义访问端口。根据服务一致性校验检查前台与后台是否一致，如不一致进行同步服务状态同步，以界面显示为准。



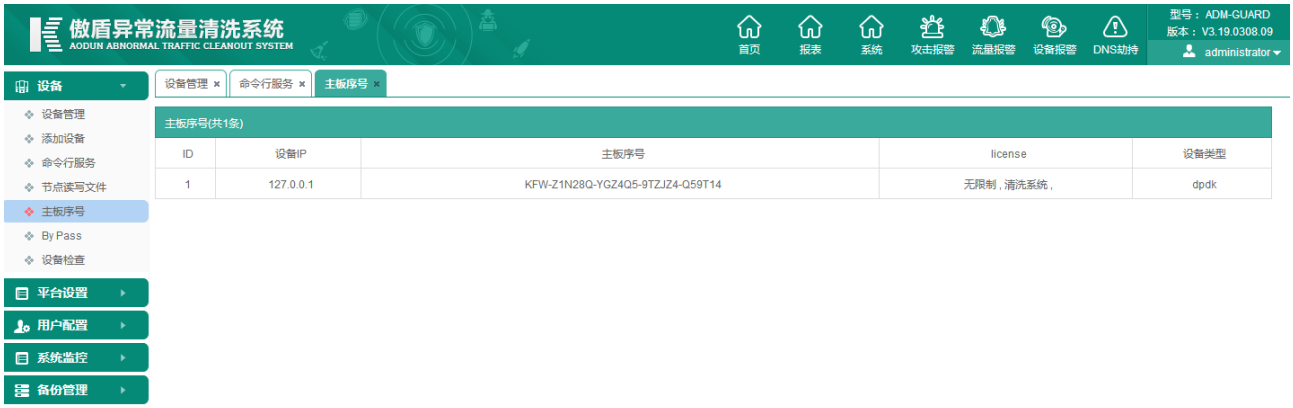
11.4 节点读写文件

管理员权限可通过读按钮取读设备信息。



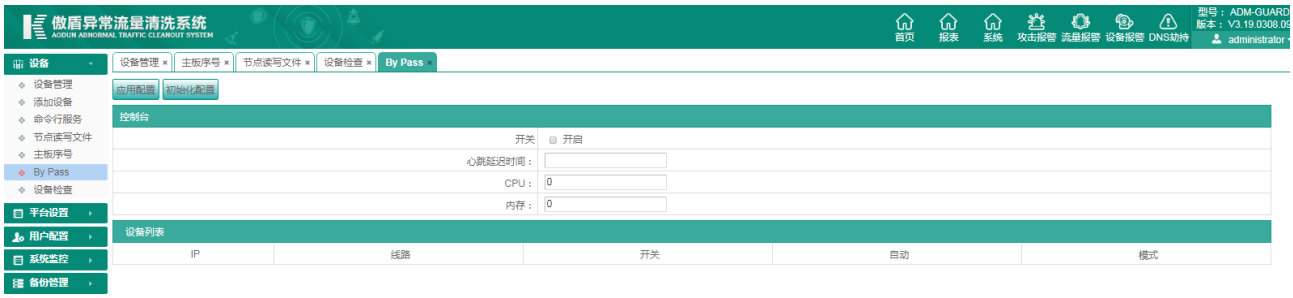
11.5 主板序号

主板序号列出每台清洗设备的序列号、硬件平台以及防护能力。



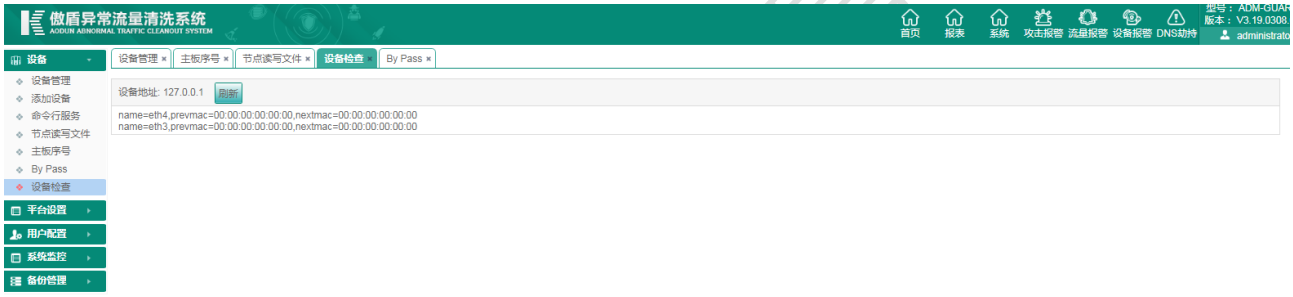
11.6 By pass

此设备支持软 by pass 模式，当设备开启了 cpu 内存检测，超过后会进行 bypas 模式，默认为关闭状态。



11.7 设备检查

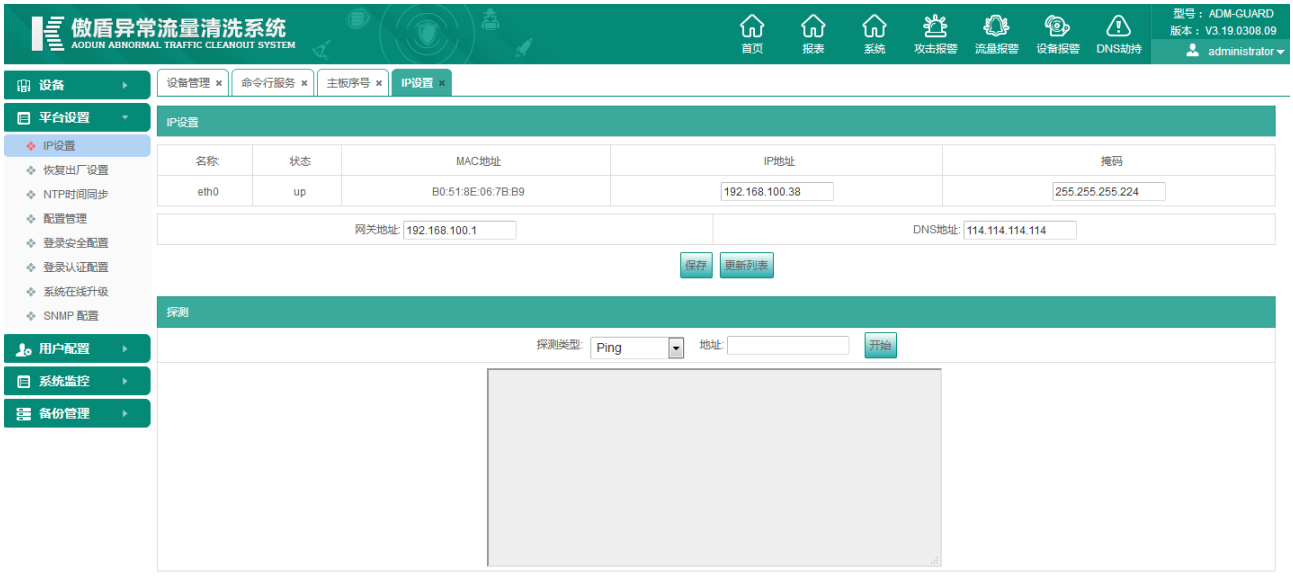
旁路部署时，方便查询设备是否学习到上一条端口接口 mac 地址，学到则判定设备回注策略正常。



12 系统 – 平台设置

12.1 IP 设置

配置设备管理 IP 地址。配置成功后，还可以进行系统向外的 ping 测试。



12.2 恢复出厂设置

恢复出厂设置会把当前用户的所有配置清空，还原到系统出厂配置。

12.3 NTP 时间同步

NTP 时间同步用于管理员设置当前管理机的时间。分可手动、自动 2 种同步方式。

12.4 配置管理

配置管理对系统的相关配置做备份与恢复。包括全部配置、牵引设置、域名过滤配置、服务器群组配置、DDoS 保护配置、DDoS 规则配置、系统配置、用户配置。

12.5 登录安全配置

密码过期设置用于定期提醒管理员更换 WEB 页面的登录密码。登录错误限制是防止非法人员恶意破解 WEB 页面的登录权限。登录模式选择可以让管理员切换访问 WEB 页面的方式。以及限制登录 WEB 页面的 IP 地址等。

12.6 登录认证配置

认证配置用于设置登录 WEB 页面的用户认证方式。

12.7 系统在线升级

在线升级需要联系傲盾工程师授权后进行升级，设计到升级过程中的细节，防止升级失败。

12.8 SNMP 设置

SNMP 设置用于设置当前系统的 SNMP。

13 系统 – 用户配置

13.1 用户

管理员可以通过权限分配，创建不同的账号分配不同的权限等级给使用此系统的其他运维人员。增加使用此系统的安全性。权限控制通过【权限】来控制。【禁用】选项可以禁止此用户登录系统。【大客户系统权限】主要是针对大客户账号的权限控制，大客户系统需要单独的端口来登录，通常是开放给某个大客户，该账号可以单独管理自己的 IP 地址、添加规则、查看相关日志信息等。【资源】选项用于关联大客户账号的 IP 地址段和规则集。

13.2 一次性账号

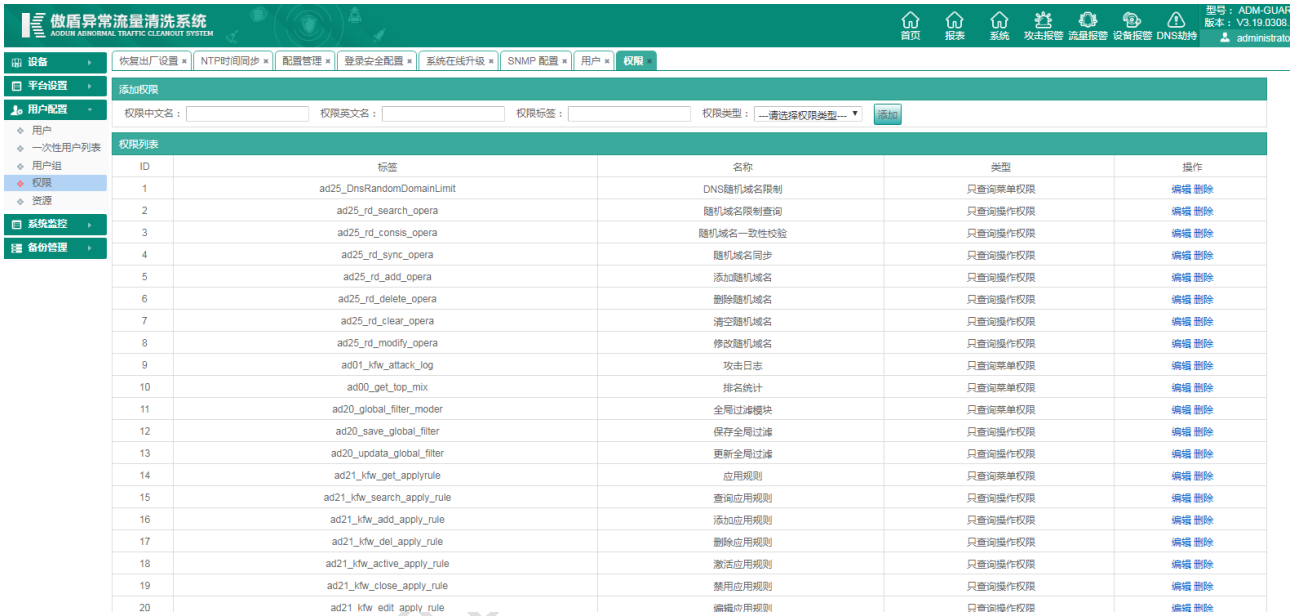
一次性账号主要是方便演示使用，当该账号登录过此系统，一旦退出，该账号就会被从系统中删除。

13.3 用户组

如果需要创建多个账号，并且所分配的权限是一样的。管理员可以通过创建用户组的方式，把这些账号添加到此组中，给该组分配权限。那么该用户组中的所有账号，将会得到相同的权限。减少管理员给账号分配权限的工作量。

13.4 权限

可根据不同模块进行设置为只查询菜单权限和只查询操作权限。



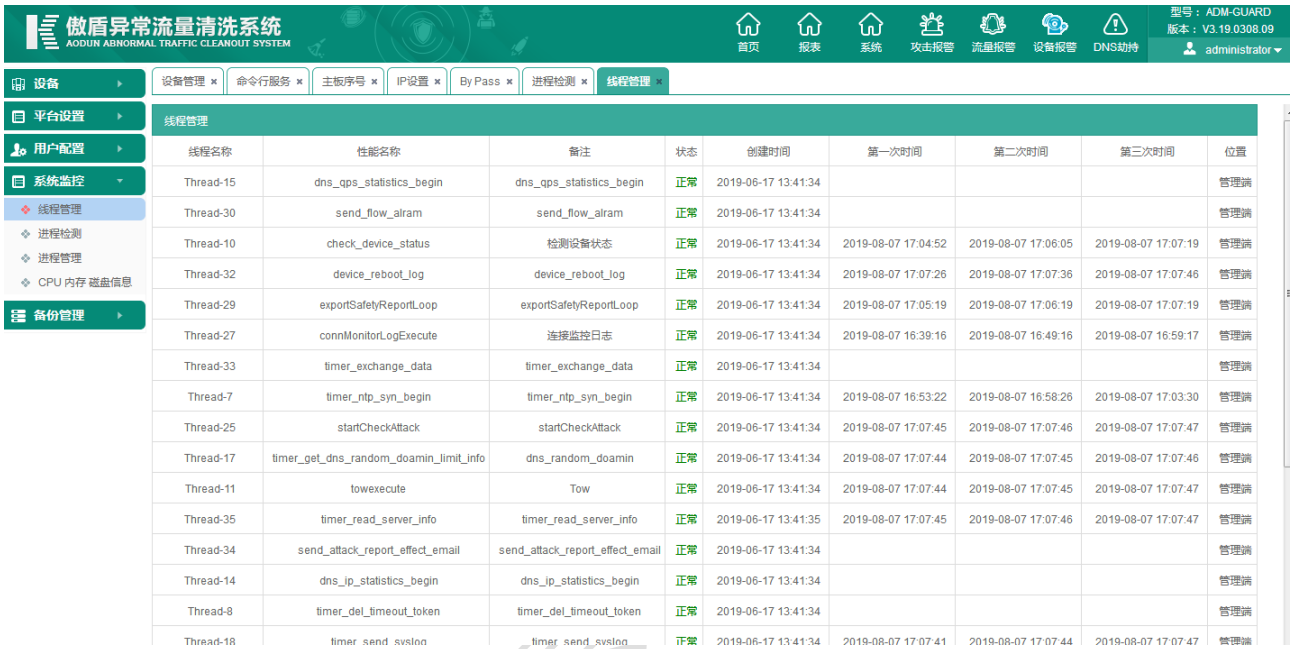
13.5 资源

在资源菜单中添加需要给大客户账号绑定的 IP 段。添加好后，在用户列表中【资源】选项中关联上这里添加的 IP 段。当使用此账号登录大客户系统时，这些 IP 段就会与该账号绑定在一起，从而达到让此账号只管理他自己的 IP 段的目的。

14 系统 - 系统监控

14.1 线程管理

管理员可查看系统的各个线程工作状态，线程创建时间，线程第一次、第二次，第三次被系统调用的时间。



线程名称	性能名称	备注	状态	创建时间	第一次时间	第二次时间	第三次时间	位置
Thread-15	dns_qps_statistics_begin	dns_qps_statistics_begin	正常	2019-06-17 13:41:34				管理端
Thread-30	send_flow_alram	send_flow_alram	正常	2019-06-17 13:41:34				管理端
Thread-10	check_device_status	检测设备状态	正常	2019-06-17 13:41:34	2019-08-07 17:04:52	2019-08-07 17:06:05	2019-08-07 17:07:19	管理端
Thread-32	device_reboot_log	device_reboot_log	正常	2019-06-17 13:41:34	2019-08-07 17:07:26	2019-08-07 17:07:36	2019-08-07 17:07:46	管理端
Thread-29	exportSafetyReportLoop	exportSafetyReportLoop	正常	2019-06-17 13:41:34	2019-08-07 17:05:19	2019-08-07 17:06:19	2019-08-07 17:07:19	管理端
Thread-27	connMonitorLogExecute	连接监控日志	正常	2019-06-17 13:41:34	2019-08-07 16:39:16	2019-08-07 16:49:16	2019-08-07 16:59:17	管理端
Thread-33	timer_exchange_data	timer_exchange_data	正常	2019-06-17 13:41:34				管理端
Thread-7	timer_ntp_syn_begin	timer_ntp_syn_begin	正常	2019-06-17 13:41:34	2019-08-07 16:53:22	2019-08-07 16:58:26	2019-08-07 17:03:30	管理端
Thread-25	startCheckAttack	startCheckAttack	正常	2019-06-17 13:41:34	2019-08-07 17:07:45	2019-08-07 17:07:46	2019-08-07 17:07:47	管理端
Thread-17	timer_get_dns_random_doamin_limit_info	dns_random_doamin	正常	2019-06-17 13:41:34	2019-08-07 17:07:44	2019-08-07 17:07:45	2019-08-07 17:07:46	管理端
Thread-11	towexecute	Tow	正常	2019-06-17 13:41:34	2019-08-07 17:07:44	2019-08-07 17:07:45	2019-08-07 17:07:47	管理端
Thread-35	timer_read_server_info	timer_read_server_info	正常	2019-06-17 13:41:35	2019-08-07 17:07:45	2019-08-07 17:07:46	2019-08-07 17:07:47	管理端
Thread-34	send_attack_report_effect_email	send_attack_report_effect_email	正常	2019-06-17 13:41:34				管理端
Thread-14	dns_ip_statistics_begin	dns_ip_statistics_begin	正常	2019-06-17 13:41:34				管理端
Thread-8	timer_del_timeout_token	timer_del_timeout_token	正常	2019-06-17 13:41:34				管理端
Thread-18	timer_send_syslog	timer_send_syslog	正常	2019-06-17 13:41:34	2019-08-07 17:07:41	2019-08-07 17:07:44	2019-08-07 17:07:47	管理端

14.2 进程检测

管理员可以查看系统的管理端进程与节点端进程工作状态。

分为管理端和设备，不通的设备在上方点击不同的模块即可

14.3 进程管理

默认有 managestart.pyc 管理端，manage.pyc 管理端和 nodestart.pyc 节点端为正常。

当缺少时可以进行添加，多出时进行删除即可。

14.4 CPU 内存 磁盘信息

管理员可查看管理机和节点设备的的 CPU 以及磁盘使用率。避免因资源不足导致系统异常的情况。

管理机信息：可以查看 CPU 使用百分比、内存使用百分比、剩余内存、剩余磁盘空间、剩余磁盘百分比

在管理机信息下方是设备信息，如果有多个设备可以通过点击不同的模块来选择要查看的设备

磁盘路径信息：可以自定义设置磁盘的路径信息（管理机）来单独查看这个路径的使用情况

15 系统 – 备份管理

15.1 MongoDB 配置

填写 mongodb 主机 ip、端口、用户名、密码、和数据库软件安装路径进行数据备份。

15.2 FTp 配置

填写 FTP 主机 ip、端口、用户名、密码、和 FTP 软件安装路径进行数据备份。

15.3 备份规则

可以根据自身需求进行手动或者自动规则备份，备份的文件可存入本地或者远端 ftp，需要备份远端 ftp 情况下需要先进行 ftp 配置。