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　　2019-12-03

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

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。

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

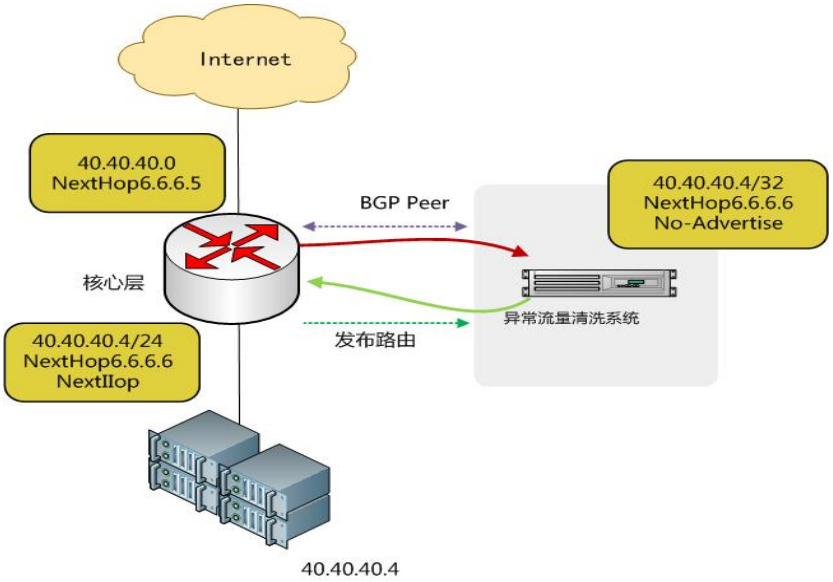
1.4 关于网络安全

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 – 全局过滤模块防护说明

3.1 防护原理

全局过滤规则是由全局触发规则加全局过滤模块组成，对设备识别到的所有防护 IP 都生效。主要防护:Syn Flood、Ack Flood、Psh+Ack Flood、Rst Flood、Udp Flood、Icmp Flood、other Flood 等。

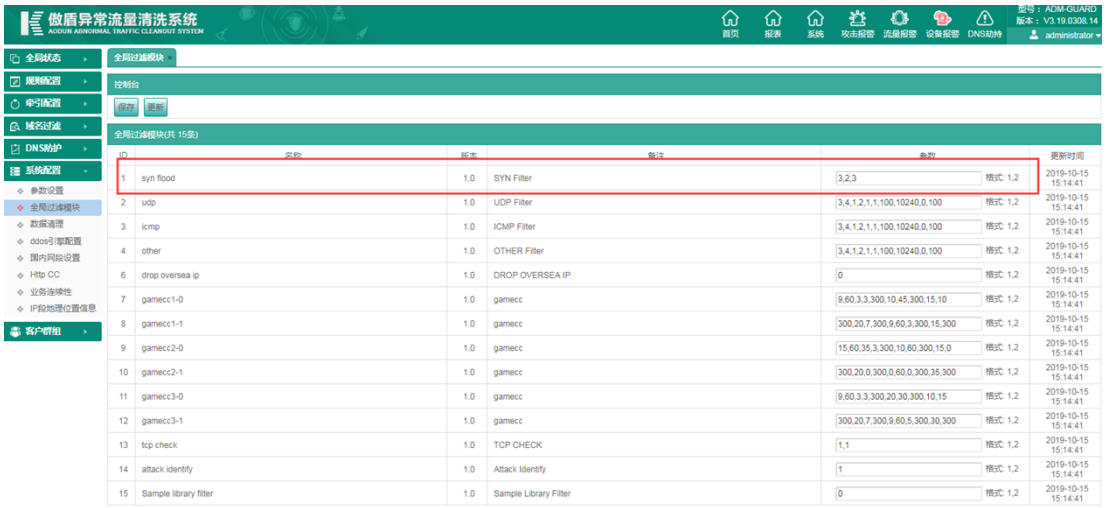
使用方法：当防护 IP 触发了全局触发规则后，会智能启用全局过滤模块，自动对传输协议特征过滤，同时对传输的数据进行采样比对，采样比对后的数据再分别发送给不同的模块进行更深层分析，比如 HTTP、DNS、UDP 音频视频传输、TCP 游戏数据等。从而最大限度的保证完全自动过滤掉攻击数据，让合法数据安全通过。

3.2 单 IP 全局触发参数定制

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。如针对较特殊业务 ip，可通过查看服务器列表观察正常状态时每秒 tcp 包数、UDP 包数、ICMP 包数等，默认可将其参数调整到平时业务量的 2 倍。

以 SYN FLOOD 攻击为例：通过全局 syn 模块高效率的防护 syn Flood 攻击。

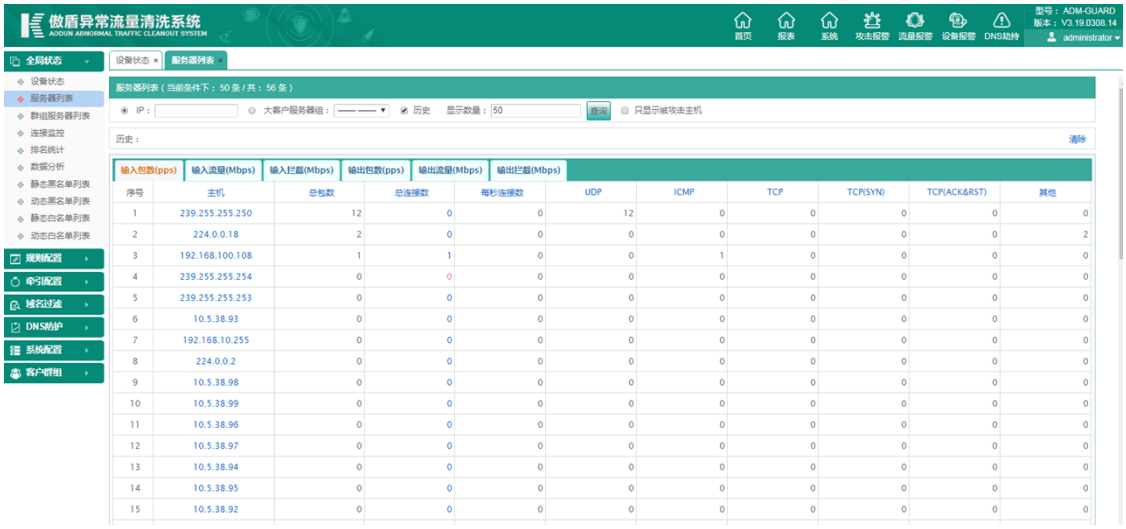
1.在【首页】-【系统配置】-【全局过滤模块】中查看 SYN Fileter 参数的第一位是否为 0，0 表示不开启 syn 防护验证，防护 SYN FLOOD 攻击必须开启 syn 防护验证。



2.在【首页】-【规则配置】-【触发规则】-【全局触发规则】中查看【S_globar Trigger】规则中每秒 TCP 包数、每秒 SYN 包数触发条件，建议使用默认【S_globar Trigger】触发值。

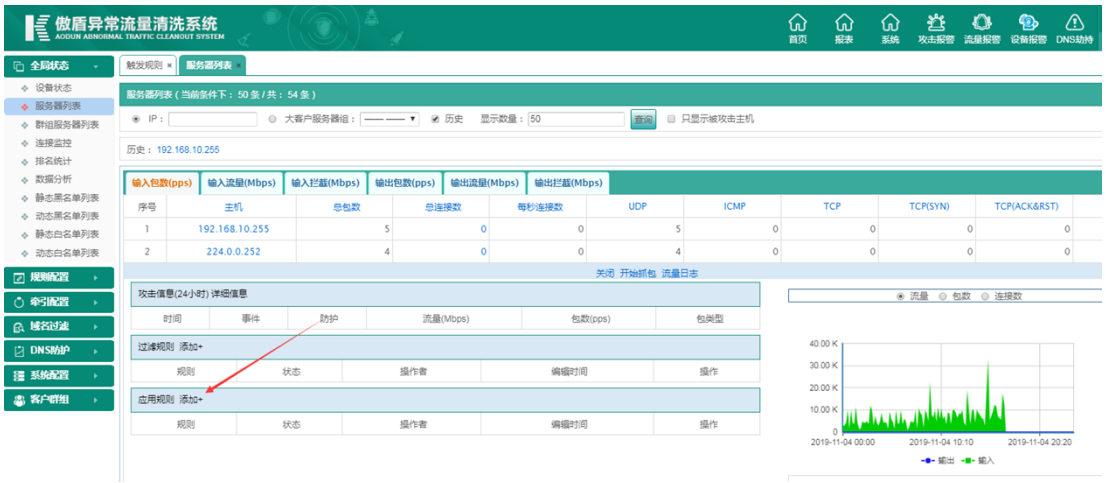
3.如需对单个防护 ip 修改全局触发规则，根据服务器列表单 ip 平时每秒 tcp 和 syn 包数自定义，最后通过应用规则把新建全局触发参数应用在此 ip 上。

在【首页】-【服务器列表】对应 ip 观察平时正常流量每秒每秒 tcp 和 syn 报数。



在【首页】-【规则配置】-【触发规则】-【全局触发规则】中新建添加一条【定制 ip 触发参数】

应用在 ip 上，在【首页】-【全局状态】-【服务器列表】中找到对应 ip 点击应该规则的添加，全局触发规则中，选中【定制 ip 触发参数】保存即可生效。



4.若某个防护 IP 添加了应用规则，检查【首页】-【规则配置】-【应用规则】中 syn 模块选项是否勾选,未勾选则未开启 syn 智能防护过滤。

4 首页 – 过滤规则使用

4.1 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；

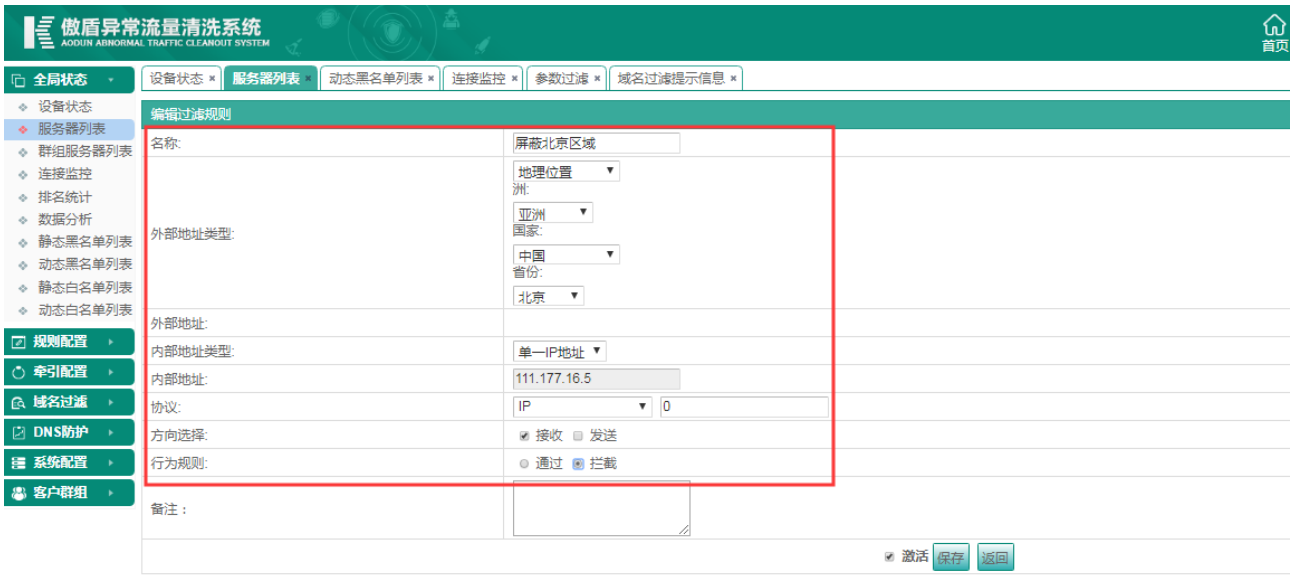
行为规则：指触发此规则后数据处理行为，这里有两种行为：通过（直接把流量送达到达服务器）、

拦截。

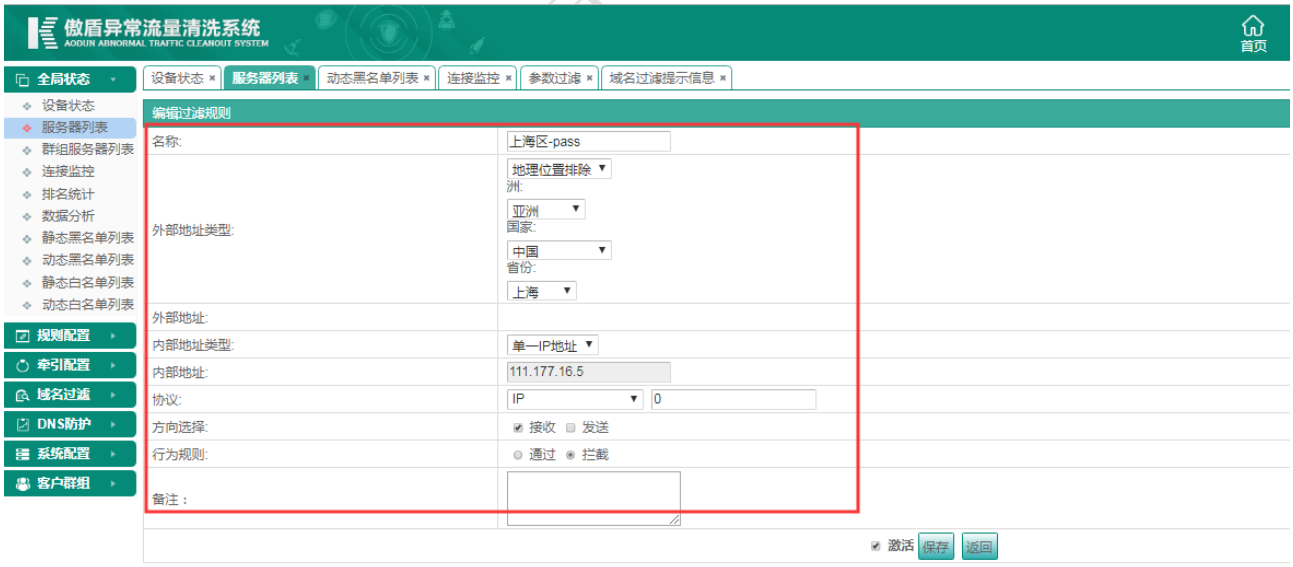
备注：自定义要备注的信息

4.2 区域访问过滤规则配置

以通过过滤规则做屏蔽北京地区进行访问服务器为例：



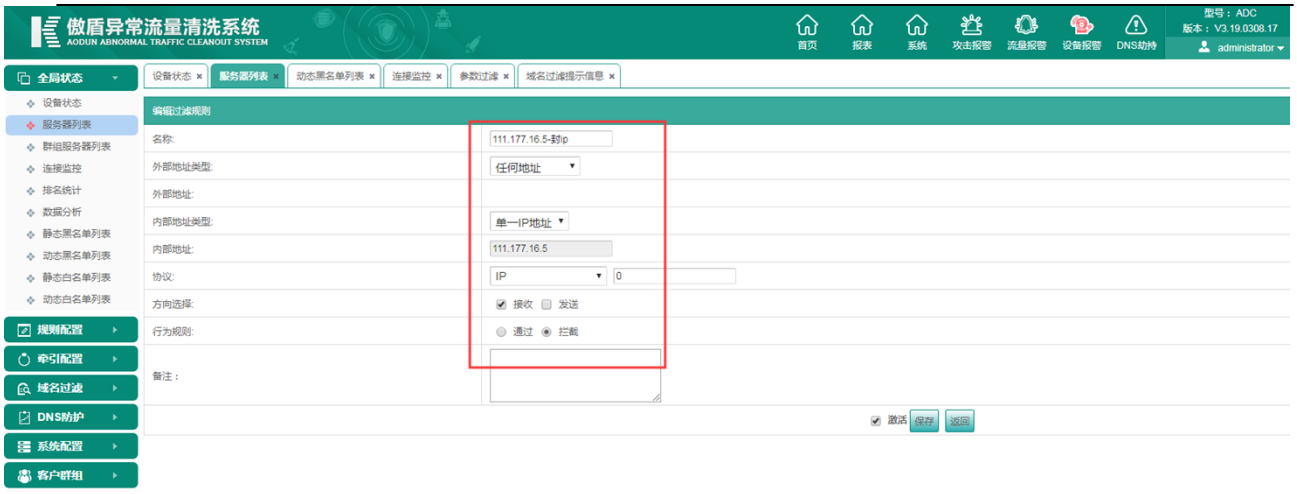
除此之外，还可以根据用户需求做到地里配置排除法，以下为例：只允许上海地区进行访问



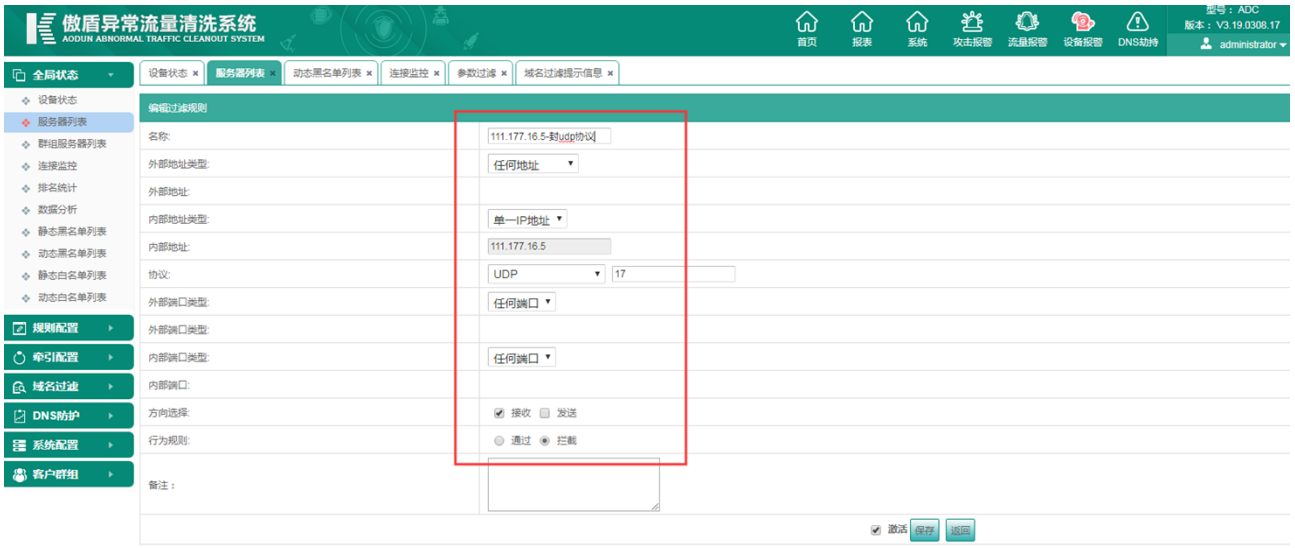
4.3 过滤规则配置示例

过滤规则类似于 ACL，每个 IP 最多添加 10 条，使用简单快捷有效。当有多条过滤规则时，从上到下依次匹配过滤。以下做几个示例：

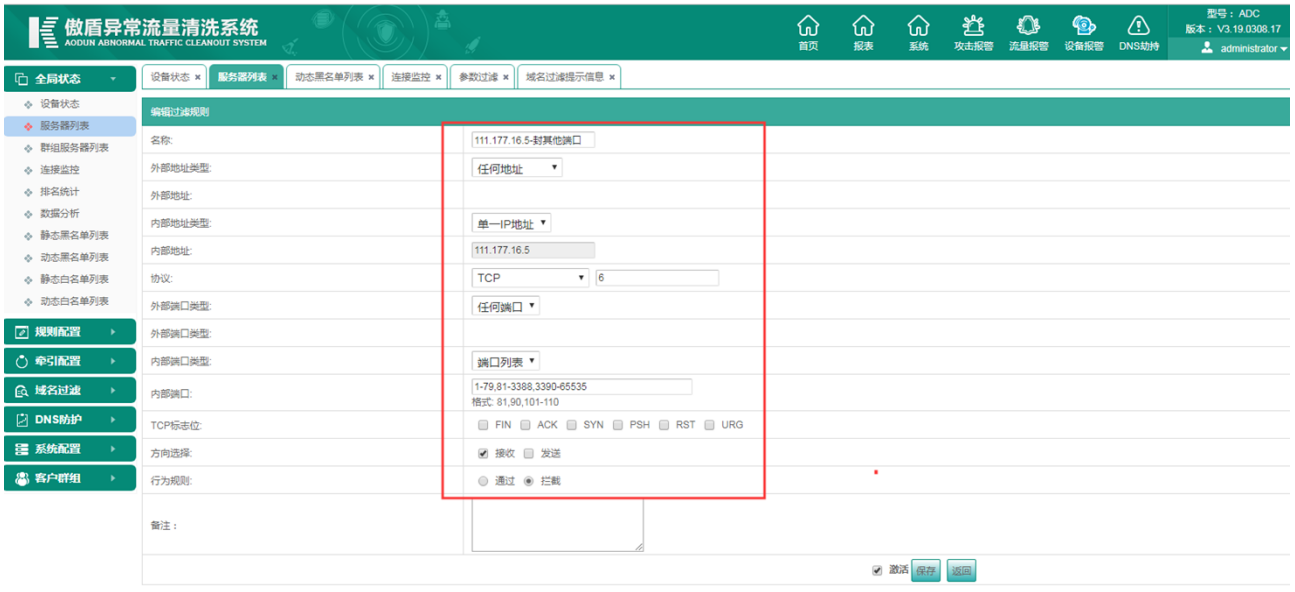
示例一：封堵 ip



示例二：封堵 udp 协议



示例三：封除业务端口 80/3389tcp 协议远程端口



5 首页 – 插件使用说明

5.1 S_HTTP_CC V2.1 插件说明

插件序列号为 10 为 HTTP CC

默认值 0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0

1 验证方式 0:小尾巴 1:按钮 2:问题 其它：按钮

2

3

4

5 syn 每秒触发数

6 ack 每秒触发数

小尾巴验证：

当源 ip 触发到全局触发规则，外部源向服务器的请求，防火墙会代理服务器回应一个带 url 的数据包，再次验证通过的时候，会加入白名单 9999s，超过白名单时间会再次验证。没验证成功默认会加入黑名单 9999S

按钮验证：

当源 ip 触发到全局触发规则，外部源向服务器的请求，防火墙会向源回应带按钮验证界面，需要人工手动通过后会加入白名单 9999s，超过白名单时间会再次验证。没验证成功默认会加入黑名单 9999S

问题验证：

当源 ip 触发到全局触发规则，外部源向服务器的请求，需要先通过防火墙提供的问题验证，通过后会加入白名单 9999s，超过白名单时间会再次验证。没验证成功默认会加入黑名单 9999S

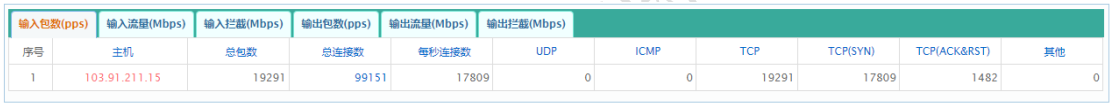
5.1.1 S_HTTP_CC V2.1 小尾巴验证

5.1.2 S_HTTP_CC V2.1 按钮验证

5.1.3 S_HTTP_CC V2.1 问题验证

5.2 S_HTTP_CC V2.1 插件使用场景

1.当前总的连接数很大，几千或者上万，每秒新建连接数非常大。



序号	主机	总包数	总连接数	每秒连接数	UDP	ICMP	TCP	TCP(SYN)	TCP(ACK&RST)	其他
1	103.91.211.15	19291	99151	17809	0	0	19291	17809	1482	0

2.连接数统计：很多源 ip 连接目的 ip 连接数量大

连接统计 (共 50条)

序号	源IP	目的IP	目的端口	连接次数	操作
1	116.228.123.138	103.91.211.15	-	636	添加黑名单
2	222.180.12.70	103.91.211.15	-	255	添加黑名单
3	202.114.123.62	103.91.211.15	-	253	添加黑名单
4	222.139.212.117	103.91.211.15	-	199	添加黑名单
5	122.226.184.234	103.91.211.15	-	173	添加黑名单
6	122.226.184.235	103.91.211.15	-	49	添加黑名单
7	116.26.126.224	103.91.211.15	-	26	添加黑名单
8	116.26.124.40	103.91.211.15	-	25	添加黑名单
9	118.122.237.174	103.91.211.15	-	22	添加黑名单

3.通过抓包分析数据包，很多异常连接，源 ip 不固定

记录分析 (共 300 条)

序号	CODE	时间	源IP	源端口	目的IP	目的端口	协议	TTL	TCP 标志位	包大小	操作
1	0	2019-01-11 13:41:38	123.132.224.34	50656	103.91.211.15	81	TCP	119	SYN /47	66	分析 下载
2	0	2019-01-11 13:41:38	115.215.113.190	18621	103.91.211.15	81	TCP	118	SYN /47	66	分析 下载
3	0	2019-01-11 13:41:38	121.27.167.114	51042	103.91.211.15	81	TCP	54	SYN /47	66	分析 下载
4	0	2019-01-11 13:41:38	115.198.89.185	52258	103.91.211.15	81	TCP	118	SYN /47	66	分析 下载
5	0	2019-01-11 13:41:38	218.76.14.18	1433	103.91.211.15	61061	TCP	116	PSH ACK /47	88	分析 下载
6	0	2019-01-11 13:41:38	171.116.67.237	58201	103.91.211.15	81	TCP	118	SYN /47	62	分析 下载
7	0	2019-01-11 13:41:38	113.247.175.139	13505	103.91.211.15	81	TCP	117	SYN /47	66	分析 下载
8	0	2019-01-11 13:41:38	220.169.229.78	56218	103.91.211.15	81	TCP	52	SYN /47	62	分析 下载
9	0	2019-01-11 13:41:38	219.144.129.69	60696	103.91.211.15	81	TCP	53	SYN /47	66	分析 下载
10	0	2019-01-11 13:41:38	88.248.172.206	52091	103.91.211.15	81	TCP	97	SYN /47	62	分析 下载
11	0	2019-01-11 13:41:38	60.180.197.93	24172	103.91.211.15	81	TCP	54	SYN /47	62	分析 下载
12	0	2019-01-11 13:41:38	117.153.14.37	7956	103.91.211.15	81	TCP	53	SYN /47	74	分析 下载
13	0	2019-01-11 13:41:38	27.224.105.196	43848	103.91.211.15	81	TCP	116	SYN /47	62	分析 下载
14	0	2019-01-11 13:41:38	42.239.70.192	28775	103.91.211.15	81	TCP	54	SYN /47	62	分析 下载
15	0	2019-01-11 13:41:38	188.13.50.16	3459	103.91.211.15	81	TCP	112	SYN /47	62	分析 下载
16	0	2019-01-11 13:41:38	218.76.14.18	1433	103.91.211.15	61116	TCP	116	PSH ACK /47	248	分析 下载
17	0	2019-01-11 13:41:38	218.76.14.18	1433	103.91.211.15	61087	TCP	116	PSH ACK /47	248	分析 下载
18	0	2019-01-11 13:41:38	49.79.216.146	6929	103.91.211.15	81	TCP	119	SYN /47	62	分析 下载
19	0	2019-01-11 13:41:38	124.77.77.108	59318	103.91.211.15	81	TCP	118	SYN /47	62	分析 下载

当遇到以上现象，切业务为 web 业务，就可应用 S_HTTP_CCV2.1 规则来进行防御。

5.3 CTmanage 插件说明

5.3.1 CTmanage 参数

Ctmanage 连接控制插件有 7 个参数

第一位 表示是否开启超出连接限制时加黑，置1表示 加黑并释放 置0表示只释放连接不加黑源IP

第二位 表示空连接探测时间，即tcp双方建立连接后，在此段时间内没有数据传输，便判定为一个空连接

第三位 源 IP 与服务器可以建立的连接上限，当一个源 IP 地址与服务建立的连接数超过此值时，如果参数一置为 1 时，源 IP 被加黑 10000 秒

第四位 置 0，保留

第六位 置 0，保留

第七位 置 0，保留

第七位 置 1 开启延时提交，0 表示不开启延时提交。**（*串接场景下使用，旁路场景开启后会导致业务不通）**

5.4 CTmanage 插件使用场景

Ctmanage 连接控制插件适用于 game 业务，针对那种进行三次握手建立 tcp 连接后，双方不进行数据交换且保存长连接的攻击进行防护。

6 首页 – 应用规则使用

6.1 应用层防护原理

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：如图 6.1

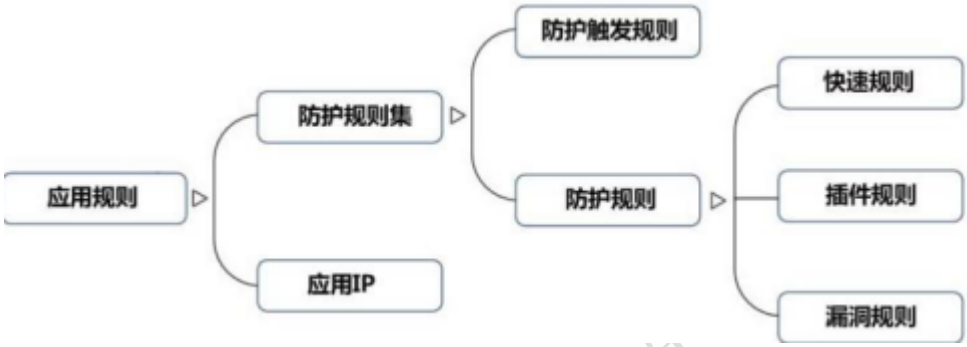
图 6-1

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。

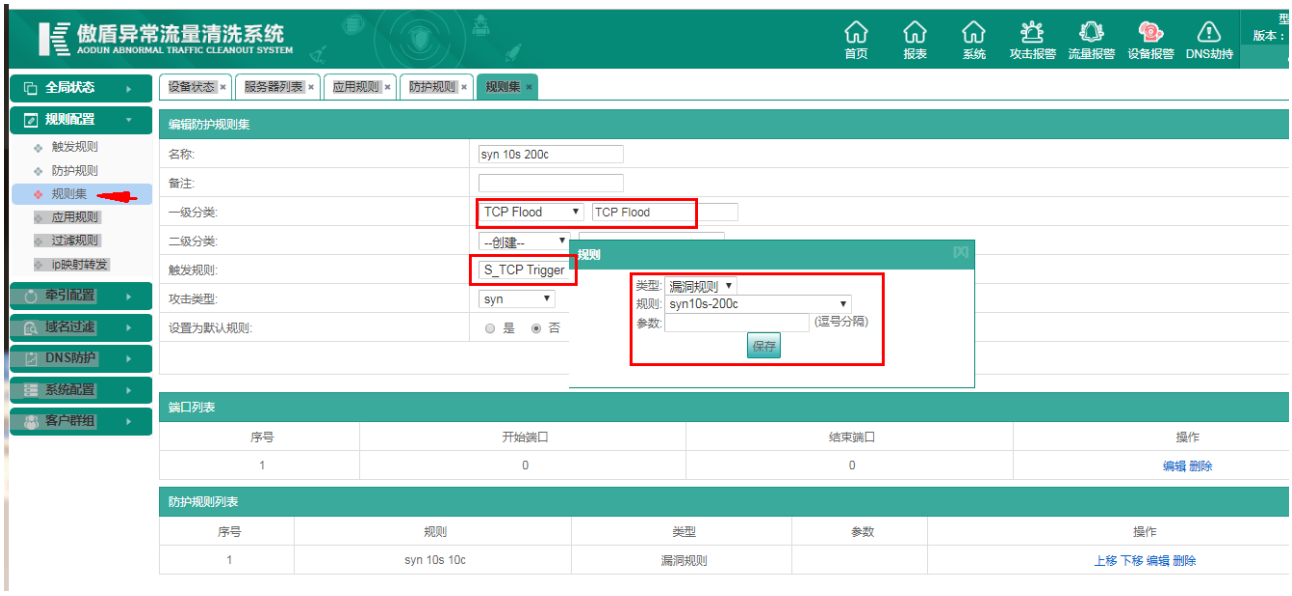
通过全局过滤模块的数据包将被送入过滤规则进行过滤，过滤规则对数据包进行简单有效的过滤。对于放行的数据包则会转入应用规则模块过滤。域名插件主要用于协助管理员对本机房域名进行审查，所有本机房备案与未备案的域名是否能被外网访问，将会在这里得到控制。流量控制模块则会对最终流向服务器的数据流进行最终的流量限制,最后转发至服务器。

6.2 自定义规则配置示例

应用规则：由防护规则集及本地服务器 IP 组成，防护规则如下图所示可实现功能强大的过滤策略。以下做几个示例。



示例一：做 syn 限速（syn10s-200c）



6.3 屏蔽国外 IP 配置

此设置支持屏蔽国外 ip，首先需要导入国内 ip 地址网段。 之后在应用规则中勾选可信源检如下图所示：

7 首页 - 牵引引流配置

7.1 引流牵引概述

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。

7.2 引流牵引设备

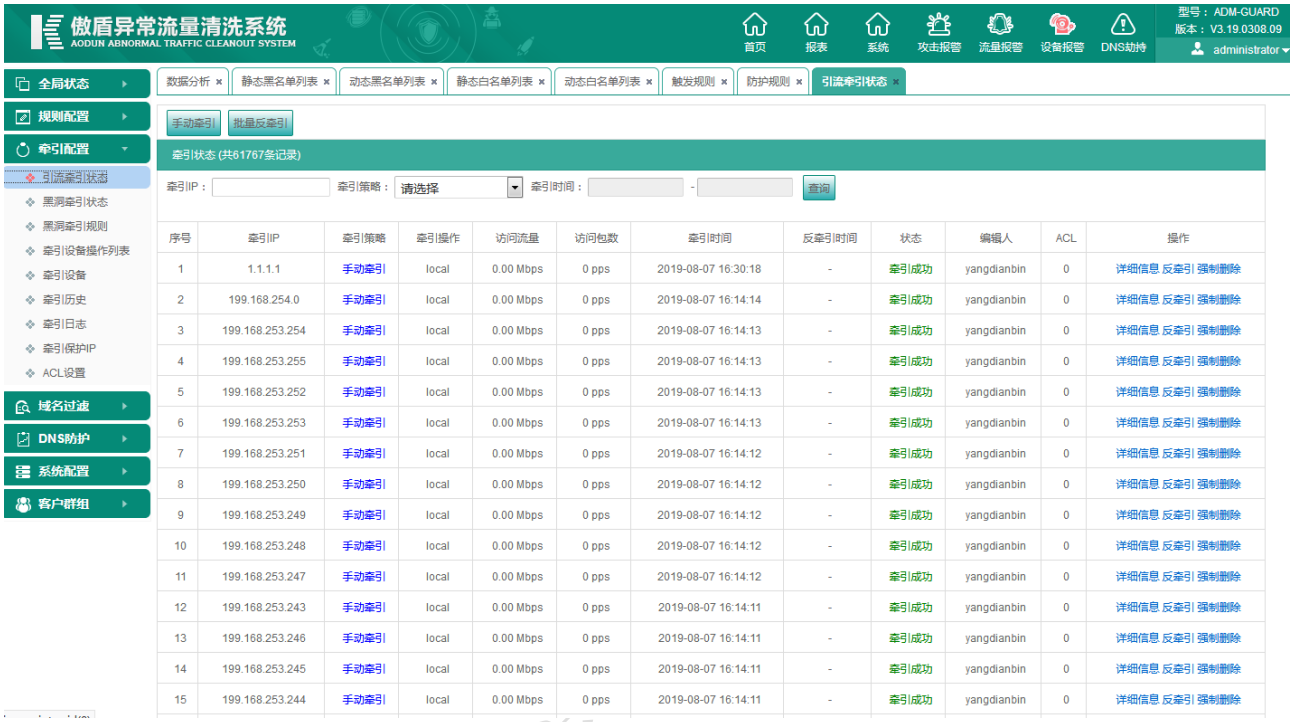
牵引设备是指用于引流的清洗设备或者上层封 IP 的交换机。引流时，牵引设备就是清洗设备本身。在添加时，可以选择 telnet 设备，IP 为每台清洗设备的管理口地址，端口对应清洗设备路由模块所监听的端口 16020。需要在上层封 IP 时，牵引设备就是该交换机对应的地址，系统支持 telnet、ssh 和 webservice 登录。条件好的牵引设备支持导入导出。

7.3 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。

7.4 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。



8 首页 – 黑洞封堵配置

8.1 黑洞牵引概述

黑洞：借助上层核心路由设备，在傲盾异常流量清洗系统上预置黑洞牵引策略，可实现对大流量攻击进行封堵，从而达到保护机房链路带宽的目的 。

8.2 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。

8.3 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。

9 首页 – 域名过滤配置

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。

9.1 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。

9.2 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。

9.3 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。

9.4 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。

10 首页 - 客户群组配置

10.1 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。

10.2 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。

10.3 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。

10.4 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。

10.5 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。

11 如何判断服务器 ip 有攻击？

11.1 服务器列表

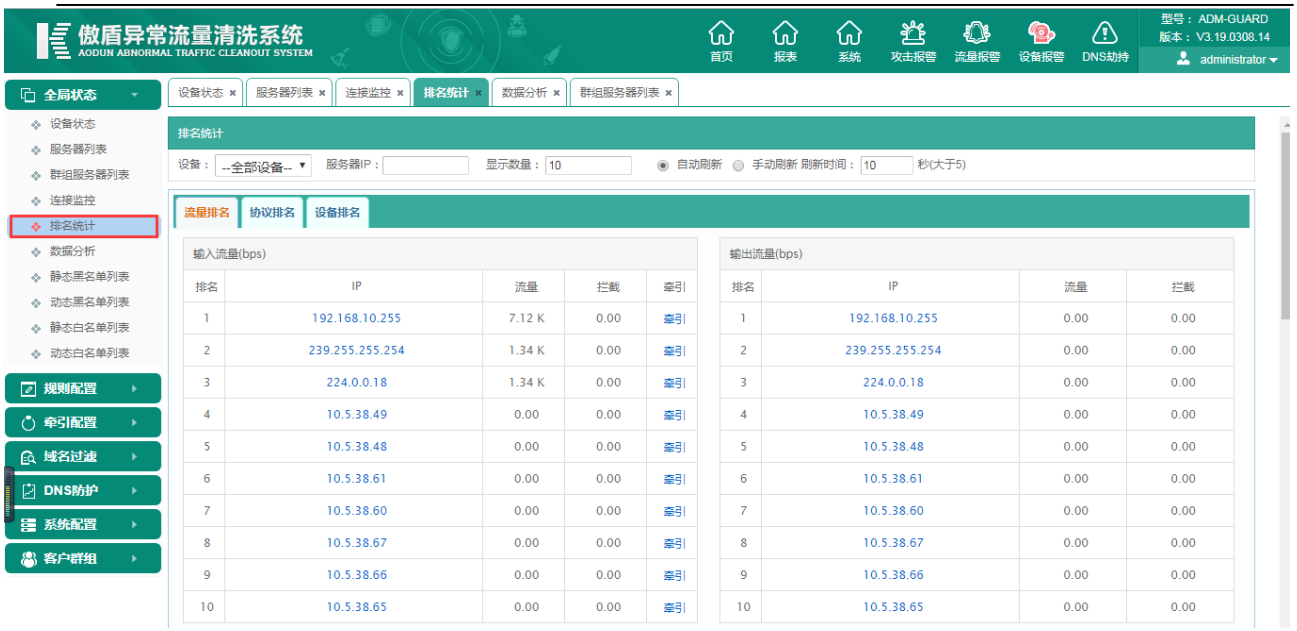
登陆防火墙点击【全局状态】-【服务器列表】查看此 IP 每秒新建连接数是否超过 300,总连接数是否超过 3000(凡业务量大的 IP 例外)，超过则判断有 SYN 或者 CC 攻击如下图所示;

11.2 连接监控

通过防火墙首页->全局状态下通过连接监控可以按照源目 IP、源目端口及协议查看哪些 IP 可能收到攻击。

11.3 统计排名

通过防火墙首页->全局状态下通过统计排名可以从流量、协议和设备方面查看哪些服务器 IP 可能遭受了攻击

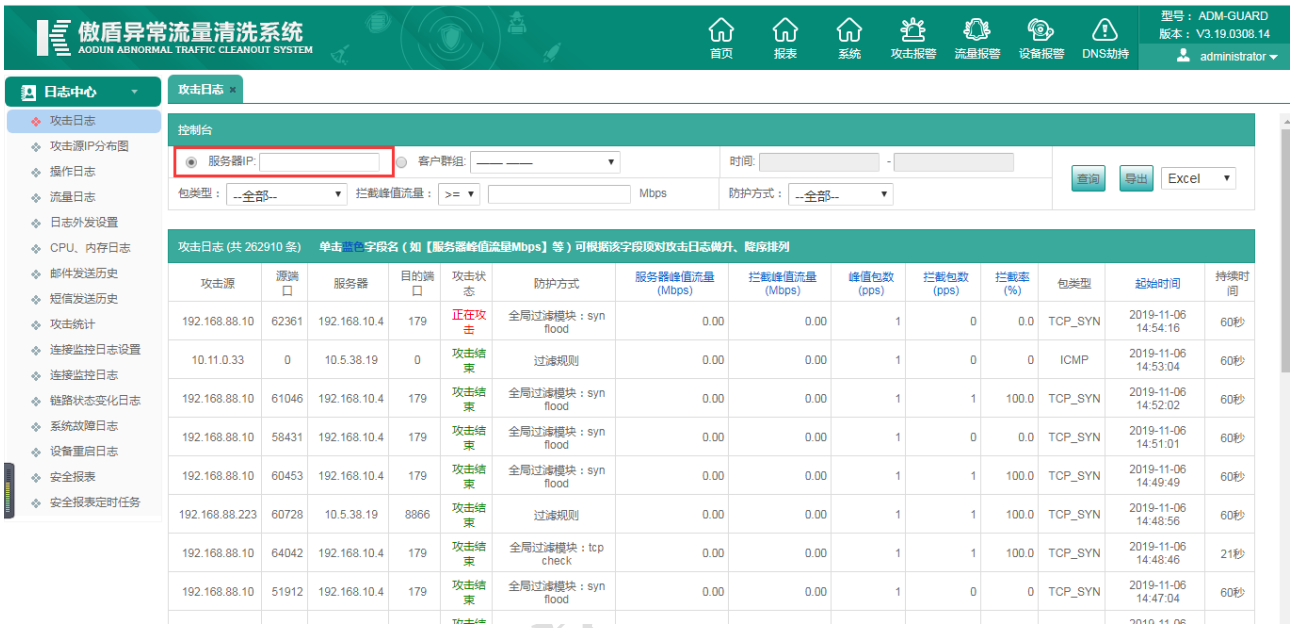

傲盾异常流量清洗系统
AODUN ABNORMAL TRAFFIC CLEANOUT SYSTEM
首页
报表
系统
攻击报警
流量报警
设备报警
DNS劫持
型号：ADM-GUARD
版本：V3.19.0308.14
administrator
全局状态
设备状态
服务器列表
群组服务器列表
连接监控
排名统计
数据分析
静态黑名单列表
动态黑名单列表
静态白名单列表
动态白名单列表
规则配置
牵引配置
域名过滤
DNS防护
系统配置
客户群组
设备状态 ×
服务器列表 ×
连接监控 ×
排名统计 ×
数据分析 ×
群组服务器列表 ×
排名统计
设备：--全部设备--
服务器IP：
显示数量：10
自动刷新
手动刷新 刷新时间：10
秒(大于5)
流量排名
协议排名
设备排名
输入流量(bps)
排名 IP 流量 拦截 牵引
1 192.168.10.255 7.12 K 0.00 牵引
2 239.255.255.254 1.34 K 0.00 牵引
3 224.0.0.18 1.34 K 0.00 牵引
4 10.5.38.49 0.00 0.00 牵引
5 10.5.38.48 0.00 0.00 牵引
6 10.5.38.61 0.00 0.00 牵引
7 10.5.38.60 0.00 0.00 牵引
8 10.5.38.67 0.00 0.00 牵引
9 10.5.38.66 0.00 0.00 牵引
10 10.5.38.65 0.00 0.00 牵引
输出流量(bps)
排名 IP 流量 拦截
1 192.168.10.255 0.00 0.00
2 239.255.255.254 0.00 0.00
3 224.0.0.18 0.00 0.00
4 10.5.38.49 0.00 0.00
5 10.5.38.48 0.00 0.00
6 10.5.38.61 0.00 0.00
7 10.5.38.60 0.00 0.00
8 10.5.38.67 0.00 0.00
9 10.5.38.66 0.00 0.00
10 10.5.38.65 0.00 0.00

12 遇到被攻击 ip 该如何处理？

12.1 攻击拦截

在确定某一台服务器被攻击后，我们要第一时间进行拦截，最大程度上保证用户的内网安全。

在我们的防火墙上有攻击日志，将受到攻击的 IP 地址填到服务器 IP 中，就可以很快找到攻击源 IP；

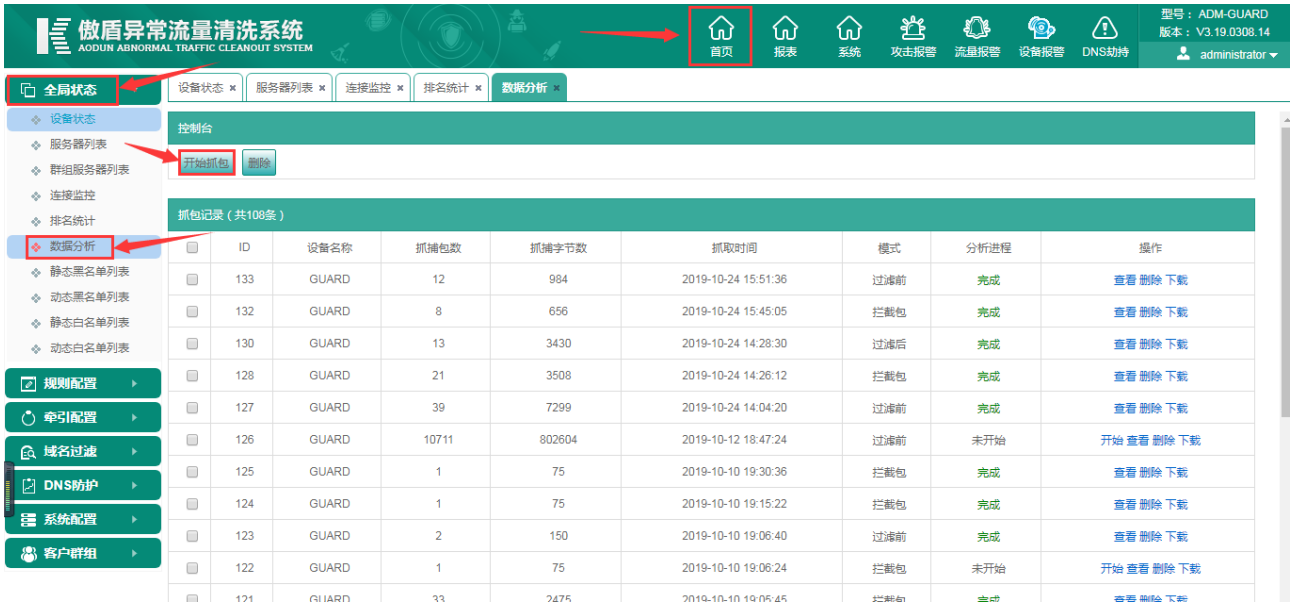


在找到攻击源 IP 之后直接将此 IP 填到防火墙的静态黑名单中即可对其进行拦截。

12.2 攻击溯源

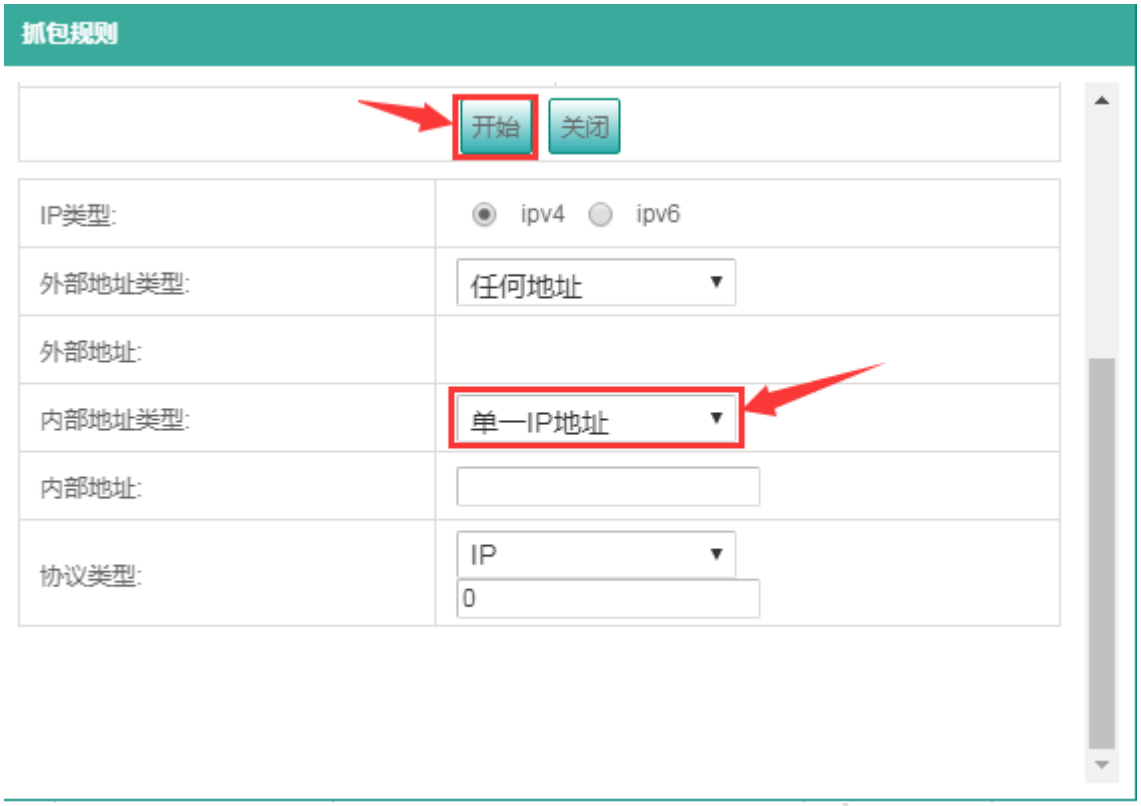
在成功拦截攻击之后，我们需要通过防火墙自带的抓包工具进一步的找到攻击源 IP，将此 IP 加入静态黑名单中，从源头上杜绝此 IP 再次对服务器进行攻击。

抓包工具：打开首页->全局状态->数据分析->开始抓包就可以自定义设置抓包的规则了



抓包方式选择抓取指定 IP 数据包，再将强制抓包勾选上；

内部地址选为单一 IP 地址后将被攻击的 IP 地址填写进去就可以开始抓包了。



12.3 攻击防护

现如今，网络的发展可谓是日新月异，而黑客的攻击手段也是在不断地发生变化，这时就需要一些有效的防御手段来抵挡黑客的攻击。

在我们的防火墙上有很多可以根据自身情况自定义调整的规则，如上述提到的过滤规则、插件规则、应用规则、防护规则等，他们都可以在一定范围内保护服务器免遭黑客攻击，真正做到事前有防护，事中有拦截，事后有溯源这三位一体的全方位保护。