中新金盾抗拒绝服务系统

（使用手册）

中新网络信息安全股份有限公司

文档编码：ZXS-TD-DMS 01 使用手册-v4.0

■ 文档变更记录

时间	版本	说明	修改人	审核人
2019-08-23	V3.1	部分内容修改	王斌	解义庆
2020-03-16	V4.0	增加聚合，路由，修改部分参数，产品型号等	王斌	解义庆

目 录

1 系统登录 3
1.1 用户登录 3
1.2 主界面介绍 4
1.3 设置管理地址 5
1.4 用户切换 7
2 状态监控 8
2.1 全局统计 8
2.2 系统负载 8
2.3 防护范围 9
2.3.1 手工添加防护范围地址 10
2.3.2 批量导入防护范围地址 11
2.4 主机状态 12
2.4.1 主机设置 15
2.5 连接监控 17
2.6 屏蔽列表 18
2.7 黑白名单 20
2.7.1 手工添加黑白名单条目 20
2.7.2 批量导入黑白名单条目 21
2.8 域名管理 22
3 攻击防御 24
3.1 全局参数 24
3.1.1 系统操作环境 24
3.1.2 系统防护参数 25
3.1.3 主机防护参数 26
3.1.4 系统变量设置 28
3.2 规则设置 32
3.2.1 规则列表 33
3.2.2 规则编辑页面 33
3.3 TCP 端口保护 35
3.3.1 TCP 端口配置 36
3.3.2 开启防护模块 38
3.3.3 插件参数 39
3.4 UDP 端口保护 49
3.4.1 添加 UDP 端口保护 50
3.4.2 UDP APP Protection v1.1 51
3.4.3 DNS 防护插件防御 51
3.4.4 开启插件 52
3.5 牵引设置 53

3.6 变量设置.....55
4 日志分析.....56
4.1 日志列表.....56
4.2 攻击分析.....57
4.3 分析报告.....58
4.4 TOP 分析.....59
4.5 流量分析.....60
4.6 连接分析.....61
4.7 事件分析.....61
4.8 性能分析.....62
4.9 攻击档案.....63
4.10 报表管理.....63
5 系统配置.....65
5.1 保存配置.....65
5.2 系统设备.....66
5.3 聚合管理.....67
5.4 集群参数.....69
5.5 控管属性.....70
5.6 路由协议.....72
5.7 用户组管理.....72
5.8 用户管理.....73
5.9 时间设定.....74
5.10 SNMP 系统.....75
5.11 SNMP Trap.....76
5.12 SNMP 用户.....76
5.13 SNMP 视图.....77
6 服务与支持.....79
6.1 关于我们.....79
6.2 报文捕捉.....79

前言

文档范围

本文涵盖中新金盾抗拒绝服务系统主要功能特点，并以 ZX-DMS 5120AC 产品为例详细介绍其使用方法。

本手册仅作为使用参考，实际产品可能会由于版本升级或者其它原因，与手册描述的内容有略微的差异。

文档用途

本手册主要用途是帮助运维或技术支持等人员了解产品功能，并熟悉和正确使用 ZX-DMS 产品。

读者对象

本文假设读者已经对 TCP/IP 协议、Linux 和 Windows 操作系统等相关知识有一定了解，文中不再赘述此类知识。

本手册主要适用于以下工程师：

- 网络运维工程师
- 网络管理工程师
- 技术支持工程师

格式约定

斜体字 —— 用户输入或非固定的变量

粗体字 —— 关键字和脚本

 —— 说明：引用信息或对文本内容的补充

 —— 提示：使用过程中的建议与技巧

 —— 注意：重要信息和需要特别明确的事项

【XXX】 —— 功能按键的表示方式

【XX】→【XX】—— 操作步骤向导

获取帮助

如果需要获取产品其它信息，请访问中新网安官方网站：http://www.cnzxsoft.com

如果对本文有不能理解的地方或者想要了解其它关于中新网安的信息，请通过以下方式与我们取得联系：

客户服务热线：**400-060-7722**（7 x 24 小时在线）

邮箱：sc@cnzxsoft.com

官方网站：http://www.cnzxsoft.com

1 系统登录

产品采用主流的 B/S 架构，能够使用加密的 HTTPS 协议与便捷的 HTTP 协议等多种可选远端管理方式，同时支持单用户多并发的账户机制。

本章将主要介绍 ZX-DMS 系列产品各个功能和管理时涉及到的一些基本概念（以 ZX-DMS 5120AC）。

1.1 用户登录

设备出厂时有多个管理 IP 地址，本文档以 *192.168.100.1* 这个 IP 为例，作为管理地址。因此请将任意一台电脑的 IP 地址设置为与系统管理地址同一网段的 IP 即可。例如：*192.168.100.10*.

在浏览器地址栏中输入 http://192.168.100.1:28099 并回车，即可打开系统的登录界面，如下图所示：

图 1.1 系统登陆界面

在设备的登录界面输入用户名账号和密码点击【登陆】按钮，进入系统 Web 管理平台。

在系统登陆界面可以选择显示语言的种类目前支持的语言有“简体中文”和“English”两种。

说明：

1、系统默认登录用户名为 admin 默认密码为 123

2、为了安全起见，请及时修改系统管理员密码。

1.2 主界面介绍

本节介绍中新金盾抗拒绝服务系统 Web 管理界面构成。如下图所示：

图 1.2 系统界面介绍

一级菜单	二级菜单
状态监控	全局统计，系统负载，防护范围，主机状态，连接监控，屏蔽列表，黑白名单，域名管理
攻击防御	全局参数，规则设置，TCP 端口保护，UDP 端口保护，牵引设置，变量设置
日志分析	日志列表，攻击分析，分析报告，TOP 统计，流量分析，连接分析，事件分析，性能分析，攻击档案，报表管理
系统配置	保存配置，系统设备，聚合管理，集群参数，控管属性，路由协议，用户组管理，用户管理，时间设定，SNMP 系统，SNMP Trap，SNMP 用户，SNMP 视图
服务支持	关于我们，版本信息，报文捕捉，产品升级

1.3 设置管理地址

根据企业实际情况确定好部署方式并将产品上架后，第一步骤设置系统的管理地址和网关，设备管理地址根据实际情况分配。

选择【系统配置】→【系统设备】进入系统管理地址设置界面，如下图所示：

图 1.3 系统设备示意图

这里我们将设备的管理地址设置为 *192.168.60.216/24* 网关地址为 *192.168.60.1*。具体操作分为以下两步：

1. 设置管理地址

在【系统设备】页面底部“设备”参数中填写设备管理接口“*eth0*”“地址”参数中填写设备的管理 IP 及掩码“192.168.60.216/24”。填写完成后点击【添加地址】按钮，如下图所示：

图 1.4 添加接口地址

2. 设置管理地址网关

在【系统设备】页面底部“设备”参数中填写设备管理接口“eth0”“地址”参数中填写设备的管理 IP 的网关地址“*192.168.60.1*”。填写完成后点击【设备网关】按钮，如下图所示：

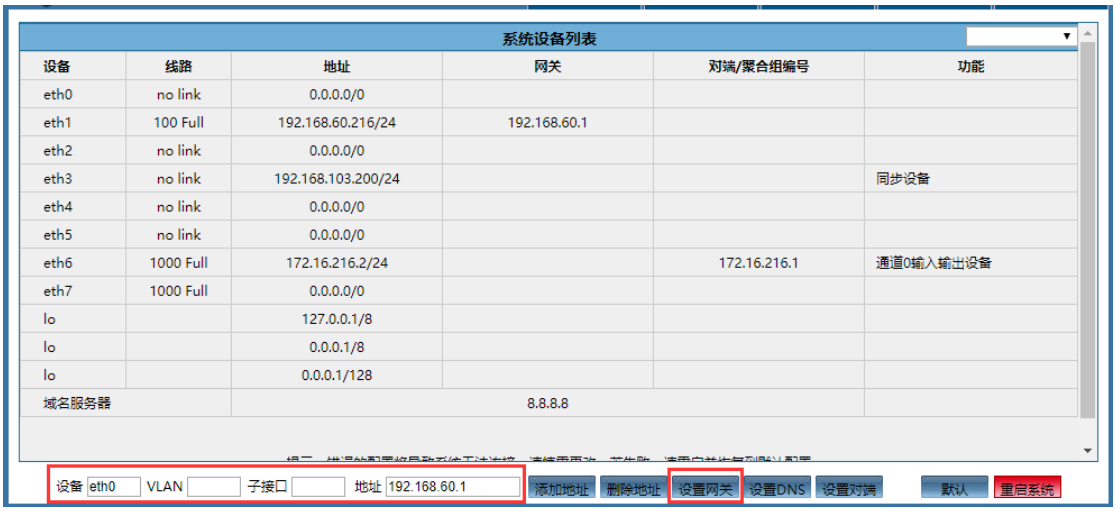


图 1.5 添加默认网关地址

管理地址添加完成后，就可以通过设置好的管理地址登陆到系统的 Web 管理平台。有关【系统设备】中具体参数设置也可参考“系统设备”相关章节。

1.4 用户切换

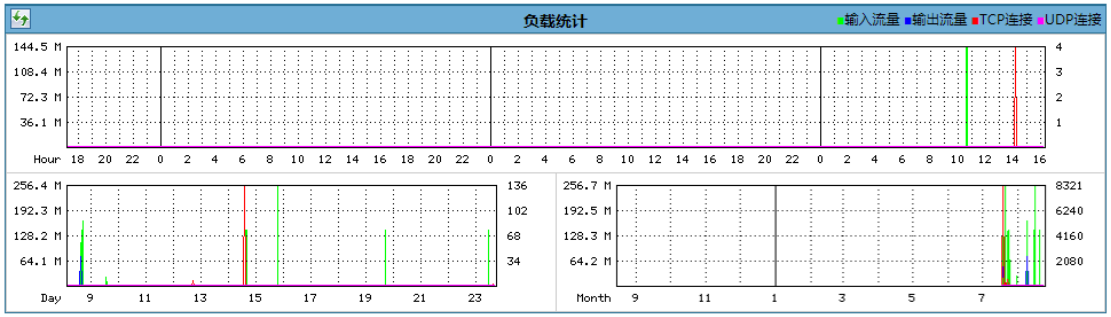
在系统 Web 管理平台的工作窗口右上角，提供了【退出登陆】按钮，点击后系统将会退回到登录窗口，此时输入账户与密码即对用户进行切换。

2 状态监控

2.1 全局统计

1. 负载统计

显示当前的流量图表、流量报表、系统概括、系统负载以及攻击记录，流量图表记录了设备总流量情况，如下图所示：



当前频率

方向	输入		匿名
	流量	报文	
外网	0.00 / 0.00 Mbps	0 / 0 pps	0.00 / 0.00 Mbps
内网	0.00 / 0.00 Mbps	0 / 0 pps	0.00 / 0.00 Mbps

图 2.1 全局统计

2. 当前频率

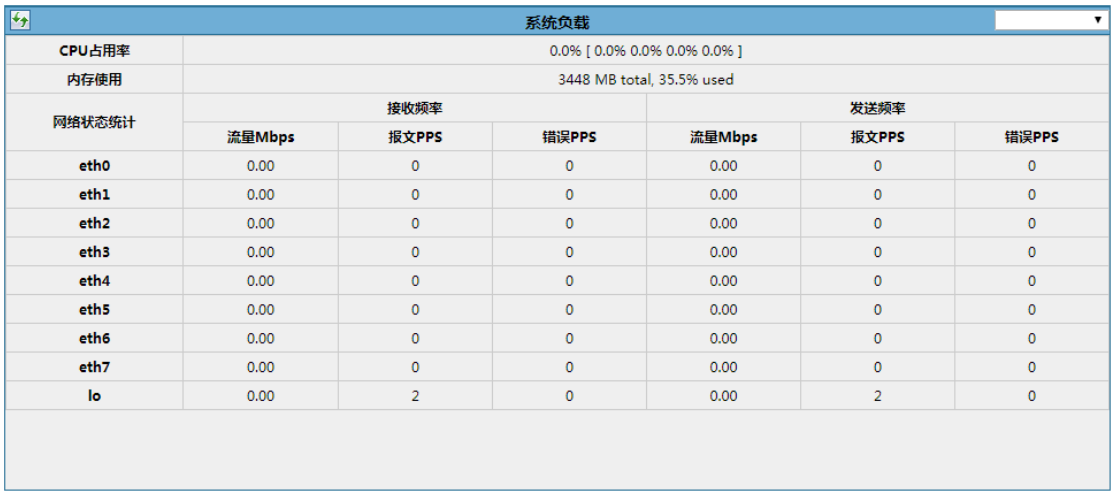
从整体上显示了设备上的流量、报文、匿名流量以及其他流量；外网为外部网络与设备的接口，即输入流量；内网为内部网络与设备的接口，即输出流量。

说明：

旁路部署模式没有输出流量和匿名流量显示

2.2 系统负载

记录了设备 CPU、内存的使用情况以及网络状态的统计。如下图所示：



系统负载

CPU占用率	0.0% [0.0% 0.0% 0.0% 0.0%]					
内存使用	3448 MB total, 35.5% used					
网络状态统计	接收频率			发送频率		
	流量Mbps	报文PPS	错误PPS	流量Mbps	报文PPS	错误PPS
eth0	0.00	0	0	0.00	0	0
eth1	0.00	0	0	0.00	0	0
eth2	0.00	0	0	0.00	0	0
eth3	0.00	0	0	0.00	0	0
eth4	0.00	0	0	0.00	0	0
eth5	0.00	0	0	0.00	0	0
eth6	0.00	0	0	0.00	0	0
eth7	0.00	0	0	0.00	0	0
lo	0.00	2	0	0.00	2	0

图 2.2 系统负载

1. CPU 占用率

CPU 选项卡可以实时的显示当前 CPU 的使用情况；

2. 内存使用

内存使用选项卡可以实时的显示当前内存的使用情况；

3. 网络状态统计

表 2.1 系统负载

功能名称	功能名称	功能说明
网络状态统计		显示了当前系统中所有网络接口，用于查看对应接口状态
输入频率	流量 Mbps	当前接口接收流量，单位 Mbps
	报文 PPS	当前接口接收流量，单位 pps
	错误 PPS	当前接口接收错误流量，单位 pps
发送频率	流量 Mbps	当前接口发送流量，单位 Mbps
	报文 PPS	当前接口发送流量，单位 pps
	错误 PPS	当前接口发送错误流量，单位 pps

2.3 防护范围

添加要防护的主机地址范围，只要在添加的主机地址范围内的主机产生流量后，主机的 IP 地址会自动在【主机状态】中显示。如下图所示。

图 2.3 防护范围

参数详解：

表 2.2 防护范围

功能名称	功能说明
控制	点击【删除】按钮即可删除一个防护范围
开始地址	指一个需要防护的地址范围中起始 IP 地址
结束地址	指一个需要防护的地址范围中起始 IP 地址
地址前缀	指一个防护范围中的 IP 地址在主机列表里面，分段合拢的掩码位
回注策略	选择流量回送时采用的模式以及填写所需的信息（旁路模式特有）

2.3.1 手工添加防护范围地址

【状态监控】→【防护范围】→选择“防护范围”→填写“防护地址”→【提交】

防护地址格式：

X.X.X.X（起始地址）*-X.X.X.X*（结束地址）*/XX*（网络前缀位数）

示例：

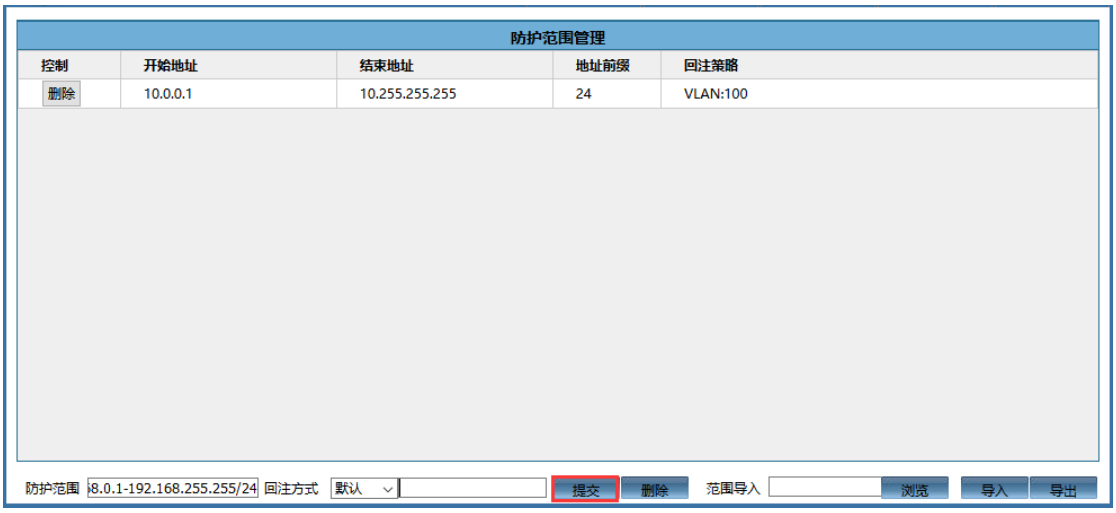


图 2.4 手工添加防护范围地址示图

192.168.0.1-192.168.255.255/24（添加了一个 B 段范围的地址，以 C 段地址为组的格式在主机列表中呈现）。

注意：

旁路部署时可能需要设置流量回注策略，填写回注策略时需要了解网络环境，在十分熟悉情况下才能操作，否则会造成流量走向乱序。

【状态监控】→【防护范围】→选择防护范围→填写“防护地址”→选择“回注方式”→填写对应“参数值”→【提交】

2.3.2 批量导入防护范围地址

【状态监控】→【防护范围】→选择“范围导入”→【浏览】→选择正确的“防护范围地址文本” →【提交】

文本内容格式：

导入的文件需要为 TXT 格式，文件内容格式如下图所示。

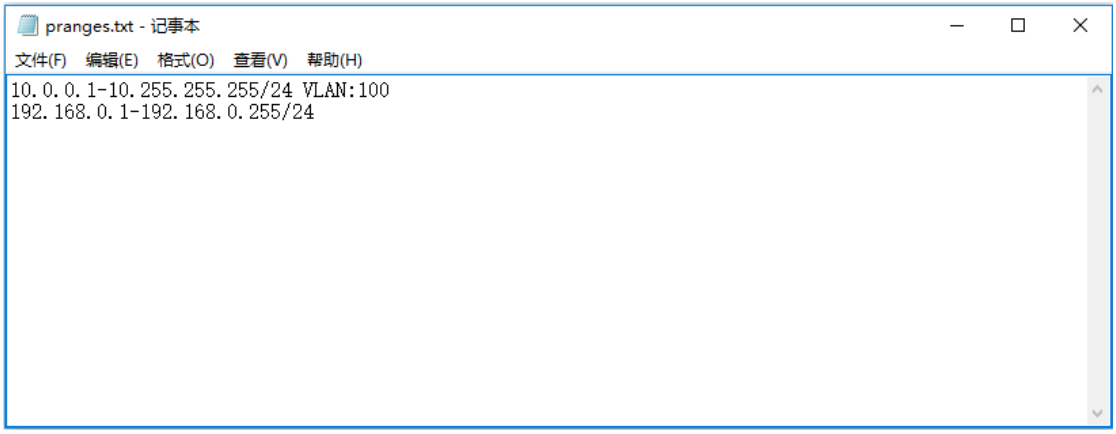


图 2.5 防护范围地址文本内容格式示图

提示：

1. “防护范围”功能仅限 IPv6&IPv4 双协议栈版本；
2. 回注策略功能，只限于旁路部署模式才具备。

2.4 主机状态

【主机状态】模块页面显示了当前设备下主机的基本状态，如主机、带宽、频率、连接、点击某个主机后可进入主机视图进行查看，如下图所示。

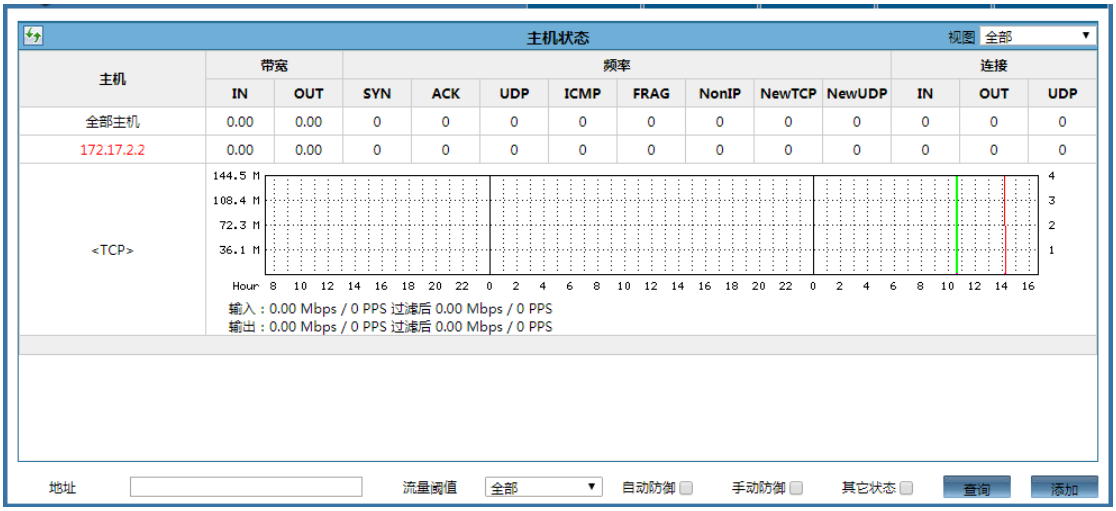


图 2.6 主机状态

■ 地址：

用于手工添加需要防护的地址，输入想要添加的主机或者子网，地址格式与防护范围相一致。

■ 流量阈值：

用于查看在某个流量大小范围内的主机信息。

■ 自动防御：

用户查询自动触发防护的主机信息。

■ 手动防御：

用于查询手动勾选了防护的主机信息。

■ 其他状态：

用于查询处于忽略所有流量、拒绝国外访问等状态的主机信息。

■ 视图

根据视图中流量 TOP 统计。

1. 主机状态

表 2.3 主机状态

名词	名词解释
主机	显示当前设备下的主机的 IP 地址，每个主机 IP 地址是一个超连接，点击后即可进入主机设置页面
带宽	显示该主机的入口和出口带宽占用，以 Mbps 为单位
频率	显示该主机当前各类报文频率，目前主要统计为 SYN 类型、ACK 类型、UDP 类型、ICMP 类型、FRAG 类型、NonIP 类型、NewTCP 类型和 NewUDP 类型
连接	显示外部与该主机建立的连接数（IN），该主机与外部建立的连接数（OUT），及 UDP 连接。

2. 添加主机

主机列表页面输入【地址】（例如：172.17.2.0-172.17.2.255/24）→【添加】。

图 2.7 添加地址

◆ 添加格式

✓ 单 IP：例如地址栏输入 172.17.2.2

✓ 范围：例如地址栏输入 172.17.2.0-172.17.2.255 或者 172.17.2.0-172.17.2.255/24

说明：

早期版本支持 IP/掩码格式，新版本此写法只是添加一个地址

3. 删除防护主机

单击某个主机 IP，进入主机视图。输入想要删除的主机或者网段，然后去掉“有效”选项框内的“√”，点击提交后即可删除单个主机。

图 2.8 删除防护主机

图 2.9 删除防护主机范围

4. 主机状态查看

点击主机列表某个主机后，会出现主机当前防护状态，保护模式显示当前主机处于的防御模式，输入输出流量显示主机输入和输出过滤前和过滤后流量，如下图所示：

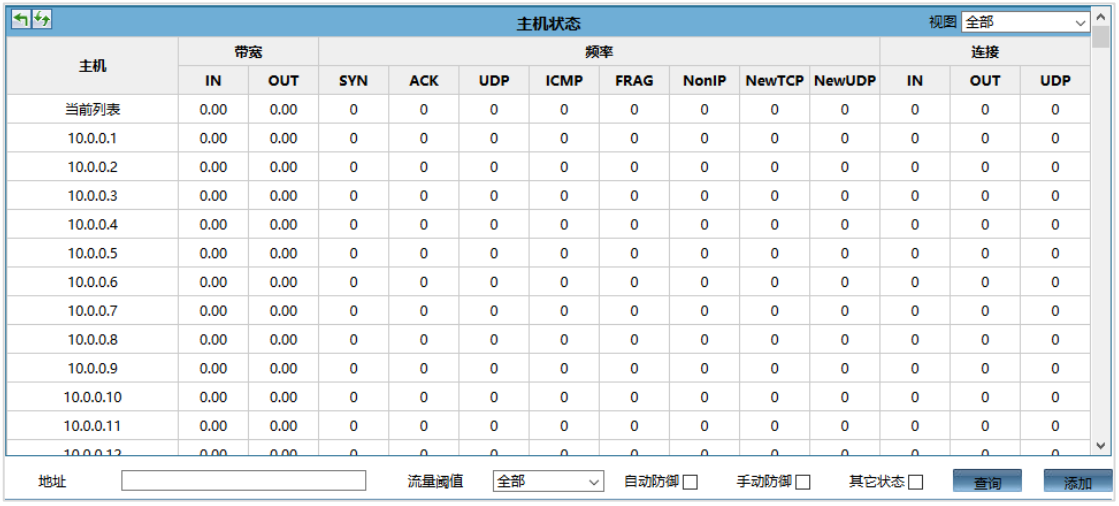


图 2.10 主机状态查看

说明：

旁路部署模式没有【带宽】→【OUT】数值。

2.4.1 主机设置

点击主机 IP，进入主机设置页面，当前显示了主机的设置参数，包括流量策略及防护策略，页面如下图所示：

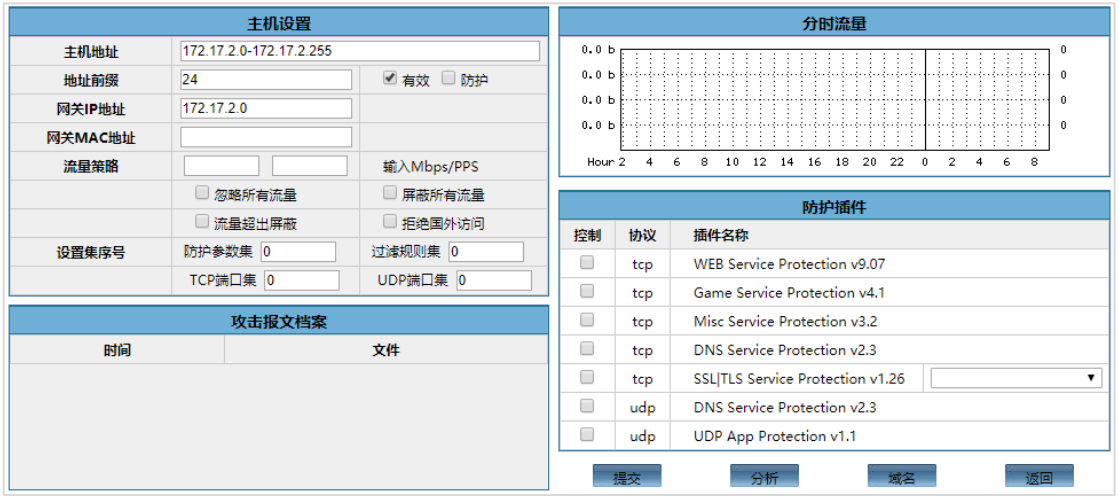


图 2.11 主机设置

1. 主机设置

该栏用于设置主机/网关 IP 地址/MAC 地址，流量策略等参数。

a. 主机地址：

显示当前主机的主机地址，“有效”复选框表示该主机是否存在。设备的主机自动发现系统有时会发现一些不存在的 IP 地址，如果您确定某主机不存在而又出现在列表中的话，请清除“有效”复选框，则该主机将被自动清除。“记录”选择此选项后将记录该主机的分时流量，并在分时流量图中体现。

b. 地址前缀：

显示当前主机的网络掩码位数，此项可根据网络地址设置识别，也可在该状态下直接进行修改。

c. 网关 IP 地址：

显示设置主机的网关 IP 地址，此项可根据网络地址设置识别，也可在该状态下直接进行修改。

d. 网关 MAC 地址：

设置主机的网关 MAC 地址，此项可根据网络地址设置识别，也可在该状态下直接进行修改。

e. 流量策略：

用于设置针对某主机的流量限制策略，以 Mbps/PPS 为单位，分为入口流量限制和出口流量限制：

表 2.4 流量策略

名词	名词解释
忽略所有流量	表示完全忽略对该地址主机数据报文的任何处理而只是简单转发

屏蔽所有流量	表示流量丢弃，对此主机的所有流量进行拦截
流量超出屏蔽	表示超出系统流量策略设置值时,会屏蔽该主机,禁止数据通行
拒绝国外访问	表示屏蔽所有国外 IP 通过

f. 设置集序号：

包括规则、TCP 端口、UDP 端口、防护参数，可根据不同需要进行规则、TCP 端口、UDP 端口、主机防护参数的调用，使得策略可以复用。

2. 攻击报文档案

当主机受攻击，主机状态发生改变时（如从[Normal]-> [SYN]或从[SYN]->[SYN][UDP]等），系统具有自动捕获数据包的功能，方便网络管理人员监控、取证等。

3. 防护插件

用来手工启用插件防护模式，针对此主机的特定防护手段，勾选相应的防护插件，点击【提交】保存当前所做更改即可。

说明：

早期版本【拒绝国外访问】因信任机制可能会出现某些国外 IP 没有拦截的情况，新版本对此功能做了修改。

2.5 连接监控

连接监控列表显示了当前设备所有的连接，页面如下图所示:

图 2.12 连接监控

◆ **选择连接**

此项可查询连接列表中地址信息，可以对特定的 IP 地址进行查询。查询方式分为两种，可以输入本地 IP 地址进行查询；另一种则是输入远程 IP 地址进行查询。查询远程 IP 地址需要加上“-”然后输入 IP 地址。例如查询远程地址为 8.8.8.8 的这个 IP 的的连接条目，输入方式为：-8.8.8.8。点击选择按钮后设备将列出所有远程地址为 8.8.8.8 的连接。

a. 选择：

输入主机 IP 地址后，勾选“输入连接/输出连接”点击【选择】按钮，会查询用户输入的连接 IP 地址所对应的连接。

b. 重置：

点击重置按钮，可以重置所勾选或者所填写 IP 地址所对应的连接。

c. 下载：

点击该按钮后将下载连接列表所有连接，输出文档格式为.txt 格式。

表 2.5 连接监控功能名词列表

名词	名词解释
本地地址	显示的是本地主机地址加上本地端口号，可较方便的定位到具体的服务
远程地址	显示了建立此数据连接的远端主机的地址及其端口号
活跃连接	显示正在工作状态的连接数量
全部连接	显示此远端主机对本地主机的服务端口数据请求建立的全部连接数量

2.6 屏蔽列表

“屏蔽列表”模块页面显示被系统所屏蔽的连接，页面如下所示：

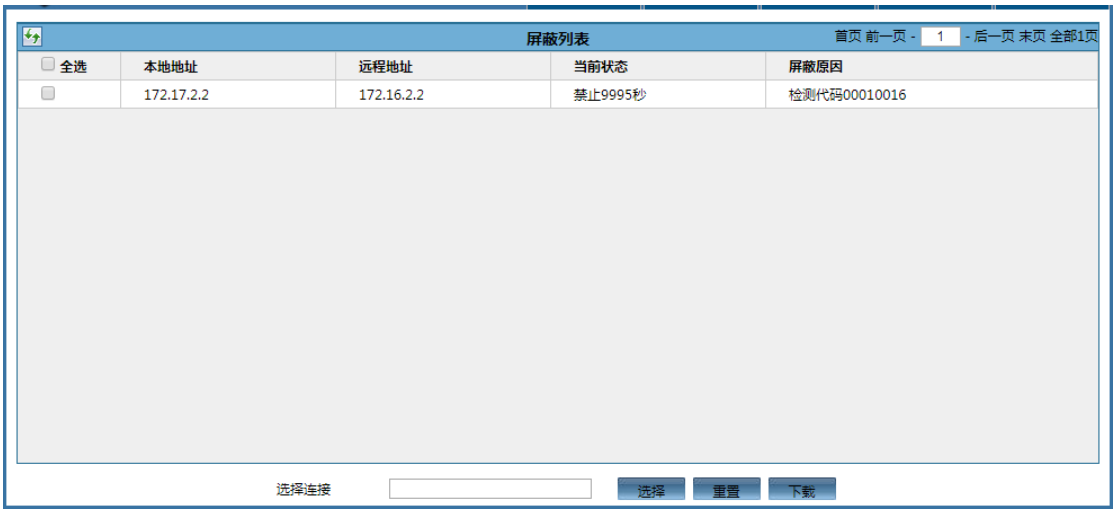


图 2.13 屏蔽列表

◆ **选择连接**

此项可查询屏蔽列表中地址信息，可对特定的 IP 地址进行查询。

a. 选择：

输入特定 IP 地址后单击该按钮将显示出该 IP 所有连接条目。

b. 重置：

可针对选择后的连接进行重置设置。

c. 下载：

可下载当前页面的屏蔽记录，输出文档格式为.txt 格式。

名词	名词解释
本地地址	显示了此会话的本地地址，可通过此记录确认屏蔽会话的目标服务器
远程地址	显示了此会话的远程地址，可通过此记录确认攻击源客户端
当前状态	显示当前屏蔽剩余时间，倒计时针
屏蔽原因	显示屏蔽会话原因，可根据此记录核对攻击行为与策略配置

表 2.6 屏蔽原因及参数对应表

屏蔽原因	对应参数
系统连接保护	【防御配置】→【全局参数】→【TCP 连接数量保护】→【/IP】
SYN Flood 攻击	【防御配置】→【全局参数】→【SYN Flood 单机保护】
报文频率限制	【防御配置】→【UDP 端口保护】→【报文频率限制】
连接数量保护	【防御配置】→【规则设置】→【频率限制】→【连接限制】
访问频率限制	【防御配置】→【规则设置】→【频率限制】→【访问频率】
端口连接保护	【防御配置】→【TCP 端口保护】→【连接数量限制】
服务器踢出	【防御配置】→【TCP 端口保护】→【踢出权重】
端口探测	【防御配置】→【TCP 端口保护】→【探测权重】
非法协议	【防御配置】→【TCP 端口保护】→【协议类型选择】
检测代码 00010015	【防御配置】→【TCP 端口保护】→【WEB 插件】→模块参数一
检测代码 00010016	【防御配置】→【TCP 端口保护】→【WEB 插件】→模块参数一
检测代码 00010017	【防御配置】→【TCP 端口保护】→【WEB 插件】→模块参数二
检测代码 00010018	【防御配置】→【TCP 端口保护】→【WEB 插件】→模块参数三
检测代码 00010019	【防御配置】→【TCP 端口保护】→【WEB 插件】→模块参数一
检测代码 0001001E	【防御配置】→【TCP 端口保护】→【WEB 插件】→模块参数一
检测代码 00020014	【防御配置】→【TCP 端口保护】→【GAME 插件】→模块参数一
检测代码 00020015	【防御配置】→【TCP 端口保护】→【GAME 插件】→模块参数二
检测代码 00020016	【防御配置】→【TCP 端口保护】→【GAME 插件】→模块参数三
检测代码 00020017	【防御配置】→【TCP 端口保护】→【GAME 插件】→模块参数五
检测代码 0006000B	【防御配置】→【TCP 端口保护】→【SSL 插件】→模块参数三
检测代码 0006000C	【防御配置】→【TCP 端口保护】→【SSL 插件】→模块参数四

检测代码 0006000D	【防御配置】→【TCP 端口保护】→【SSL 插件】→模块参数一
集群同步屏蔽	表示此屏蔽是由其他集群墙同步而来，并且会结合其他屏蔽原因同时出现。

2.7 黑白名单

在【黑白名单】模块管理页面，可直接将 IP 加到黑名单和白名单。页面如下图所示：

图 2.14 黑白名单管理

参数详解：

表 2.7 黑白名单

名词	名词解释
全选	勾选对应的地址后，点击【删除】按键可删除单条或多条名单记录
地址	黑白名单的基准 IP 地址，点分十进制显示
类型	显示当前地址是黑名单还是白名单
匹配	匹配次数，记录着每条策略的命中次数
备注	添加黑白名单时用来备注信息，方便后期维护

2.7.1 手工添加黑白名单条目

【状态监控】→【黑白名单】→选择“地址”→填写“黑白名单 IP 地址”→【提交】

黑白名单填写格式：

a. 白名单格式

+X.X.X.X 或者+X.X.X.X-X.X.X.X（“+”代表白名单）

b. 黑名单格式

-X.X.X.X 或者-X.X.X.X-X.X.X.X（“-”代表黑名单）

示例：

图 2.15 手工添加单 IP 黑名单

图 2.16 手工添加范围 IP 黑名单

2.7.2 批量导入黑白名单条目

【状态监控】→【黑白名单】→选择“名单列表”→【浏览】→选择正确的“黑白名单列表文本” →【提交】

文本内容格式：

导入的文件需要为 TXT 格式，文件内容格式如下图所示。

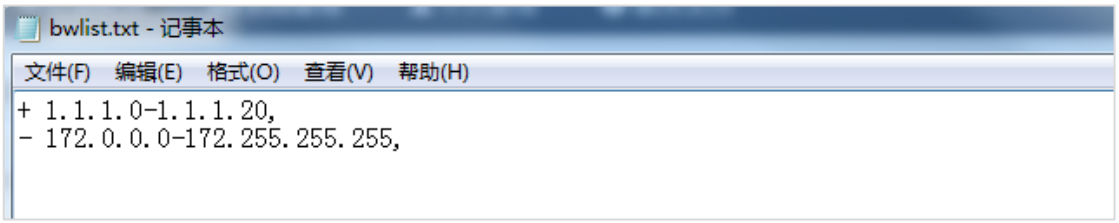


图 2.17 黑白名单列表文本内容格式示图

提示：

黑白名单列表是对应的策略表单，若要开启黑白名单功能需要在主机做在的主机参数集中勾选相应的名单选项，使得参数集被防护 IP 调用时启用。

不是所有的版本均支持范围形式添加，详细请联系中新网络信息安全股份有限公司售后人员确认。

2.8 域名管理

在【域名管理】模块页面可以设置域名的黑名单和白名单，页面如下图所示：

图 2.18 域名管理

- 域名：在关键字一栏输入想要查询的关键字，点击查询后即可显示该域名的详细信息。
  - 提交：如果想单独添加单个域名，可以直接在关键字一栏输入想要添加的域名，然后提交后即可。其中，“-”表示拒绝“+”表示放行。“-.”表示拒绝所有。“+.“、”表示放行所有。例如拒绝：www.baidu.com 这个域名，相应格式可以填写为：-www.baidu.com，提交后即可。该策略只针对设备下主机有效，即外网 IP 访问到设备下主机。

- 删除：在域名一栏输入关键字或者直接勾选对应的域名，点击删除按钮就可删除相应域名。
- 查询：在域名一栏输入关键字，点击查询按钮就可列出所有包含该关键字的域名。
- 清除：用于清除自动收集的域名。系统开启了“域名审计”功能后，便会自动收集所有主机域名，并以“域名 IP 数量”的格式显示出来，点【清除】便可清除所有自动收集的域名；

提示：

因自动收集的域名会自动设置为白名单，建议先设置好域名管理策略。

◆ 域名列表：该栏用于批量进行添加域名，方式类似于黑名单的添加，也需在本地以相应格式编写.txt 文档，并且保存的格式为 utf-8,然后浏览到该文档点击导入后即可。添加格式如下图所示：

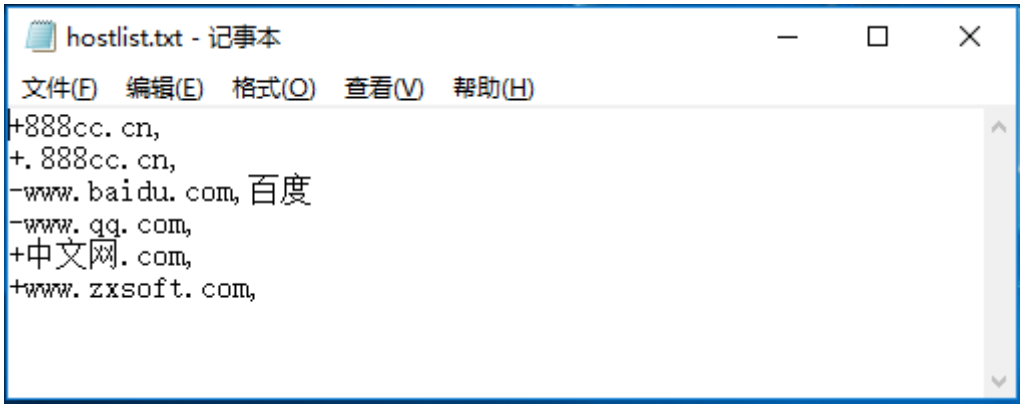


图 2.19 域名列表

注意：

导入新的域名文档后会把现有的域名列表给覆盖掉，这一点还请注意，以免造成不必要的麻烦。

3 攻击防御

3.1 全局参数

【全局参数】模块设置页面，提供了一些通用参数的设置接口，用户可方便的配置设备防护行为。页面如下图所示：

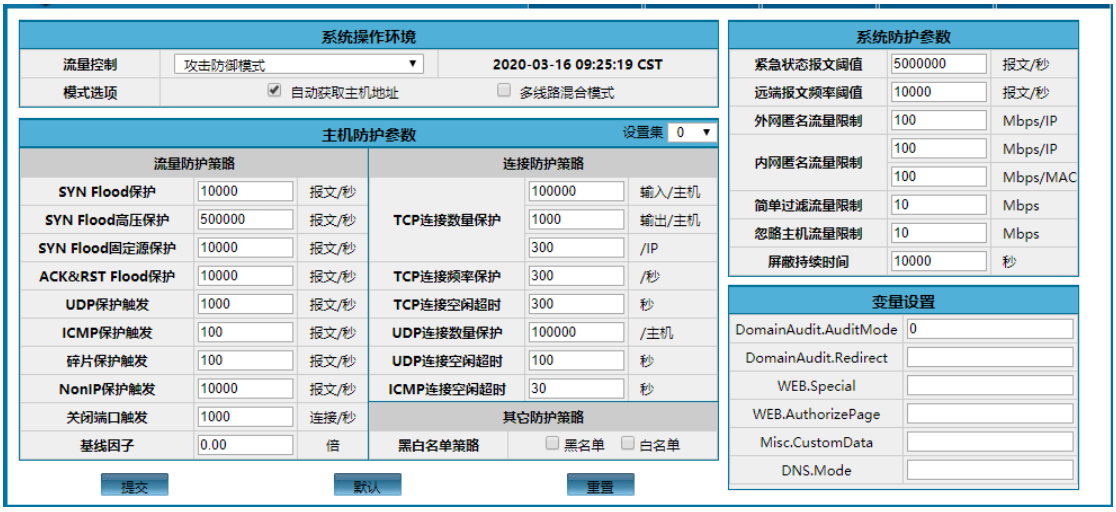


图 3.1 全局参数

3.1.1 系统操作环境

系统操作环境提供系统全局范围的主机防护参数，主要包括流量控制、系统时间和策略选项：

◆ 流量控制：全局型的流量控制，包括透明直通、攻击防御模式（自动）、攻击防御模式（手动）

■ 透明直通

设备相当于一根导线，只是简单的转发数据而不进行处理；

■ 攻击防御模式

此模式下，系统运行完整的攻击过滤流程，过滤攻击保证正常流量到达主机。

■ 攻击防御模式（自动）

旁路模式特有，功能类似串联的攻击防御模式，选择此模式可以联动分析器一起使用实现按需牵引。

- 攻击防御模式（手动）

旁路模式特有，功能类似串联的攻击防御模式，选择此模式时无法与分析器联动使用。

◆ 模式选项

- 自动获取主机地址

当设备检测到墙下主机进出流量均经过设备时则自动添加到主机列表

- 多线路混合模式

启用此选择会对设备下每台主机记录进入设备时的 MAC 地址，回应时直接对调源目的 MAC 地址。

- 主机探测

旁路特有，用于旁路模式二层部署环境中主机 MAC 地址发现；

- SYN 重传验证

旁路特有，SYN 重传机制验证源 IP

- ACK 重传验证

旁路特有，ACK 重传机制验证源 IP

- 验证方式一

旁路特有，通过半连接验证的方式防御 SYN 泛洪攻击，设备会主动断开首次三次握手进行真实源验证

- 验证方式二

旁路特有，通过全连接验证的方式防御 SYN 泛洪攻击，设备回复错误的 ACK 序列号进行真实源验证

3.1.2 系统防护参数

系统防护参数主要是针对一些攻击流量做限制，针对设备全局有效。

◆ 报文紧急状态阈值

当设备每秒收到的报文超过此值时，设备将进入严格过滤状态，此时只放行已经信任的 IP。

◆ 远端报文频率阈值

某远端地址报文频率超过此值，屏蔽此源 IP 流量。

◆ 外网匿名流量限制

外网固定源 IP 攻击设备下主机，或者内网主机 IP 攻击外网固定 IP，且内网主机 IP 不再设备主机列表中，此参数会限制流量，默认为 100Mbps/IP。

◆ 内网匿名流量限制

可按内网主机 IP 或者 MAC 来设置，值小优先。又可分为两种情况，1-当外网攻击设备下固定主机 IP，2-内网主机使用固定 IP 或者使用固定 MAC 攻击外网主机。这两种情况都满足内网主机不在设备主机列表中，此时此参数限制流量，默认为 100Mbps/IP。

◆ 简单过滤流量限制

限制一些简单攻击数据包的流量，目前支持检查数据部分都相同和源目地址相同的数据包，默认为 10Mbps。

◆ 忽略主机流量限制

当在设备上忽略 IP 流量检查时，此处可以限制此类 IP 的流量，默认为 10Mbps。

◆ 屏蔽持续时间

屏蔽列表中的屏蔽时间，默认为 10000 秒。

◆ 防护释放时间

旁路特有，自动牵引模式，停止攻击后释放防护的时间，默认 300 秒

3.1.3 主机防护参数

主机防护参数可针对不同服务主机进行特殊参数设置，通过“设置集”将某主机设置为指定参数集，在该集中调整参数而不影响其他主机服务。

◆ 流量防护策略

■ SYN Flood 保护

当设备下主机 IP 收到 SYN 报文数量，每秒超过次数设置值时（此处设置为 10000），此设备下主机进入 SYN Flood 防御模式，防御模式在攻击量小于设置值一段时间后自动释放。

■ SYN Flood 高压保护

当设备下主机 IP 收到 SYN 报文数量，每秒超过次数设置值时（此处设置为 500000），此设备下主机进入 SYN Flood 高压防御模式，此防御模式将更为严格的防御 SYN 攻击，防御模式在攻击量小于设置值一段时间后自动释放。

■ SYN Flood 固定源保护

用于防护单 IP 发送频率高的攻击，当单 IP 发送的 SYN 每 16s 的频率超过设置值时，系统将屏蔽此 IP。

■ ACK&RST Flood 保护

当设备下主机每秒收到的 ACK 或者 RST 报文超过设置值（此处为 10000），此设备下主机进入 ACK Flood 或者 RST Flood 防御模式，此时丢弃所有非信任主机 ACK 或者 RST 数据包。防御模式在攻击量小于设置值一段时间后自动释放。

- UDP 保护触发

当设备下主机每秒收到的 UDP 报文超过设置值（此处为 1000），此设备下主机进入 UDP Flood 防御模式，此时丢弃所有超时时间外针对此 IP 的 UDP 数据包。防御模式在攻击量小于设置值一段时间后自动释放。

- ICMP 保护触发

当设备下主机每秒收到的 ICMP 报文超过设置值（此处为 100），此设备下主机进入 ICMP Flood 防御模式，此时丢弃所有超时时间外针对此 IP 的 ICMP 数据包。防御模式在攻击量小于设置值一段时间后自动释放。

- 碎片保护触发

当设备下主机每秒收到的 Fragment 碎片报文超过设置值（此处为 100），此设备下主机进入 Fragment Flood 防御模式，此时丢弃所有针对此 IP 的 Fragment 数据包。防御模式在攻击量小于设置值一段时间后自动释放。

- NonIP 保护触发

当设备下主机每秒收到不常用 IP 协议族其他协议数据报文超过设置值（此处为 10000），此设备下主机进入 NonIP Flood 防御模式，此时丢弃所有针对此 IP 的 NonIP 数据包。防御模式在攻击量小于设置值一段时间后自动释放。

- 关闭端口触发

服务器未开放端口，如果每秒接受数据包数量超过设置值，则设备会拒绝此端口的连接。

- 基线因子

计算主机前 1 小时当前时间的平均流量，作为基线流量。当流量超过平均流量 x 倍基线因子，主机会进入[Bline]防护，此状态不会过滤报文，只是会提示主机进入此种防护。

提示：

设置基线因子参数主机的流量图里能看到一个橙色的线，这个就是流量基线，0 表示关闭流量学习功能。

（举例 ：若基线因子填“2”倍，那么主机当前流量超过了基线流量 2 倍，会进入[Bline]防护）

- 连接防护策略
  - TCP 连接数量保护：此项分为三个参数：

1. 第一个参数控制设备下主机的输入连接，默认参数设置为 100000，即主机输入方向并发连接；
2. 第二个参数控制设备下主机的输出连接，默认参数设置为 1000，即主机输出方向并发连接；
3. 第三个参数指当外网机器 A 与设备下主机 B 的 tcp 连接数量每秒超过此设置值后（默认为 300），会屏蔽 A 对 B 的访问，屏蔽时间为系统防护参数中的屏蔽持续时间设置的值，默认为 10000 秒。

■ TCP 连接频率保护

当外网机器 A 与设备下主机 B 的访问次数每秒数量超过此设置值后（默认为 300），会屏蔽 A 对 B 的访问，屏蔽时间为系统防护参数中的屏蔽持续时间设置的值，默认为 10000 秒。

■ TCP 连接空闲超时

已经建立的连接在设置时间内没有任何数据交互（默认为 300 秒），则重置该连接。

■ UDP 连接数量控制

每个主机最多能建立 100000（默认为 100000）个 UDP 链接；

■ UDP 链接空闲超时

配合 UDP 保护使用。

■ ICMP 链接超时

配合 ICMP 保护使用。

◆ 其他防护策略

■ 黑白名单策略

用来启用 IP 黑白名单策略。

3.1.4 系统变量设置

参数针对设备全局有效

◆ DomainAudit.AuditMode

通过设置不同的值来控制域名审计行为。如下图所示

图 3.2 DomainAudit.AuditMode 设置

- 0

默认值，不启用域名审计。

- 1

允许 IP 地址访问，禁止访问域名点数超过 10 的域名，禁止访问黑名单域名

- 2

允许 IP 地址访问，禁止访问域名点数超过 10 的域名，只允许访问白名单域名

- 3

允许 IP 地址访问，禁止访问域名点数超过 10 的域名，允许访问白名单域名，禁止访问黑名单域名，不在域名列表的会自动添加为白名单

- 9

功能和参数 1 类似，不允许 IP 直接访问

- 10

功能和参数 2 类似，不允许 IP 直接访问

- 11

功能和参数 3 类似，不允许 IP 直接访问

◆ DomainAudit.Redirect

当开启域名审计时，被阻止的访问自动跳转到此处填写的 Web 页面中。比如跳转到 *www.baidu.com*，那么填写如下图所示：

图 3.3 DomainAudit.Redirect 设置

◆ WEB.Special

有些访问无法通过 TCP 端口保护中的 WEB 插件防御检验，有需要放行时，再次填写此访问的特征，例如如果放行百度蜘蛛的访问，则填写 *Baiduspider*，如下图所示：

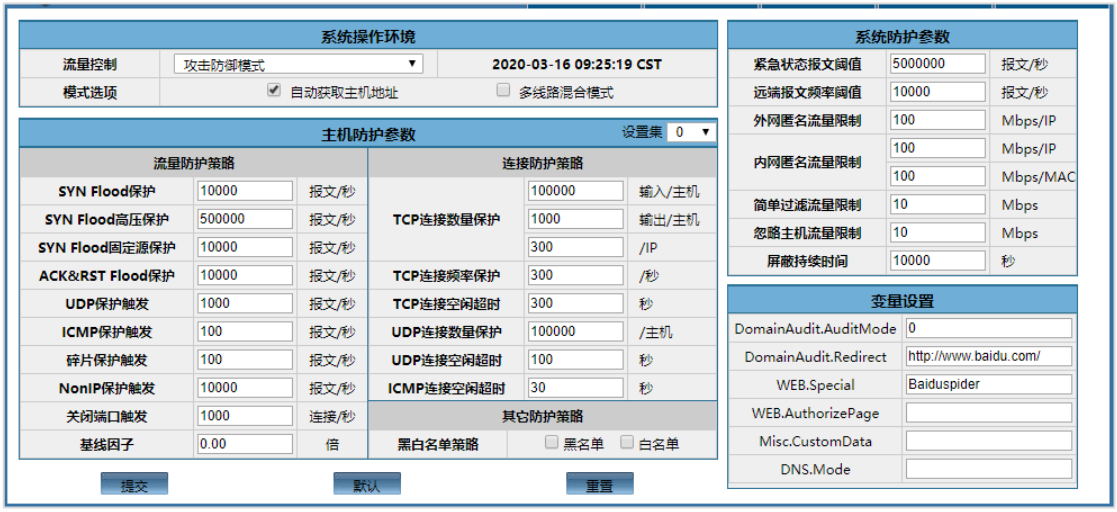


图 3.4 WEB.Special 设置

◆ WEB.AuthorizePage

有些网站防御需要用到验证码，此处填写验证服务器的地址。假如我们验证服务器地址为：http://*192.168.200.200/auth.php*，在该栏直接输入即可。如下图所示：

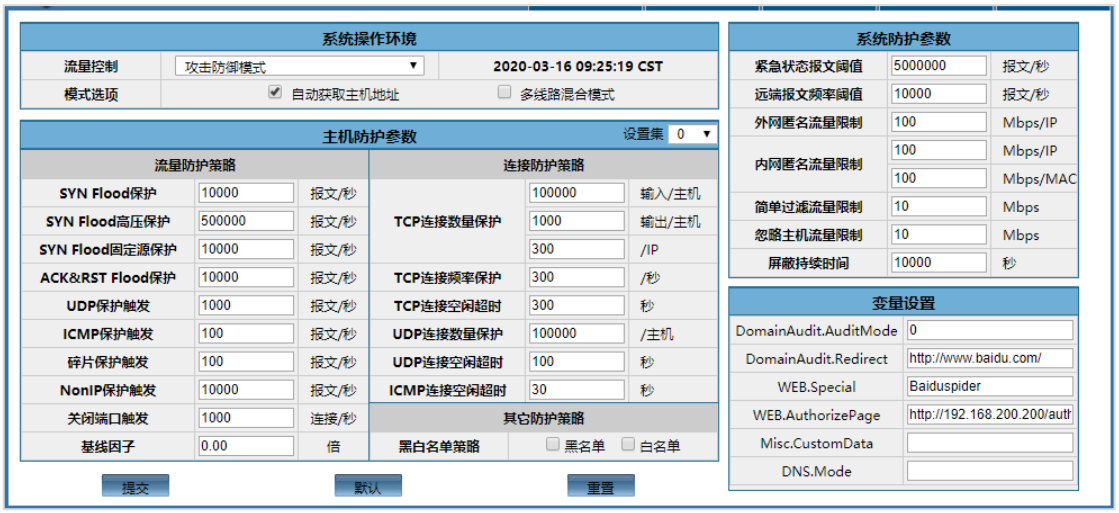


图 3.5 WEB.AuthorizePage 设置

◆ Misc.CustomData

对应 TCP 端口防护中的 Misc 插件，填写数据格式为服务器回复数据:客户端回应的正则表达式，最多写 8 组，中间用空格分开，Misc 插件使用 10-17 来调用 8 组数据，用户 TCP 建立连接后，服务器先发送数据，然后客户端再发送数据的情况。比如服务器回复数据部分为 00 01 12 31 然后客户端发送数据部分开始两个字节为 16 03，则书写格式为 00011231: ^\x16\x03 如下图所示：

图 3.6 Misc.CustomData 设置

◆ DNS.Mode

用于清除 DNS 插件学习到的白名单地址，参数为 clear。填写格式如下图所示：

DNS.Mode 设置

说明：

参数为 clear，提交之后立即清理，用于一次性触发，不会在输入框中显示

3.2 规则设置

【规则设置】模块页面显示了当前设备系统中的规则，包括系统规则及用户定义规则。页面如下图所示：

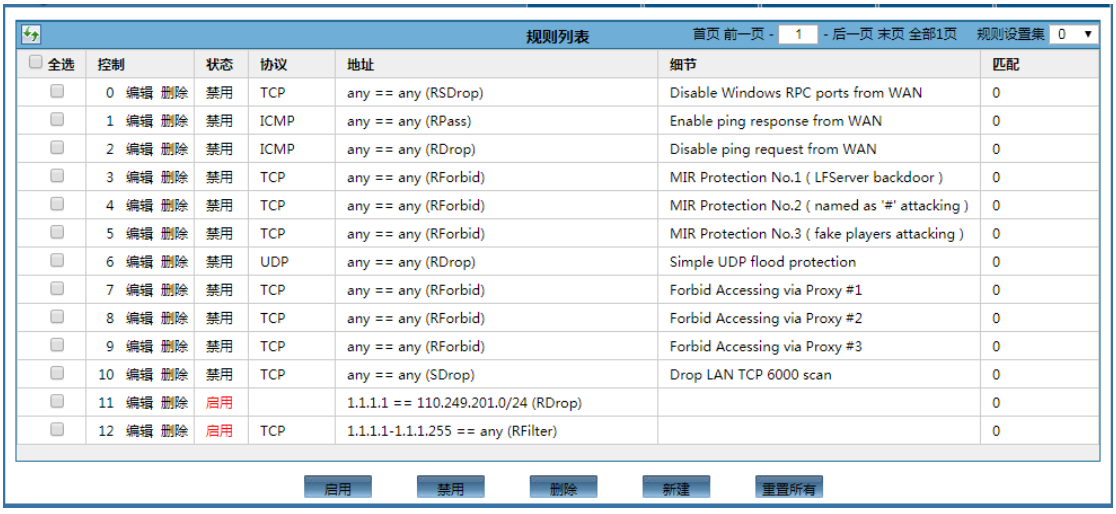


图 3.7 规则设置

点击“新建”按钮或者某规则的“编辑”操作，将进入规则编辑页面。点击“重置所有”按钮则将取消所有规则。单机“删除”则将删除该规则。具体描述如下：

3.2.1 规则列表

- 规则设置集：范围 0-15，对于一台主机可适用多项规则，也可用于规则的重叠设置，通过主机状态中的规则设置集选择某台主机的生效规则。
- 控制：用于规则的编辑删除操作。
- 协议：表示该规则的协议域，如 TCP，UDP，ICMP 等。
- 地址：表示该规则的地址域。
- 细节：该规则的其它细节性的描述，根据规则不同内容也不同。如果规则包含描述域，则显示该规则的描述文本。
- 匹配：规则匹配的次数。
- 启用：选择对应的规则后点击“启用”开启规则
- 禁用：选择对应的规则后点击“禁用”禁用规则
- 删除：选择对应的规则后点击“删除”删除规则
- 重置所有：点击“重置所有”后将清除所有非系统规则

3.2.2 规则编辑页面

规则编辑页面用于编辑或添加某个用户定义规则。页面如下图所示：

图 3.8 规则编辑

- 规则序号：设置此规则在规则列表中的位置，可通过自定义设置规则生效顺序。
- 规则描述：此规则以文本形式描述，使用户快速理解规则的用途。
- 报文长度：指定该规则匹配的报文的长度范围。
- 本地地址：选项“所有地址”，表明此规则匹配所有的本地地址；“地址范围”指定一个地址的范围用于规则的本地地址匹配， 如“192.168.1.1-192.168.1.255”；“网络掩码”指定一个网络地址范围用于规则的本地地址匹配，如“192.168.1.1:255.255.255.0”。
- 远程地址：选项“所有地址”，表明此规则匹配所有的远程地址；“地址范围”指定一个地址的范围用于规则的远程地址匹配， 如“192.168.1.1-192.168.1.255”；“网络掩码”指定一个网络地址范围用于规则的远程地址匹配，如“192.168.1.1:255.255.255.0”；“指定域名”表明此规则的远程地址将匹配对该域名的地址解析请求（若选择此项，则“协议”域自动设为 UDP，远程端口自动设成 53）。
- 协议类型：指示规则匹配的报文的协议类型，分为 IP，TCP，UDP，ICMP 等几种。其中，TCP、UDP 及 ICMP 协议将各自激活相应的系列规则设置。
- 本地端口/远程端口：TCP 及 UDP 协议的规则，将激活此设置域，指示规则的端口匹配值，为空则表示匹配所有端口；当规则为 TCP/UDP 协议时，可指定相应的端口域。可指定的端口类型可以为单一端口，如“80”；也可为端口范围，如“135-445”；还可以为离散端口，如“7000, 7100, 7200”。
- TCP 标志位：TCP 协议设置的特定域，指示规则匹配报文的 TCP 标志，包括 FIN，SYN，RST，PSH，ACK，URG。
- TCP 窗口大小：针对数据包的 win 值大小的设置。
- ICMP 类型/ICMP 代码：ICMP 协议设置的特定域，指示规则匹配报文的 ICMP 数值。
- 模式匹配

该规则匹配的关键字，可选项还包括“顺序匹配”和“忽略大小写”。指定规则匹配包含的关键字。本设备内建高效的模式匹配算法，可快速、批量的进行数据匹配，从原始报文中找出某一组关键字用于规则模式匹配。可以是单一关键字，如“haha”；也可以是一组关键字，如“haha heihei hoho”；如果关键字包含不可见字符，还可以通过“\”进行代码转义，如“\a8\aa”。并可通过“顺序匹配”和“忽略大小写”来自定义需要匹配内容。

- 顺序匹配

  指定的匹配内容按顺序匹配，如果不勾选则可以不按顺序匹配，比如需要匹配 12345，如果没有勾选则 34215 也可以匹配到

- 忽略大小写

  当匹配内容是字符串时是否区分匹配内容中的大小写字母

- 方向选择：指示该规则匹配的数据流方向。
- 规则行为：指示该规则被某个报文匹配后，将对该报文所做的处理，包括过滤、拦截、放行和屏蔽，并且还可以在规则匹配的同时在日志记录中产生一条日志。
- 频率限制
  - 统计 ID：没有实际意义，小于 16 只拦截不屏蔽，大于 16 达到阈值后屏蔽
  - 连接限制：针对模式匹配内容达到匹配连接次数则屏蔽
  - 访问频率：针对模式匹配内容达到匹配频率则屏蔽

3.3 TCP 端口保护

【TCP 端口保护设置】模块页面提供了针对每个端口的独立设置参数，用户可根据某种端口的服务类型更改相应的处理策略。页面如下图所示：

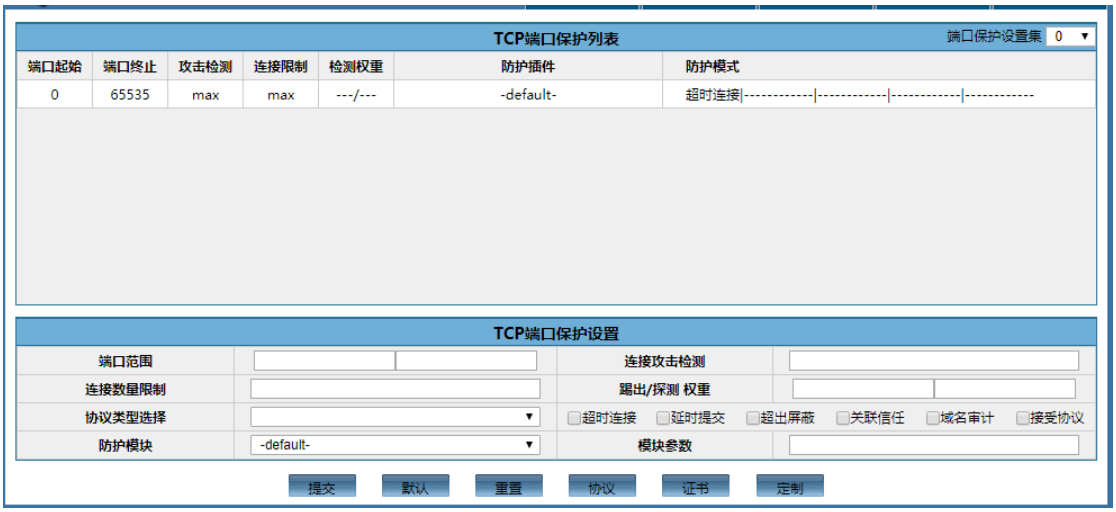


图 3.9 TCP 端口保护

- 端口保护设置集：范围 0-15，对于一台主机可适用多项端口防护设置，也可用于同一端口的重叠设置，通过主机状态中的 TCP 端口保护集选择某台主机的生效端口防护。
- 端口起始/终止：显示设置防护的端口范围,默认针对“0-65535”端口进行防护。
- 攻击检测：显示设置端口的连接攻击检测频率数值，max 表示无限大。
- 连接限制：显示设置端口的连接数量限制数值，max 表示无限大。
- 检测权重：显示设置端口的踢出/探测权重的数值。
- 防护插件：显示设置端口启用的防护模块类型，default 为默认防护。
- 防护模式：显示设置端口启用的防护标志有哪些，默认仅启用“超时连接”模式。

- 提交：添加 TCP 端口保护设置。
- 默认：“默认”系统使用默认端口保护设置。
- 重置：重置 TCP 端口保护设置一栏所填参数。
- 协议：自定义协议类型。
- 证书：点击跳转到证书管理页面
- 定制：点击跳转到 web 插件定制页面

3.3.1 TCP 端口配置

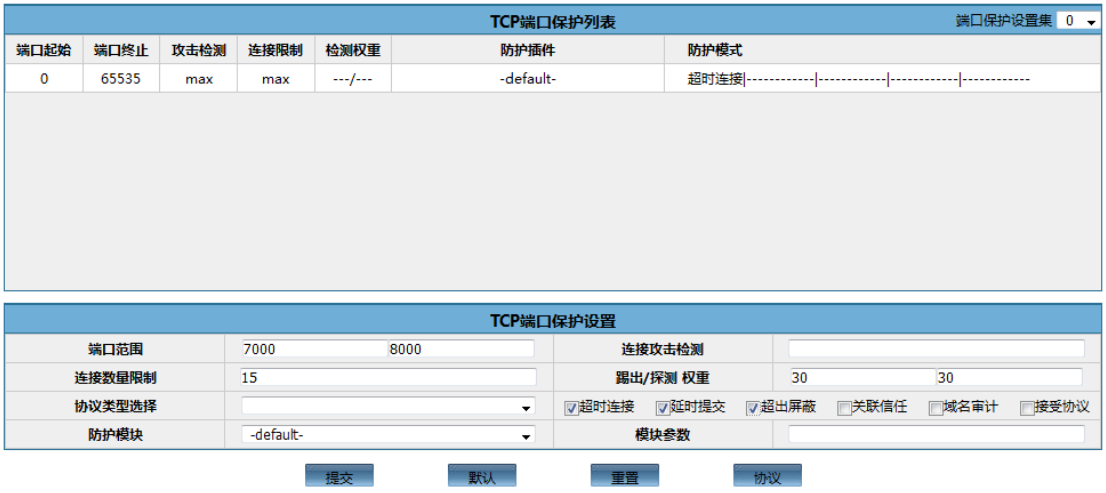


图 3.10 添加 TCP 端口保护

- 端口范围：用于设置指定端口，可以是一个端口也可以是一个端口范围。
- 连接攻击检测：用于自动启用 TCP 防护插件。设置该参数后，当主机与该端口范围的 TCP 连接频率超过设置数值，该主机将自动进入 TCP 防护模式，设置的插件将被启用，当连接频率小于该数值后一段时间，该主机将自动取消 TCP 防护模式。

提示：

在主机设置页面手工设置 TCP 防护不会自动取消。

- 连接数量限制

限制每个客户端允许与主机建立的连接数量，超出设置数量该连接被屏蔽。一般来说，Web 服务应将此数值保持为空即为不限制，而其它对连接数量依赖较小的服务可设置合适的数值来避免主机在单一客户上耗费过多资源。

- 踢出/探测 权重

限制每个客户端允许与主机建立空连接的数量，超出设置限制该连接被屏蔽。

- 协议类型选择

用于设置指定协议类型，可设定接收或拒绝某端口的访问协议。如对于某些需要拒绝 HTTP 协议的端口（如受代理攻击的某些游戏），则应该在协议类型里选择 HTTP，然后不选择“接受协议”，则该端口将拒绝 HTTP 协议的访问，相反如果选择了“接受协议”则表示接收 HTTP 协议。点击上方协议按钮，会出现协议定义界面，利用正则表达式定义协议特征，此数据为建立 TCP 三次握手后，由客户端首先发送的数据特征，如下图所示：

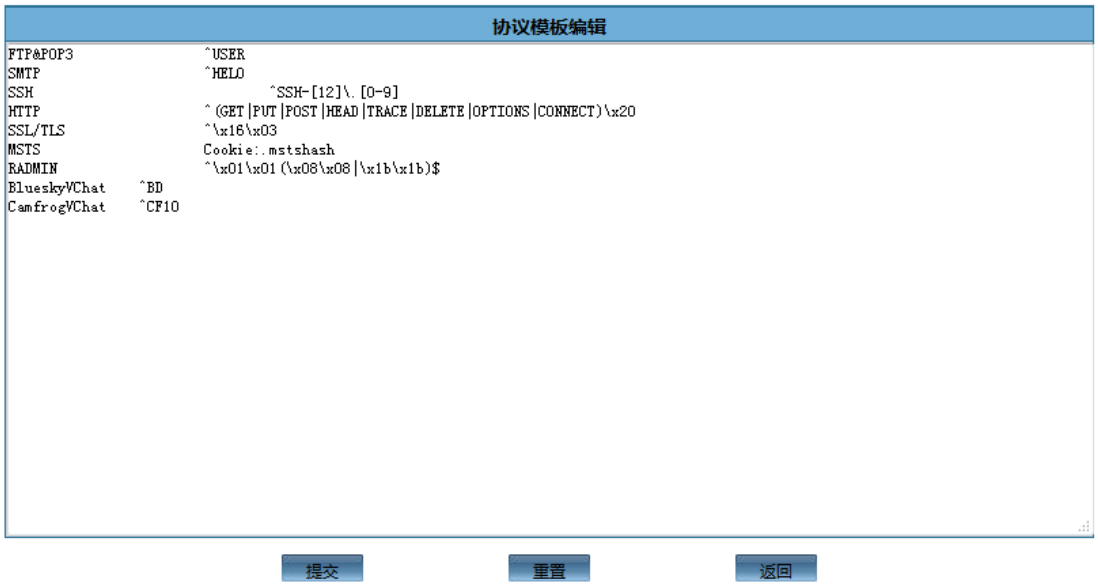


图 3.11 协议定义

◆ 防护模式有六种：超时连接、延时提交、超出屏蔽、关联信任、域名审计和接受协议。

■ 超时连接

设置超时连接标志后，此端口建立的连接如果持续一段时间保持空闲，则该连接将被重置以释放资源。此种策略对于某些应用可能造成连接数据中断的情况，此时应把相应端口设为禁止屏蔽。

■ 延时提交

设置此选项的端口，系统将无限缓存该连接，除非客户端有数据发送或者该连接被重置。

■ 超出屏蔽

设置超出屏蔽后，客户端在此端口进行的访问如果连接数大于连接限制设置的数值，则此客户端将被屏蔽。

■ 关联信任

用于设置游戏的防御，指定在连接游戏端口之前连接验证端口。

■ 域名审计

设置启用域名管理黑、白名单策略，配置全局参数中 DomainAudit.AuditMode 使用。

■ 接受协议

可用于设置各端口指定接受的协议类型。

◆ 防护模块

TCP 端口防护模块是针对特殊应用而开发的防护手段。

3.3.2 开启防护模块

开启 TCP 防护模块有两种方式，一种是在连接攻击检测处填写一个数值，当 TCP 新建连接达到此值时，将自动开启 TCP 插件防御，当连接数低于此值一段时间后，TCP 插件防御将取消，如下图所示：

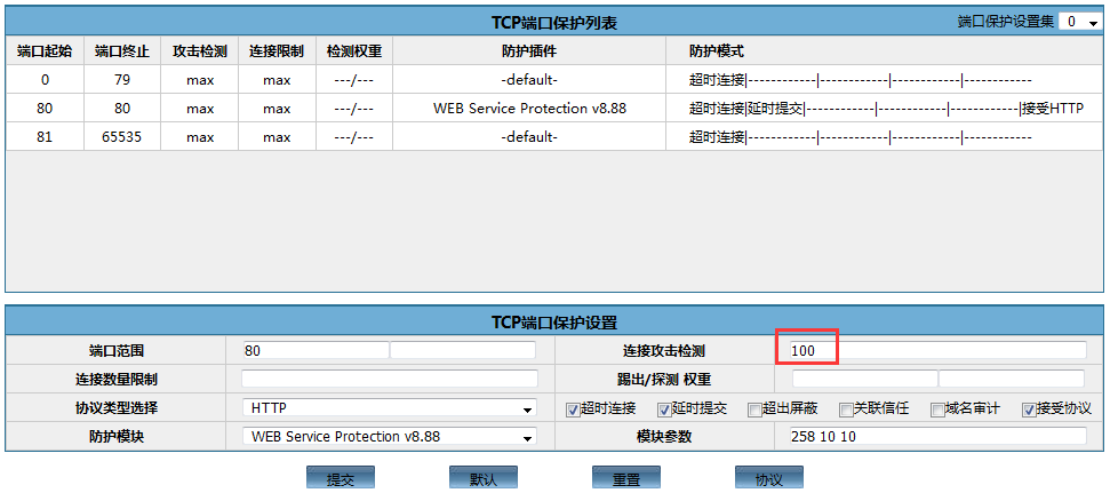


图 3.12 连接攻击检测

另一种方式是在主机设置中的防护插件中勾选相关插件，这样则强制开启 TCP 防御插件，如下图所示：

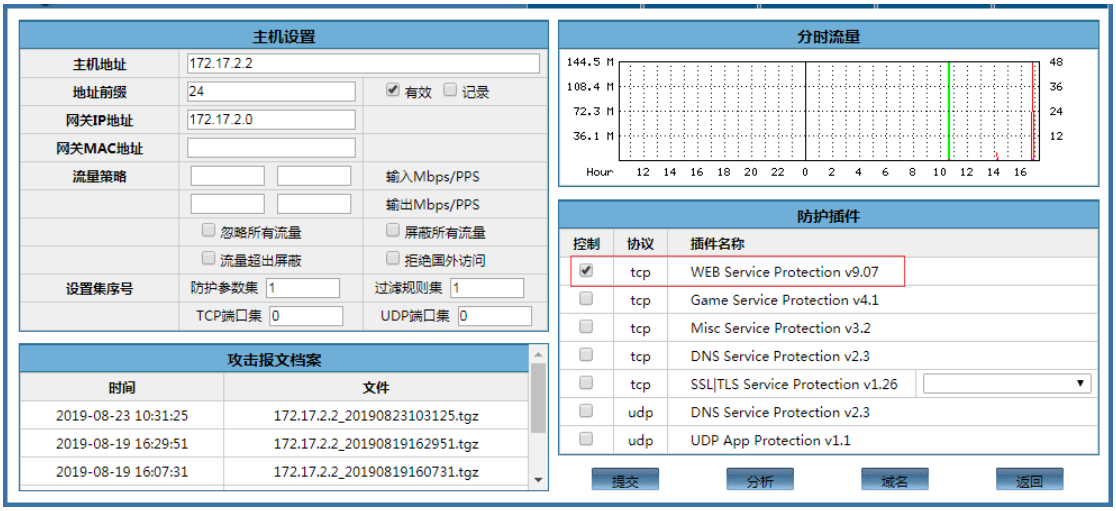


图 3.13 手动勾选防护插件

3.3.3 插件参数

3.3.3.1 WEB Service Protection

动态验证策略是中新金盾抗拒绝服务系统特适用于 Web 服务的一种防护方案，是针对目前愈演愈烈的 CC-HTTP Proxy 类攻击而开发的。应用此种策略的端口，系统将对进入的 HTTP 请求进行验证操作，确保该请求来自正常的客户浏览行为，而非正常的访问行为（如通过代理进行攻击等）将被加入黑名单进行屏蔽；动态验证模块，只对设置了 WebCC 保护模式的主机采用该验证策略，没有设置该保护模式的主机不受影响。

金盾抗拒绝服务系统使用 WEB Plugin 来对 HTTP 类攻击进行防御。当客户端访问服务器时，WEB Plugin 会返回脚本让客户端进行计算，然后客户端返回计算结果，如果结果正确，则通过插件验证，将该客户端列入正常的用户列表，如果结果错误，则屏蔽此客户端 IP，攻击器无法解析脚本，无法完成验证码的计算。

设置界面如下图所示：

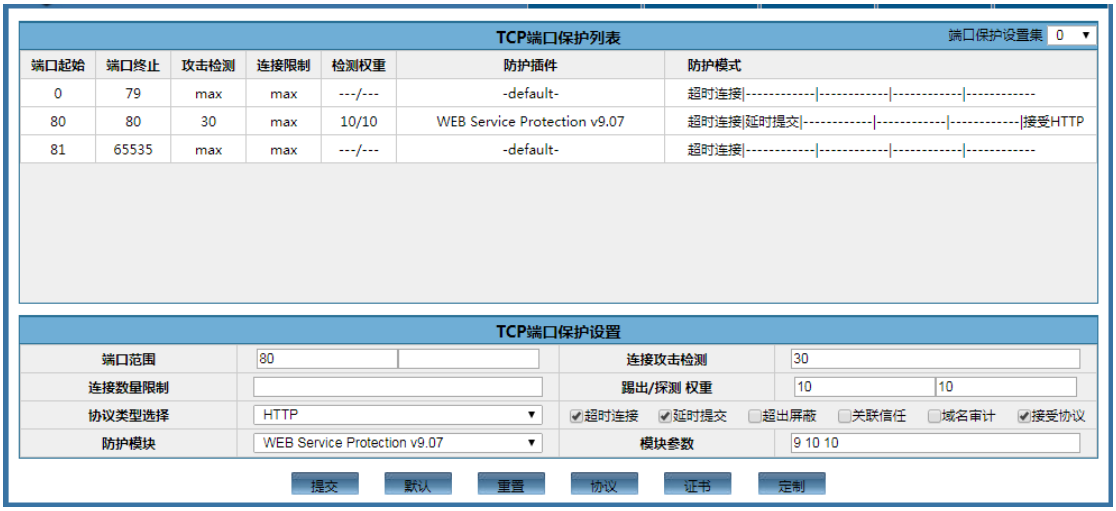


图 3.14 添加 Web 插件

防护模块中选择 WEB 防护模块，模块参数一共有 9 组，后面的模块参数这里填写的是 259 10 10 1，每个参数的意义如下：

- 参数一：启用的验证模式。此值大于 256，表示对所有类型的页面进行验证
  a. 0 或 256：不执行跳转过程。
  b. 1 或 257：一般验证模式，不需要手工干预。
  c. 2 或 258：复杂验证模式，不需要手工干预。
  d. 3 或 259：严格验证模式，打开网页时会出现点击进入的对话框，手工点击进入，有中文和英文字体。
  e. 4 或 260：完美验证模式，需要配合验证服务器进行验证，需要输入验证码。
  f. 5 或 261：重定向验证模式，不需要手工干预。HTTP 1.1 POST 验证时返回 307，其它验证返回 302。
  g. 6 或 262：多种脚本运行方式，随机选择以一种生成验证脚本。
  h. 7 或 263: 图片验证码方式验证，需要手动输入验证码，不需要验证服务器。
  i. 8 或 264：手动点击跳转，由用户手动点击，有中英繁三种选择（V9.06）
  j. 9 或 265：滑动滑块验证（V9.07）
- 参数二：对同一个页面的请求次数，如果超过次设置值，则该客户端将被屏蔽。一般默认设置 10 至 30 之间；
- 参数三：监测服务器回应，若超过次数值没有 304 Not Modified，则执行一次异常。一般默认设置 10 至 30 之间；
- 参数四：验证脚本使用 gz 压缩开关；0 未开启 gz 加密、 1 开启 gz 加密。

- 参数五： 验证脚本中英文提示；0 显示中文 "点击继续访问" 、1 显示英文 "click to continue"；
- 参数六：不做异常屏蔽代码
  a. --1：HTTP 头部报文检测，对应参数 1，配置 1，则不会屏蔽头部异常的连接，屏蔽代码 00010015
  b. --2：认证请求检测，对应参数 1，则 web 插件不会屏蔽认证请求连接，屏蔽代码 00010016
  c. --4：对应参数 2（相同请求次数），配置 4，不会屏蔽，屏蔽代码 00010017
  d. --8：对应参数 3（检测 304），配置 8，不会屏蔽，屏蔽代码 00010018
  e. --16：挎包检测，对应参数 1，配置 16，不会屏蔽挎包，屏蔽代码 00010019
  f. --32：认证服务器检测（参数 1 的 4），对应参数 1，配置 32，不会屏蔽认证服务器，屏蔽代码 0001001E
  g. --组合：比如设置 7=1+2+4，则上述中前三个都不会屏蔽
- 参数 7：WEB 插件定制页面索引值

3.3.3.1.1 插件定制

图 3.15 定制页面

- 认证方法
  - 表达式重定向认证（第一个参数设置 3/259）
  - 验证码认证（第一个参数设置 7/263）
  - 脚本认证（第一个参数设置 9/265）

  详细使用方案可参考定制页面帮助按钮。

图 3.16 定制帮助

◆ 表达式重定向认证示例

index.html

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>WEB插件表达式重定向验证</title>
    <PLUGIN_AUTHENTICATION>WEB插件表达式重定向验证</PLUGIN_AUTHENTICATION>
</head>
<body>
</body>
</html>
```

图 3.17 表达式重定向认证示例

◆ 验证码认证示例

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>WEB插件验证码认证</title>
    <link rel="stylesheet" type="text/css" href="https://cdn.bootcss.com/twitter-bootstrap/4.3.1/css/
    bootstrap.min.css">
</head>
<body>
    <PLUGIN_AUTHENTICATION>
        <div>
            <div id="img2" style="width: 120px;height: 60px"></div>
            <form class="form-inline">
                <input class="form-control" id="inputRandom" type="text" placeholder="请输入验证码">
                <input class="btn  btn-danger" type="button" onclick="_click()" value="提交验证">
            </form>
        </div>
    </PLUGIN_AUTHENTICATION>
</body>
</html>
```

图 3.18 验证码认证示例

◆ 脚本认证示例

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>WEB插件脚本认证</title>
    <link rel="stylesheet" type="text/css" href="https://cdn.bootcss.com/twitter-bootstrap/4.3.1/css/
    bootstrap.min.css">
    <script type="text/javascript" src="https://cdn.bootcss.com/jquery/3.3.1/jquery.min.js"></script>
</head>
<body>
<h2>WEB插件脚本认证</h2>
<div id="content"></div>
<button class="btn btn-primary" onclick="webCodeAuthTest();return false;">点击我啊</button>
</body>
</html>
<script type="text/javascript">
    function webCodeAuthTest() {
        $('#content').text('这个是点击之后出来的，说明你正在进行验证');
        <PLUGIN_AUTHENTICATION></PLUGIN_AUTHENTICATION>
    }
</script>
```

图 3.19 脚本认证示例

◆ 定制配置

如图导入 index.html，索引序号是 1，认证方式是表达式重定向认证。在 tcp 端口保护中 web 插件第七个参数设置 1 则应用此定制页面，如果索引值 1 不存在，则按照原始参数 3 的“点击继续访问”。

图 3.20 定制列表

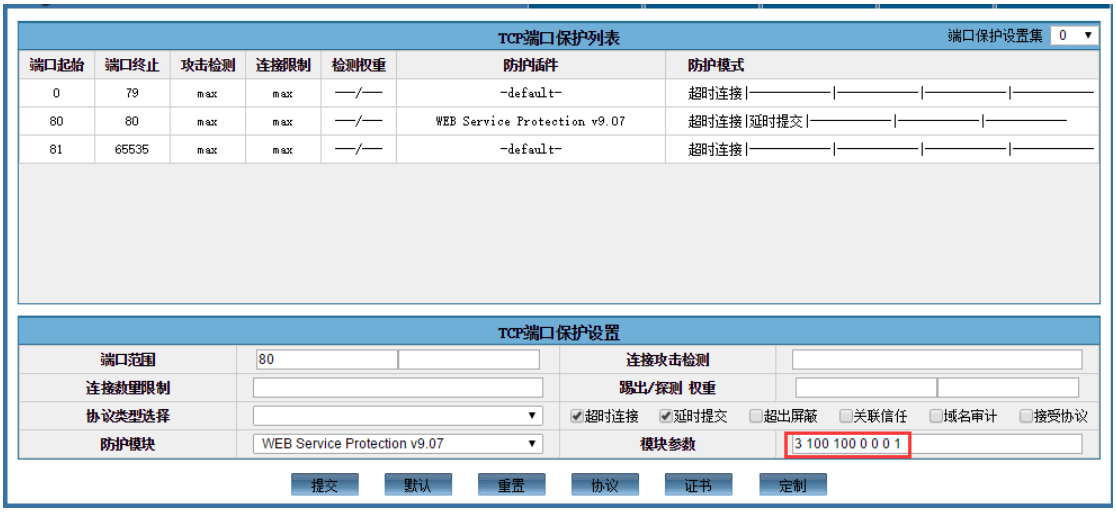


图 3.21 定制配置

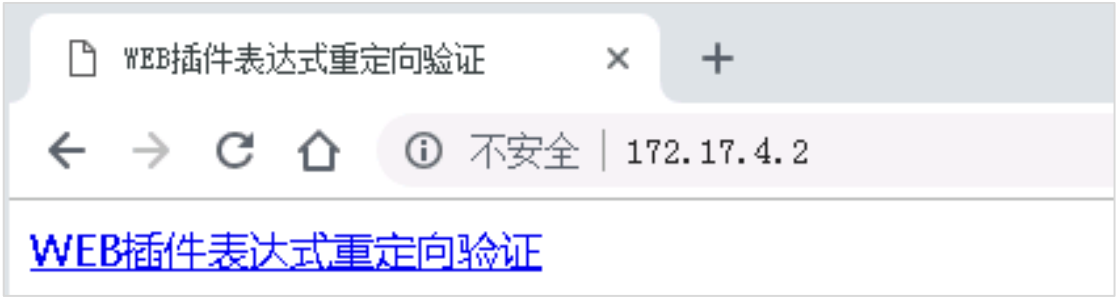


图 3.22 展示页面

3.3.3.2 SSL|TLS Service Protection

HTTPS 业务数据均是加密数据。当被攻击时，传统的防护手段只能通过限制 Hello 频率或者 Exchange 频率，防护效果不佳，SSL|TLS 插件可对数据进行解密并有效防护。

步骤一：导入证书（可选）

【攻击防御】→【TCP 端口保护】→【证书】→填写相关参数并导入证书和私钥。

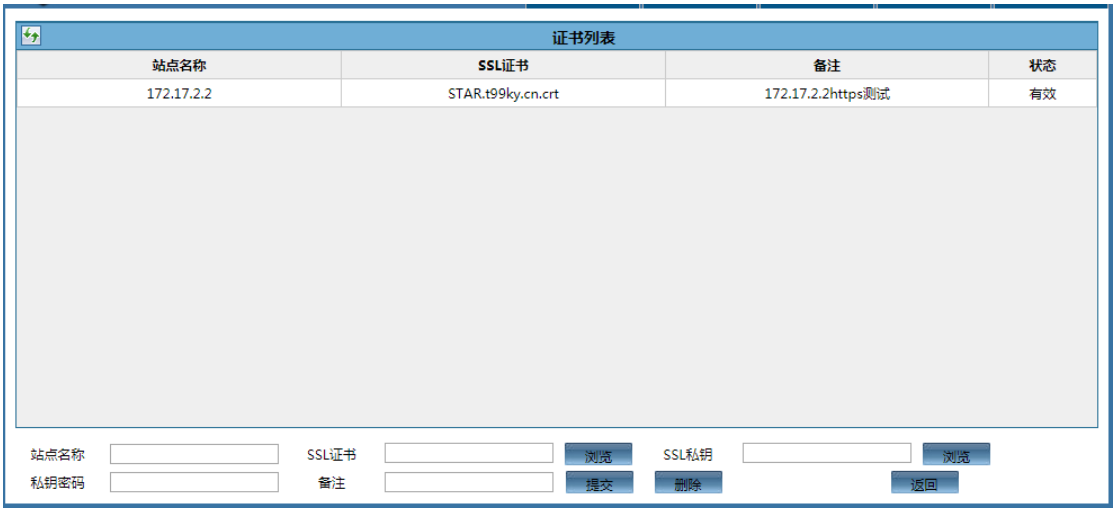


图 3.23 证书管理

步骤二：选择证书

【状态监控】→【主机状态】→【主机设置】→防护插件选择 SSL|TLS 后面的证书选择框→【提交】。

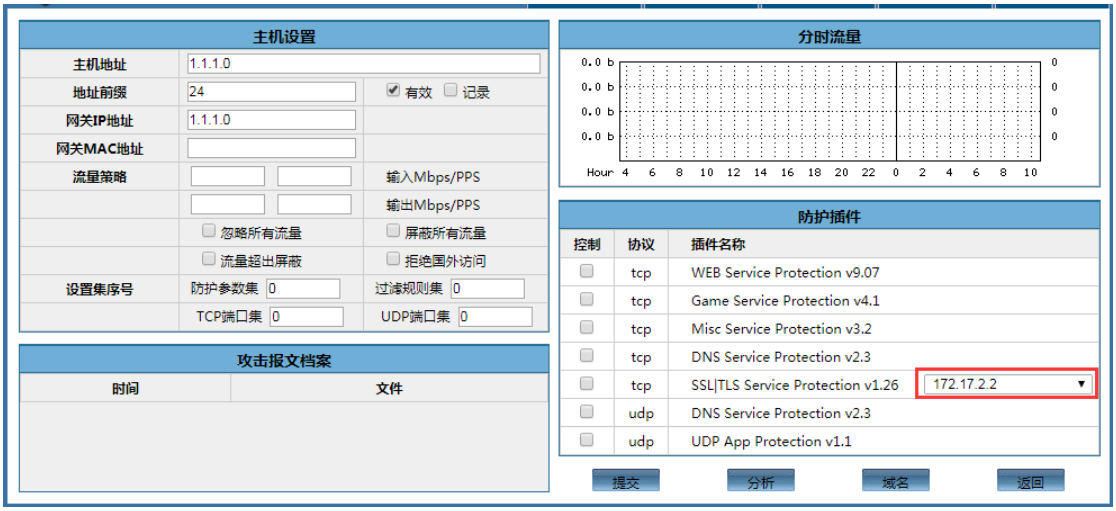


图 3.24 证书应用

步骤三：设置 SSL 插件

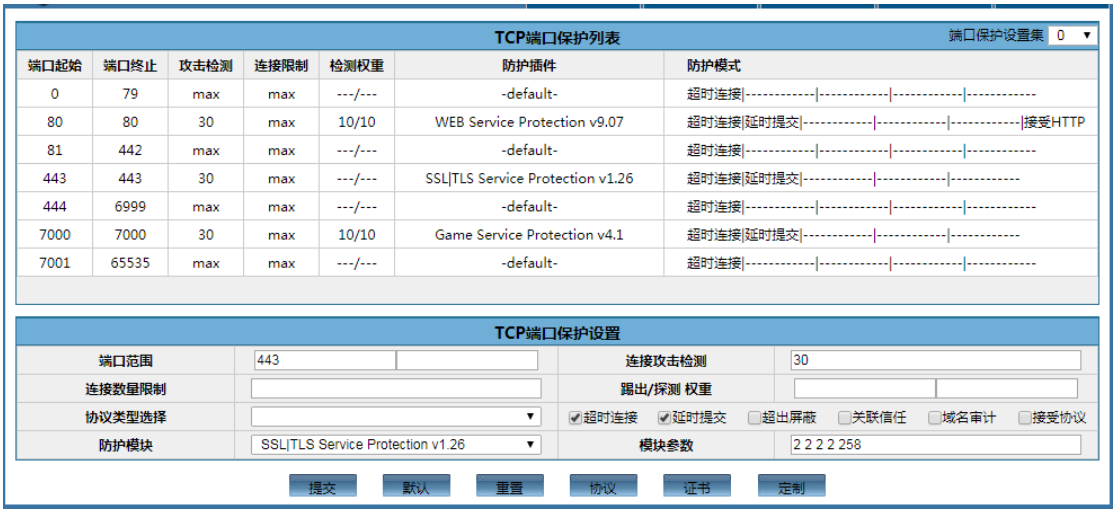


图 3.25 设置 SSL 插件

参数详解

1. 参数 1: ssl_method，SSL 插件防护方法，取值 0、1、2:
   a. == 0: SSL 防护，仅检查 client-hello 报文合法性、频率检测和 client-key-exchange 的频率检测，无须导入证书
   b. == 1: SSL 防护，导入证书和密钥对报文解密，客户端可以和墙完成握手协议则认证通过
   c. == 2: HTTPS 防护，入证书和密钥对报文解密后，基于现有的丰富的 web 插件功能来防护 HTTPS 攻击
2. 参数 2: connect_linit:同一个 IP 的连接数超过阈值，开启握手协议代理
3. 参数 3: hello_limit: client-hello 报文频率检测
4. 参数 4: key_exchange_limit: client-key-exchange 报文频率检测

参数 5：HTTP 启用的验证模式，即从参数 5 开始配置参数和 WEB 插件配置参数一样。

3.3.3.3 Game Service Protection

- 对于刷端口攻击，很多攻击器都是对同一个端口频繁建立连接。因此插件判断某个客户端是否打开若干个服务器端口，若只对同一个端口频繁连接，则会屏蔽该客户端。
- 对于游戏应用来说，服务器回应的数据比客户端发送的数据要大很多，因此该插件还会判断客户端同服务器之间的数据比例，如果比例无法达到设定值，则会屏蔽该客户端。
- 对于传奇假人攻击，插件会在玩家登陆 30 秒后发送验证码对话框，玩家若无法完成验证码的输入，则会被断开连接。次数过多则会被屏蔽。

参数设置如下图所示：

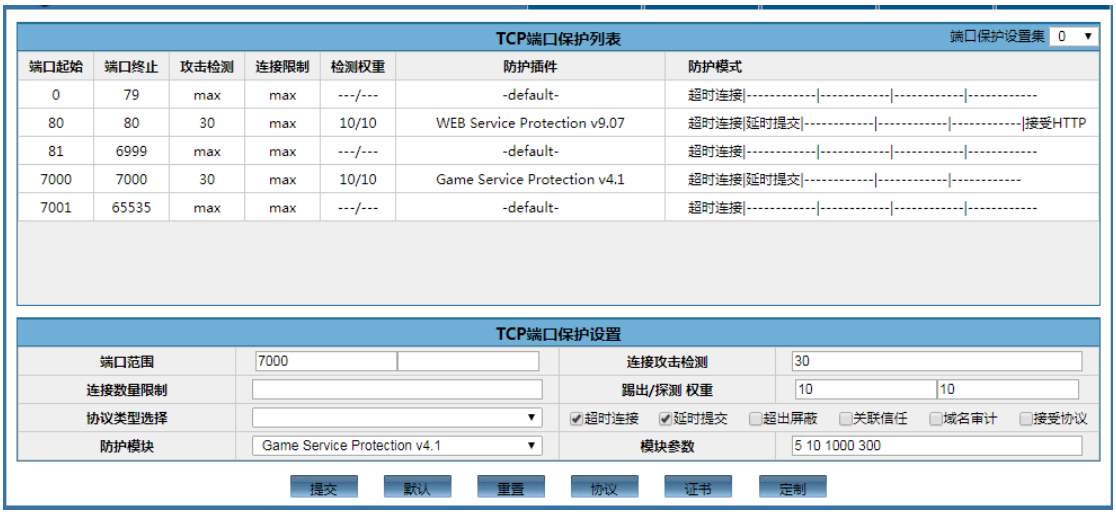


图 3.26 添加 game 插件

参数 1： 客户端连接次数

参数 2： 客户端发送的报文数

参数 3： 客户端发送的字节数

参数 4： 服务器端需要做的回应字节数

参数 5： 相同数据部分字段的连接次数

参数 6： 检测数据部分的起始位置

参数 7： 检测数据部分的结束位置

3.3.3.4 Misc Service Protection

Misc 模块主要用于防护游戏，Misc 模块可以自定义回复数据，分为两种情况，第一种为默认：0-ftp，1-smtp，2-pop3。第二种是自定义：10-17，是 8 组自定义回复策略，用于建立连接后服务器首先发送固定数据给客户端，然后客户端回复固定数据，需要在系统环境变量里，设置 misc.customdata，格式是：服务器回复数据:客户端回应的正则表达式，主要是用于游戏连接时，服务器先回复固定数据，然后客户端发送的第一个包的数据相同，可以设置最多 8 组，设置如下图所示：

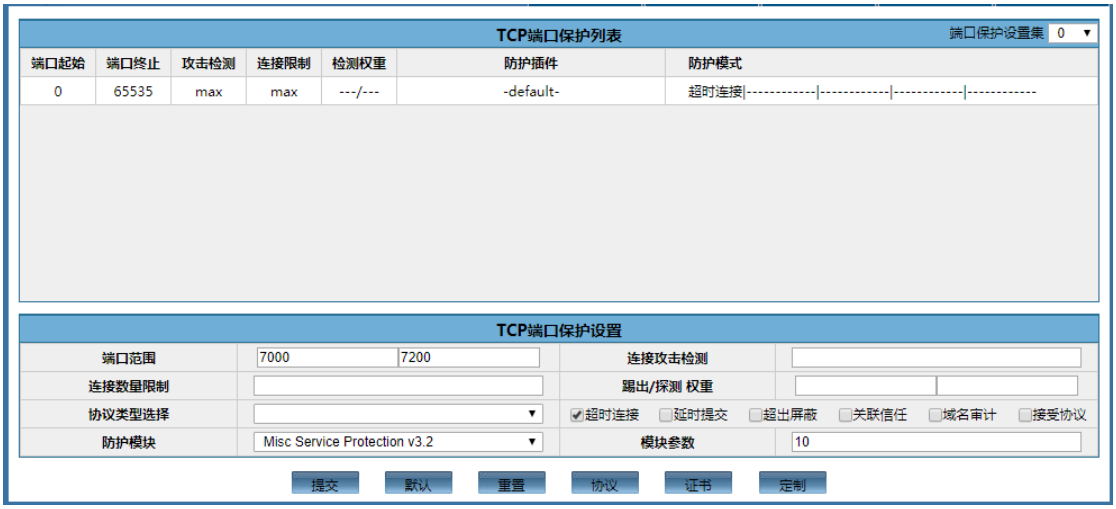


图 3.27 添加 Misc 插件

此时代表建立连接后服务器先发送固定数据，为 00011231，然后客户端回应数据的开始两个字节为\x16\x03。如果建立三次握手后，不符合设置数据格式，将被屏蔽。

3.3.3.5 DNS 防护模块

◆ DNS 防护模块如下图所示，开启 TCP 53 端口的 DNS 插件防御，有的客户端也可以用 TCP 的 53 端口进行 DNS 解析，所以建议 TCP 的 53 端口也开启 DNS 插件防御

图 3.28 添加 DNS 插件

普通防御，设置为参数 10 1 即可，第一个 10 表示每秒允许查询 10*10000 次，第二个参数表示是否允许反向查询。

3.4 UDP 端口保护

【UDP 端口保护设置】模块页面提供了针对每个端口的独立设置参数，用户可根据某种端口的服务类型更改相应的处理策略。页面如下图所示：

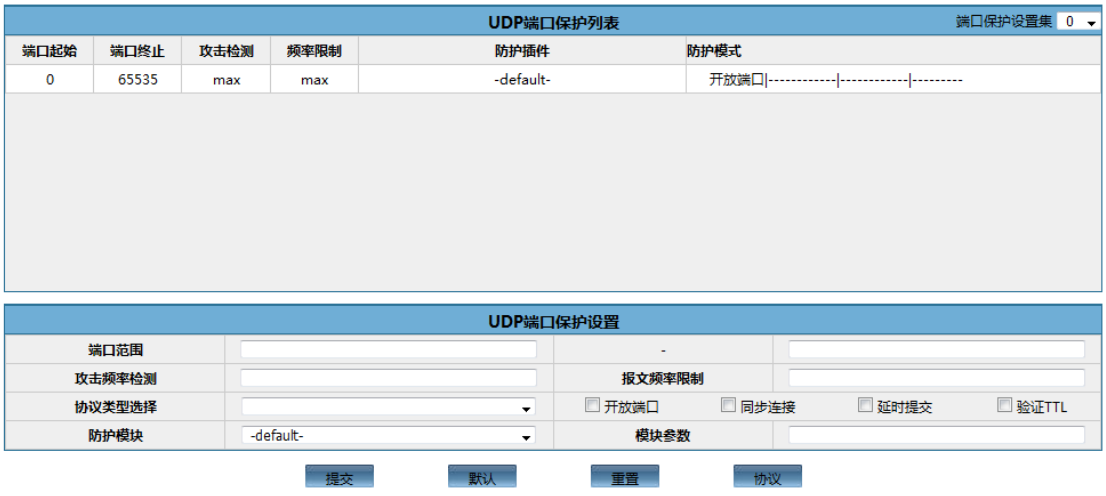


图 3.29 UDP 端口保护设置

- 端口保护设置集：对于一台主机可适用多项端口防护设置，也可用于同一端口的重叠设置，通过主机状态中的 TCP 端口保护集选择某台主机的生效端口防护。
- 提交：添加 TCP 端口保护设置。
- 默认：“默认”系统使用默认端口保护设置。

- 重置：重置 TCP 端口保护设置一栏所填参数。
- 协议：自定义协议类型。
- 端口起始/终止：显示设置防护的端口范围,默认针对“0-65535”端口进行防护。
- 攻击检测：显示设置端口的连接攻击检测频率数值，max 表示无限大。
- 频率限制：显示设置端口的连接数量限制数值，max 表示无限大。
- 防护插件：显示设置端口启用的防护模块类型，default 为默认防护。
- 防护模式：显示设置端口启用的防护标志有哪些，默认仅启用“开放端口”模式。

3.4.1 添加 UDP 端口保护

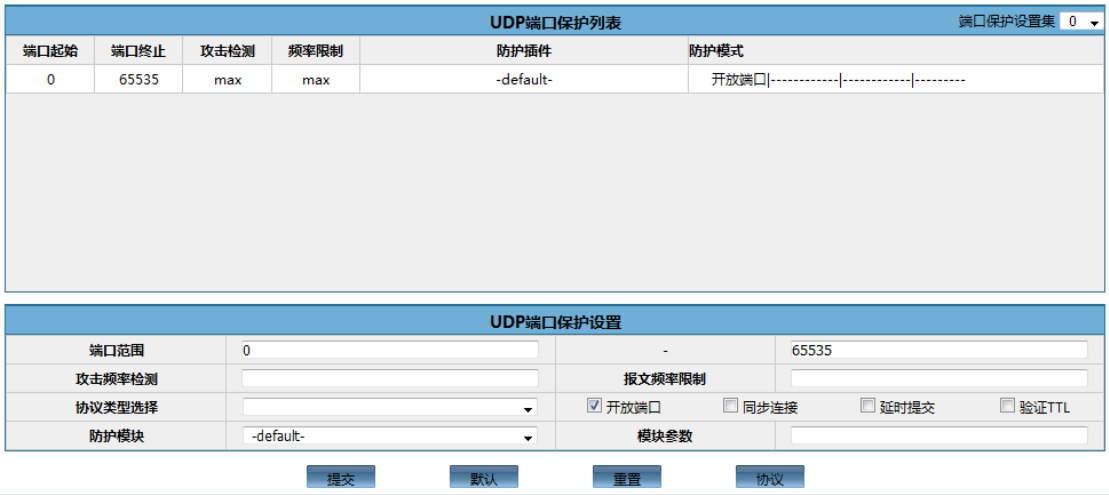


图 3.30 添加 UDP 端口保护

添加 UDP 端口保护中的各项参数除了防护模式外，其他含义同“TCP 端口保护”设置页面相同。

- 防护模式：防护模式有四种：开放端口、同步连接、延时提交、验证 TTL。
  - 开放端口：指设备会允许此端口的连接，如果没有选，设备就拦截外网进来的连接此端口的数据。
  - 同步连接：选中后，此端口（或范围）先得有 TCP 连接才会接受 UDP 连接，否则拦截 UDP 的数据包。
  - 延时提交：此选项主要用于防护 DNS-Flood，即丢弃 Client 发过来的第一次 DNS 请求，这个和 TCP 延时提交的意思不一样。
  - 验证 TTL：检测 UDP 包中的 TTL 值是否不一样（对 udp 数据的 ip 头部 ttl 进行统计，如果某个数值的 ttl 频率过高会进行屏蔽，可在一定程度上防御 udp 类攻击）的。

3.4.2 UDP APP Protection v1.1

◆ 该插件参数配置对应变量设置中 udpfilter.Data

配置文件中 index 配置索引。比如，在变量设置中 udpfilter.Data 中针对当前业务防护设置的客户端和服务器数据流信息在“index = {1};”中， 那么在 udp 端口保护中业务端口开启 UDP APP Protection v1.1 防护模块，对应模块参数就是 1。

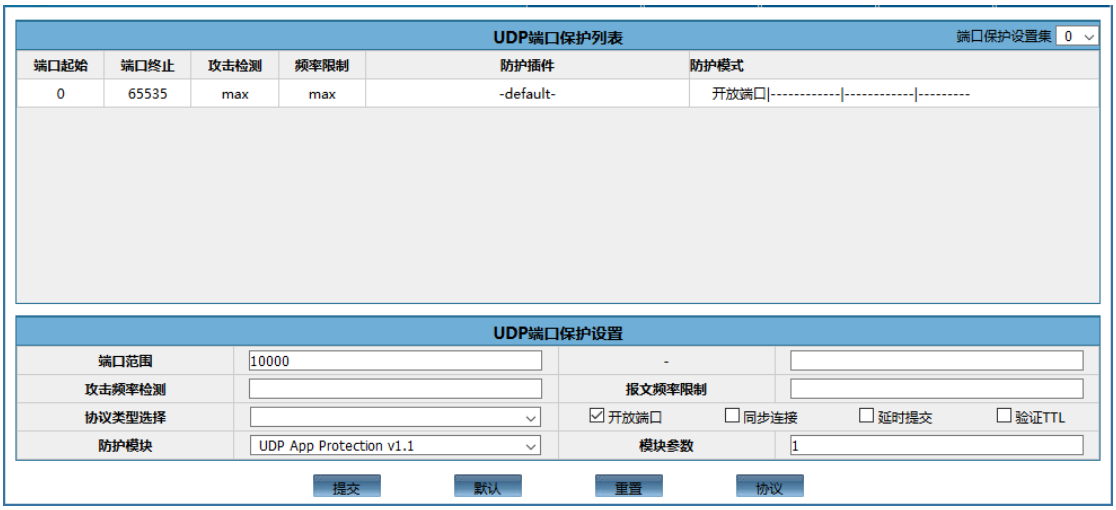


图 3.31 添加 UDP APP 防护

3.4.3 DNS 防护插件防御

如下图所示，开启 UDP 53 端口的 DNS 插件防御，有的客户端也可以用 TCP 的 53 端口进行 DNS 解析，所以建议 TCP 的 53 端口也开启 DNS 插件防御，方式和 UDP 的一样

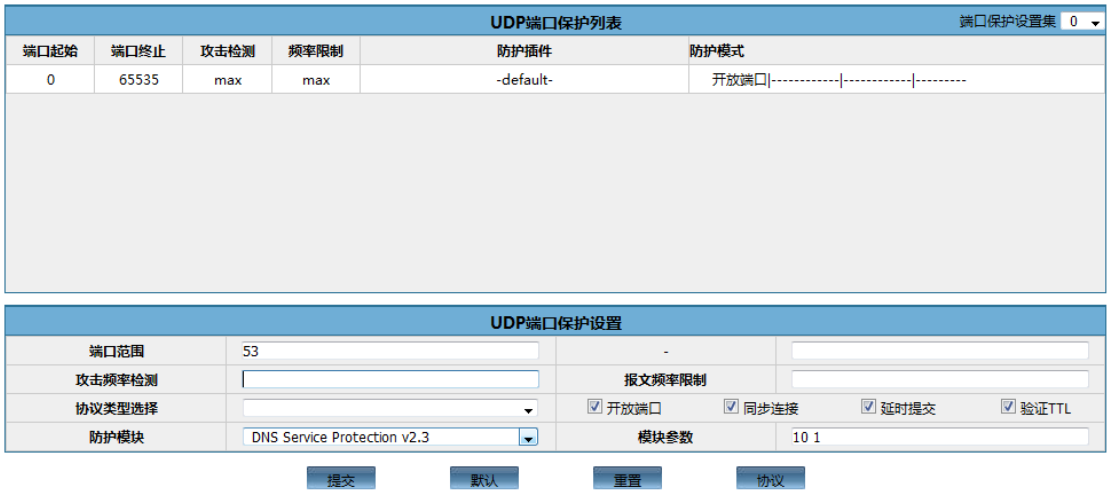


图 3.32 添加 DNS 防护插件

模块参数中的参数的意义：

第一个参数：为同时只回应参数*10000 个查询，比如上图中，同时只回应 100000 个回应。

第二个参数：为空或者 1,1 表示禁用反向 dns 解析信任机制。

开启此插件后，客户端的 DNS 查询都会被强制使用 TCP 进行查询，此时就需要服务器端支持 TCP 的 53 端口 DNS 查询。

3.4.4 开启插件

开启 UDP 插件防御有两种方式，一种是在攻击频率检测处填写一个数值，当收端口每秒接收到到 UDP 数达到此值时，将自动开启 UDP 插件防御，当连接数低于此值一段时间后，UDP 插件防御将取消，如下图所示：

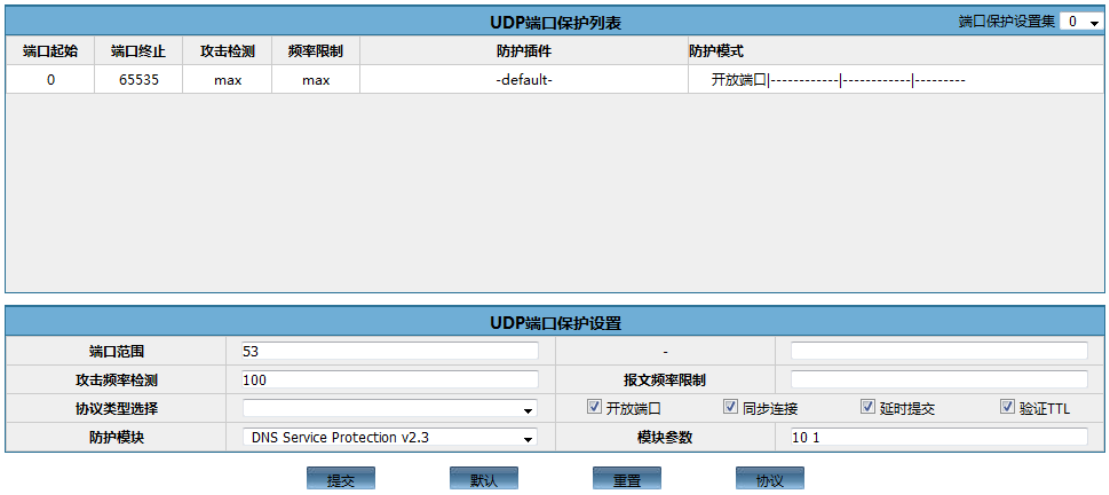


图 3.33 攻击频率检测

另一种方式是在主机设置中的防护插件中勾选相关插件，这样则强制开启 UDP 防御插件，如下图所示：

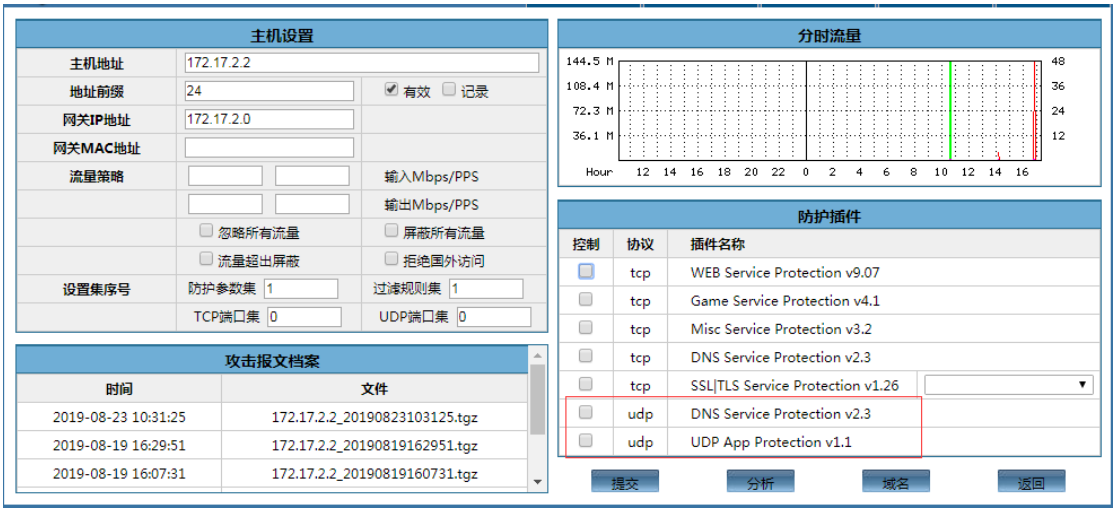


图 3.34 手段勾选防护插件

3.5 牵引设置

图 3.35 牵引设置

- 牵引策略选项：
  - 异常流量牵引：勾选开启牵引功能。
  - 主机牵引告警：勾选后主机被牵引的同时通过邮件进行告警。邮件信息在【系统配置】-【控管属性】-【邮件属性】中设置。
  - 流量限制模式牵引：勾选后，流量达到【监控状态】-【主机状态】-【主机设置】中的流量策略阈值后，自动牵引主机。
- 全局总流量：当全局流量达到阈值时开始牵引主机，配合“批量牵引主机”使用。
- 批量牵引主机：全局流量达到阈值后同时牵引多少台主机。

- 牵引触发流量：单台主机达到阈值时牵引该主机。
- 牵引释放方式：设定主机被牵引后，已何种方式取消牵引，分为【主机状态】和【牵引超时】。选择【主机状态】表示主机防护状态消失后自动取消牵引。【牵引超时】后设置对应的时间，超时后自动取消牵引。
- ACL 规则范围：用于需要登录牵引设备上面执行 ACL 里面的规则序列号。
- 手动牵引地址：手工设定主机进行流量牵引，此处需要填写具体的 IP 地址。
- 牵引：设定手动牵引主机地址后，点击"牵引"，该主机流量将被牵引。手动牵引地址可以设置自动释放时间，释放时间超时，该手动牵引的主机自动被释放。
- 取消：设定手动牵引主机地址后，点击"取消"，该主机流量将被取消牵引。
- 牵引脚本：此处脚本需要根据不同厂商交换或是路由设备进行正确填写，下面以思科和华为设备进行说明：

华为设备

```
 [-TELNET 1.1.1.1-]
username
password
system
<FLOWDIV_CANCEL_KEYWORD>undo     </FLOWDIV_CANCEL_KEYWORD>ip     route-static
<HOST_ADDRESS> 255.255.255.255 null0
quit
quit
```

思科设备

```
[-TELNET 1.1.1.1-]
username
password
enable
conf t
<FLOWDIV_CANCEL_KEYWORD>no  </FLOWDIV_CANCEL_KEYWORD>ip  route  <HOST_ADDRESS>
255.255.255.255 null0
exit
exit
```

提示：

telnet 后面 IP 地址表示交换机管理地址，也可以支持 HTTP 方式登录

"<<#### ####>>"此标识符表示对账号或密码进行加密，比如交换机登录密码是"123"，那么可以用"<<####123####>>"进行密码加密。

"<FLOWDIV_CANCEL_KEYWORD>"是取消牵引时变量。

"<HOST_ADDRESS>"牵引主机变理。

- 牵引日志：牵引时，登录牵引设备执行的命令。
- 牵引主机列表：显示被牵引的主机和释放时间。

3.6 变量设置

针对有一定访问规律的 udp 攻击。用于防护具有一定访问规律的 UDP 攻击。此模块防护攻击时需要客户端第一次请求数据、服务器回应数据、确认回应的数据固定。使用之前需要对配置文件进行设置。

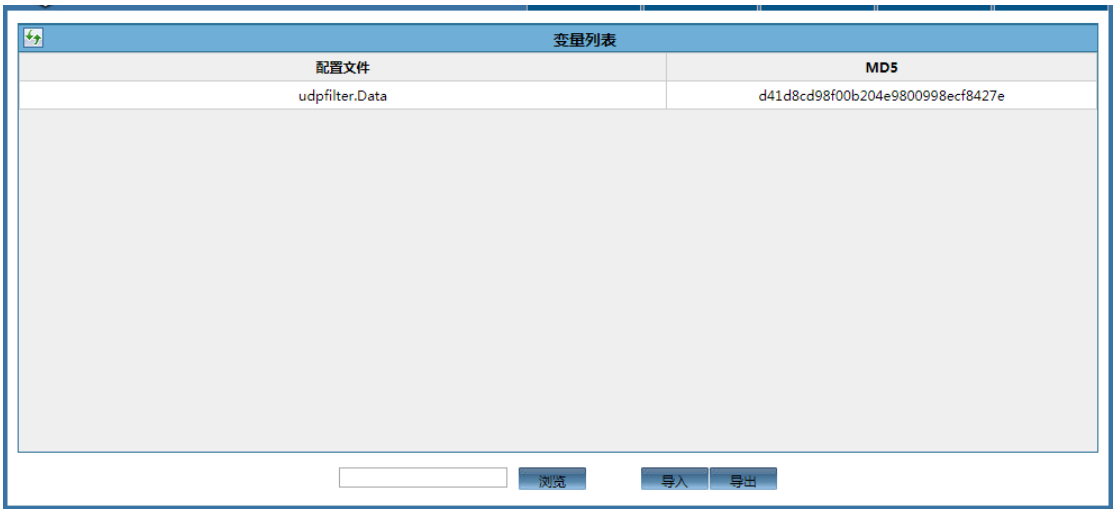


图 3.36 变量设置

提示：

“udpfilter.Data”文件里，如果索引为“0”，那么设置插件时，模块参数需要写“0”，但提交后模块参数不显示，建议索引不要从“0”开始，可以从“1”开始定义，最大可以定义 1024 个。

4 日志分析

4.1 日志列表

【日志管理】模块列出系统中所有的日志项，并可按事件进行分类。页面如下图所示：

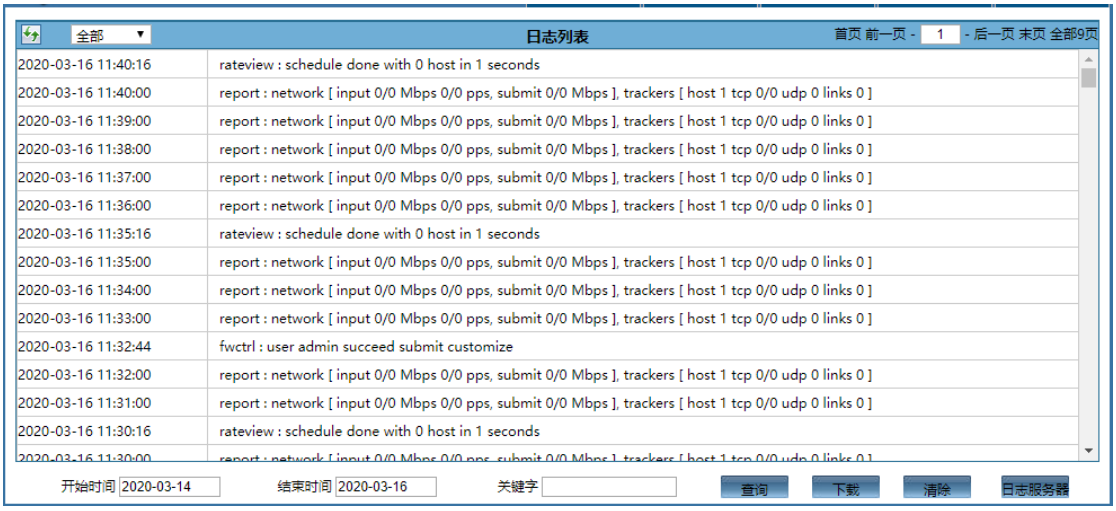


图 4.1 日志管理

系统日志管理中的日志列表可清晰查看设备各项操作记录,并记录设备每分钟流量、CPU 和内存使用情况。

◆ 日志列表

显示详细日志时间，并记录该时间内设备的状态及操作记录。“全部”记录到的所有日志信息；“重要事件”记录重启信息；“防护事件”记录是否进入防护状态及相关防护信息；“普通事件”记录网络使用流量、CPU 和内存，以及各项操作权限所进行的操作记录。

◆ 日志类型下拉框

选择日志类型进行下载和查看，类型包括：重要事件、防护事件以、普通事件和用户事件。

◆ 开始时间/结束时间

选择需要查询的日志时间段。点击查询按钮后设备将罗列除所有符合时间的日志记录。

- 关键字

  通过关键字查询相关的日志。关键字可以是一个 ip，也可以是一个词组。

- 下载

  下载当前日志，输出文本为.txt。

- 清除

  清除所有日志。

- 日志服务器

图 4.2 日志服务器

支持不同事件类型发送到不同的日志服务器，格式：IP:PORT 或者域名:PORT。

4.2 攻击分析

开启该模块方法：在【系统配置】→【控管属性】→【控管特性】中勾选【异常攻击分析】。目的主机只支持单个主机查询。

图 4.3 攻击分析

4.3 分析报告

【分析报告】模块统计出了设备全局的最大以及平均的流量、连接值，并可以查询单个主机的防护状态以及连接、流量记录。如下图所示：

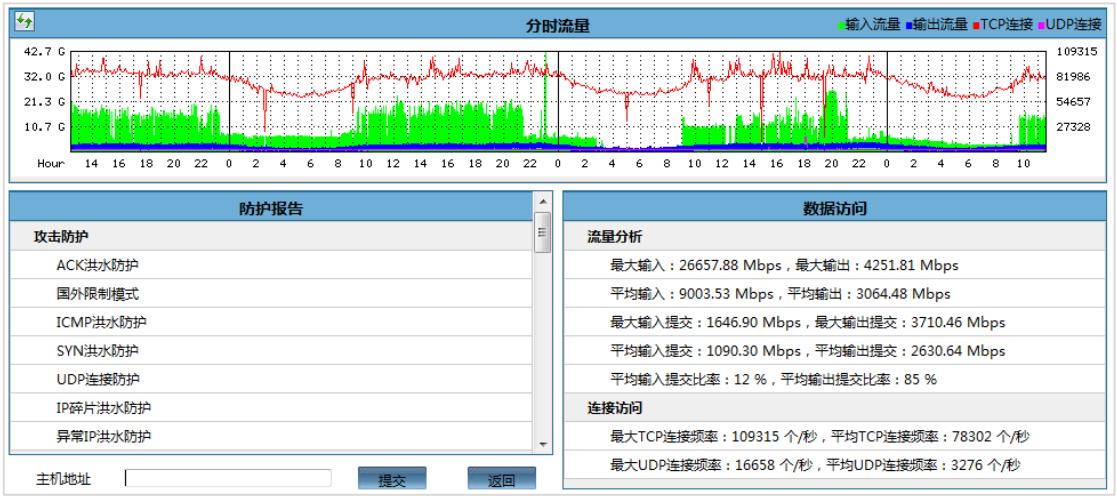


图 4.4 分析报告

- 主机地址：在该栏填写相应主机可查询对应主机的相关信息，只支持单个主机查询。：

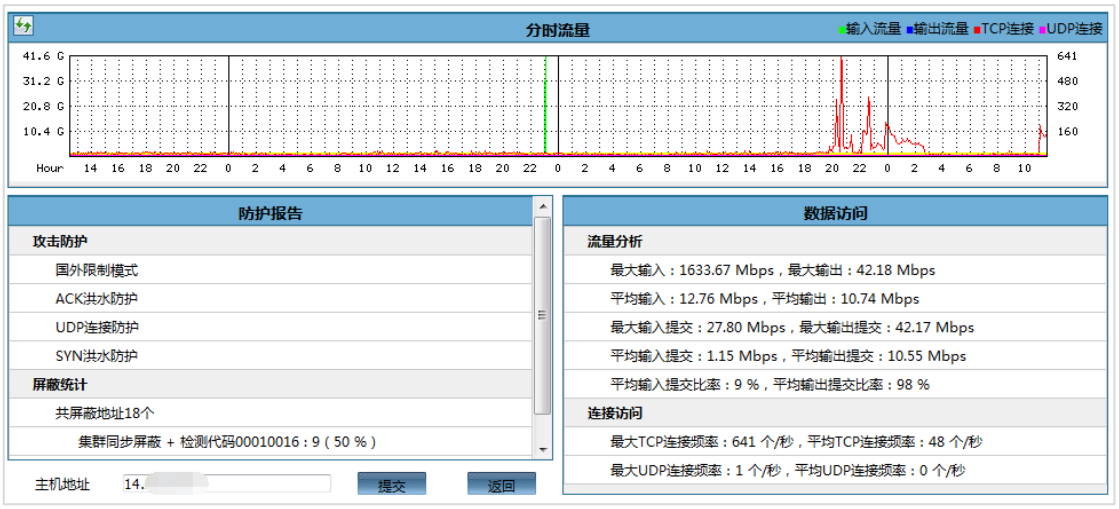


图 4.5 单个主机分析报告

- 分时流量：该栏主要记录了单个主机三天内的流量、连接输入输出情况。
- 防护报告
  - 攻击防护：查看主机三天内所触发的防护参数。
  - 屏蔽统计：列出出主机三天内被屏蔽原因的百分比统计。
- 数据访问
  - 流量分析：列出主机一天内主机流量的最大输入、输出和平均输入、输出流量。
  - 连接分析：列出相应主机一天内 TCP、UDP 单位时间内最大连接以及平均连接频率。

4.4 TOP 分析

【TOP 分析】模块统计出了最近五分钟、一个小时、一天或指定时间段内输入流量排名前 10、前 50、前 100、前 500 的主机信息。如下图所示：

图 4.6 TOP 分析

4.5 流量分析

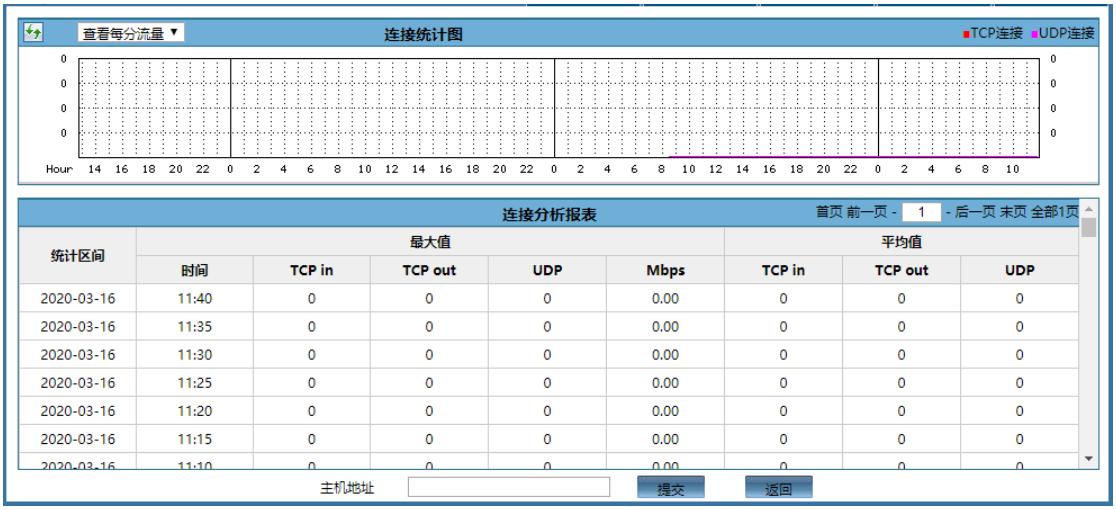
【流量分析】模块统计出了全局以及单个主机的每日和每月的最大、平均的流量输入、输出报表。如下图所示：

图 4.7 流量分析

- 查看方式下拉列表：可以选择查看每日或者每月的流量输入输出报表。
- 流量统计图：图形方式显示全局/主机的流量统计。
- 流量分析报表：记录了全局/主机最近六天内输入、输出流量的最大值以及平均值。
- 主机地址：输入想要查询的单个主机的 IP，即可查询该主机六天内的流量输入输出情况。默认不输入主机 IP 查询则显示为全局流量，只支持查询单个主机。

4.6 连接分析

【连接分析】模块用于查询全局/单个主机的一天/一月内的最大、平均连接值。如下图所示：



统计区间	最大值					平均值		
	时间	TCP in	TCP out	UDP	Mbps	TCP in	TCP out	UDP
2020-03-16	11:40	0	0	0	0.00	0	0	0
2020-03-16	11:35	0	0	0	0.00	0	0	0
2020-03-16	11:30	0	0	0	0.00	0	0	0
2020-03-16	11:25	0	0	0	0.00	0	0	0
2020-03-16	11:20	0	0	0	0.00	0	0	0
2020-03-16	11:15	0	0	0	0.00	0	0	0

图 4.8 连接分析

- 查看方式下拉列表：可以选择查看每日或者每月的连接输入输出报表。
- 连接统计图：图形方式显示全局/主机的连接统计。
- 连接分析报表：记录了全局/主机最近六天内输入、输出的 TCP 以及 UDP 连接的最大值以及平均值。
- 主机地址：输入想要查询的单个主机的 IP，即可查询该主机六天内的 TCP 以及 UDP 连接输入输出情况。默认不输入主机 IP 查询则显示为全局流量。

4.7 事件分析

该栏罗列出了主机六天内的所触发的防护参数事件以及最大/平均的的输入输出数据包频率。统计方式有：BPS、PPS 以及 SPS。如下图所示：

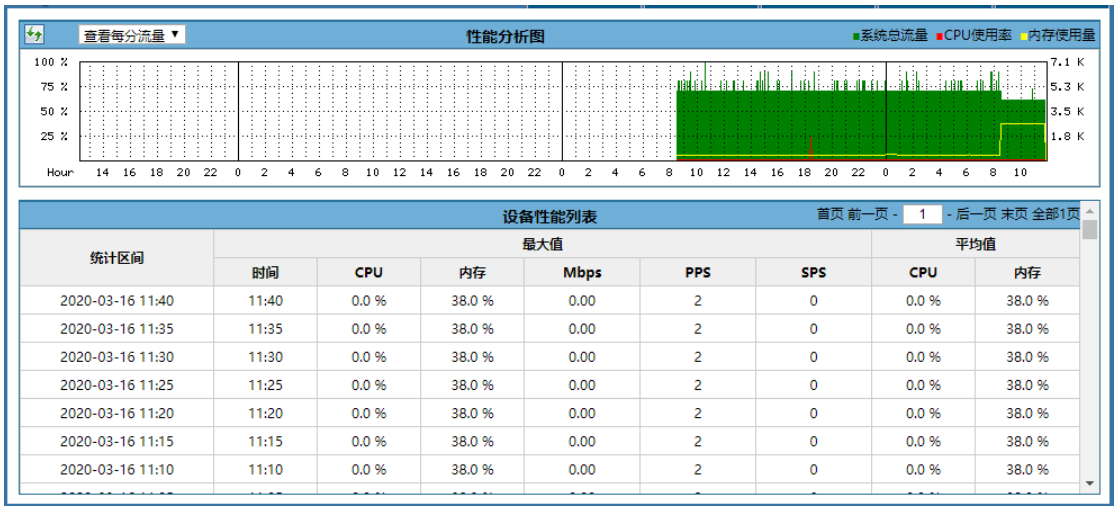
事件时间	主机地址	事件类型	累计流量	最大值			平均值		
				Mbps	PPS	SPS	Mbps	PPS	SPS
2020-03-16 11:40	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 11:35	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 11:30	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 11:25	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 11:20	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 11:15	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 11:10	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 11:05	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 11:00	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 10:55	global		0.23	0.00	3	0	0.00	3	0
2020-03-16 10:50	global		0.23	0.00	2	0	0.00	2	0
2020-03-16 10:45	global		0.23	0.01	3	0	0.01	3	0
2020-03-16 10:40	global		0.23	0.00	2	0	0.00	2	0

图 4.9 事件分析

◆ 地址：在该栏输入特定 IP 提交后即可查看单个主机的统计信息。

4.8 性能分析

【性能分析】模块列出了系统的最大/平均输入输出流量以及 CPU 和内存的使用率。如下图所示：



统计区间	最大值						平均值	
	时间	CPU	内存	Mbps	PPS	SPS	CPU	内存
2020-03-16 11:40	11:40	0.0 %	38.0 %	0.00	2	0	0.0 %	38.0 %
2020-03-16 11:35	11:35	0.0 %	38.0 %	0.00	2	0	0.0 %	38.0 %
2020-03-16 11:30	11:30	0.0 %	38.0 %	0.00	2	0	0.0 %	38.0 %
2020-03-16 11:25	11:25	0.0 %	38.0 %	0.00	2	0	0.0 %	38.0 %
2020-03-16 11:20	11:20	0.0 %	38.0 %	0.00	2	0	0.0 %	38.0 %
2020-03-16 11:15	11:15	0.0 %	38.0 %	0.00	2	0	0.0 %	38.0 %
2020-03-16 11:10	11:10	0.0 %	38.0 %	0.00	2	0	0.0 %	38.0 %

图 4.10 性能分析

◆ 查看方式下拉列表：可以选择查看每日或者每月的连接输入输出以及 CPU/内存负载报表。

4.9 攻击档案

开启该模块方法：在【系统配置】-【控管属性】-【控管特性】中勾选【异常攻击分析】、【攻击报文归档】。【攻击报文档案】页面如下图所示：

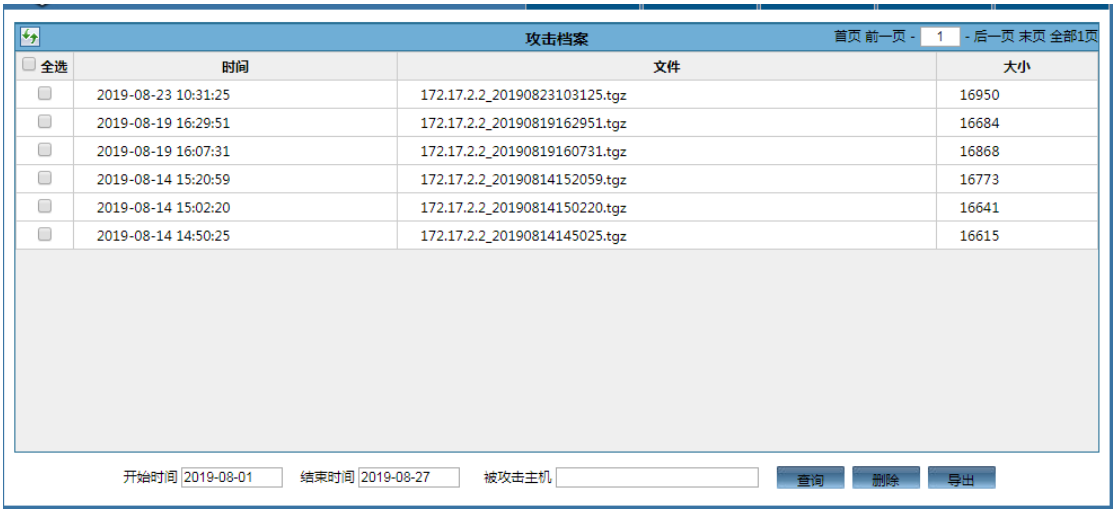


图 4.11 攻击档案

- 时间：抓取报文的时间
- 文件：抓取的报文文件名，以”IP_time.tgz”格式命名。
- 大小：抓取的报文大小，单位 Byte。
- 被攻击主机：查询主机 IP 对应的抓包文件或者删除主机 IP 对应的抓包文件。
- 文件：选择某一个报文文件后，可以将该文件导出到本地进行报文分析。
- 每个主机最多保存 10 条记录。

4.10 报表管理

通过邮件或 tftp 方式获取设备上的报表文件，勾选 tftp 传递后会出现配置 tftp 服务器一栏。或者直接勾选报表类型导出。

图 4.12 报表管理

- 同步方式：支持邮件或 tftp 按同步周期发送报表。
- 邮件传递：勾选表示将定期发送邮件到对应邮箱。
- TFTP 传递：勾选表示定期向 TFTP 服务器发送报表。设置此项后需要添加 TFTP 服务器地址。如下图所示：

图 4.13 报表管理-TFTP 传递

- 同步周期：按时（一小时同步一次）、日（每天同步一次）、周同步（每周同步一次）。
- 报表类型：选择需要同步的报表
- 导出：选择报表类型后，选择导出可以手动将对应的报表导出到本地。

5 系统配置

5.1 保存配置

【保存配置】模块用于对设备的相关设置进行保存，可按网络设备地址、全局防护参数、TCP/UDP 端口保护参数、主机及配置参数以及规则列表进行选择性保存，并可进行配置的导入和导出操作，页面如下图所示：

图 5.1 保存配置

- 保存配置方式：在该栏我们可以选择性保存某项配置。
  - 网络设备地址：指保存系统设备地址，设置外网管理地址后需要选择此项保存，以保留配置的管理地址重启后不会丢失。
  - 全局防护参数：指保存攻击防御中的全局参数，以保留原配置参数重启后不会丢失。
  - TCP/UDP 端口保护参数：指保存 TCP/UDP 端口保护设置，以保留原端口保护设置重启后不会丢失。
  - 主机及配置参数：指保存主机状态及主机设置参数，以保留原原主机配置重启后不会丢失。
  - 规则列表：指保存攻击防御的规则设置，以保留原设定规定规则重启后不会丢失。

如产品升级后功能区别较大，需要重新设置原参数，不可选择保存配置，以免影响新功能的正常使用。

- 浏览配置：点击该选项后将弹出对话框，选择配置文件后点击导入配置按钮即可实现导入。
- 保存配置：勾选保存配置方式复选框以及浏览到配置文件即可实现配置的保存以及上传操作。
- 下载配置：选择保存配置方式中的复选框，点击下载配置按钮，会导出相应的配置。
- 删除配置：点击该按钮后将删除所有系统配置，重启后即可恢复出厂配置。

5.2 系统设备

【系统设备】模块提供了一个对设备硬件相关的配置接口。页面如下图所示：

图 5.2 系统设备

- 系统设备列表：主要对设备系统的网卡接口的地址进行配置，输入项表示为设备的数据入口、输出项表示为设备的数据出口，不需要 IP 地址；而其它项均为设备的配置接口，用户可更改这些网卡的 IP 地址，方便访问。同时，还可将某些网卡接入外网，并配置外网 IP 地址，这样就无须控制机的中转；
  - 添加地址

    在“系统设备列表“底部，设备接口栏目填写，如图：

gbe3 添加管理地址 172.16.11.76

gbe3 删除管理地址 172.16.11.76

gbe3 设置管理地址网关 172.16.1.1

提示：

当设备系统版本为 IPv4 版本时，可以通过方法一或者方法二修改接口地址，当系统版本为 IPv6 版本时只能通过方法二修改接口地址。

- 域名服务器：写入域名服务器地址，该域名服务器对应的是“系统配置“中”控管属性“下邮件配置如图所示，用于解析 SMTP 服务器如图所示：

图 5.3 系统设备

- 默认：使得设备默认配置。另外，为了防止错误配置导致设备的永久损坏，设备重启后将恢复默认设置；
- 重启系统：按钮将重启设备，用于某些特殊情况（如设备异常）。

5.3 聚合管理

用于链路聚合，优化以前的链路聚合模式。

图 5.4 聚合管理

点击【新建】按钮，可选择聚合编号，0-7 最大 8 个。成员口只能是通道口。

图 5.5 聚合添加

添加成功后在设备管理页面可以看到对应的聚合口，点击聚合口编号可以超链接到聚合管理界面。

图 5.6 聚合展示

5.4 集群参数

【集群参数】模块用于设备集群系统的配置及启动，由于集群模式安装的复杂性，本页面由金盾抗拒绝服务系统技术人员使用。页面如下图所示：

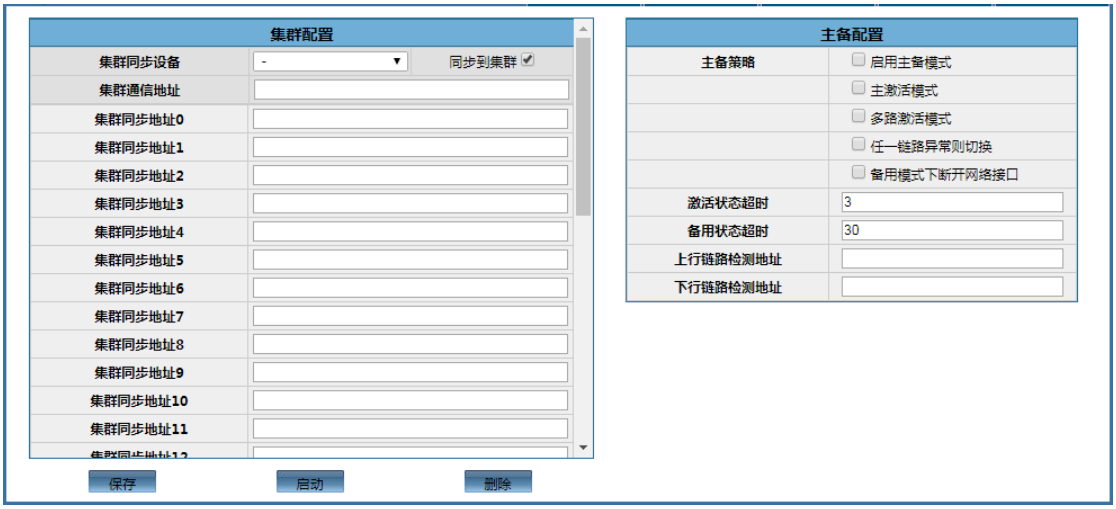


图 5.7 集群参数

- 集群配置：集群管理用于设置集群心跳地址及启动集群设置。
- 热备配置：用于配置双击热备功能。
  - 启动主备模式：开启主备的开关
  - 主激活模式：主备时需要设置为主设备的勾选
  - 多路激活模式：多组主备时勾选
  - 任一链路异常则切换：检测到通道口异常则进行主备切换

- 备用模式下断开网络接口：备设备自动端口通道
- 激活状态超时：主设备在设置时间内检测不到接口数据则切换为备设备
- 备用状态超时：备设备再设置时间内检测不到主设备发的状态包则切换为主设备

说明：

在配置主备时参数设置只会无需点击“保存”，直接点击“开启即可”。

5.5 控管属性

图 5.8 控管特性

- 统计与存储

  设置系统保存日志和记录的时间、条数以及磁盘进行自动清理的阈值。

- 邮件属性

  接收地址列表可设置多个，接收地址列表含有多个邮箱时用“;”号分割。

- 安全属性：
  - 密码最小长度

    可以设置用密码的最小长度 0 为不限制；

  - 密码过期时间

    设置用户密码多少天过期 0 为不过期；

  - 登陆空闲超时

    设置用户登陆后多长时间没有操作设备后需要重新登陆；

  - 密码复杂

设置用户密码的复杂度可以规定密码中含有多少种字符组合；

- 密码历史记录

针对用户多次修改密码，可以设置保存多个修改前的密码，0 指只保存修改后的密码；

- 登录失败限制和登录屏蔽时间

设置登陆失败 5 次和屏蔽地址 300 秒时，当用户登陆失败次数达到 5 次后，设备将屏蔽用户 IP，屏蔽时间为 300 秒。

◆ NFS 服务配置

- NFS 服务：用于开启或者关闭 NFS 功能
- 服务地址：NFS 服务器地址
- 服务协议：TCP 协议、UDP 协议
- 服务目录：NFS 服务器存储目录

◆ AAA

- AAA 认证配置

图 5.9 AAA 配置

◆ 认证选项

本地任何和外部认证，本地认证 DMS 自带认证方式，外部认证需要外部认证服务器

◆ 认证协议

radius 和 tacacs+

◆ 最大重传次数

认证失败时允许最大的重传次数

◆ 服务器设置

外部认证服务器配置

◆ 外部认证测试

外部认证时测试外部认证服务器连通性

5.6 路由协议

旁路模式特有，支持多种路由协议。在配置路由协议之前必须先开启相应的协议，否则在 CLI 配置之后不生效。在开启时必须保证已经退出 CLI 管理界面。

图 5.10 路由协议

5.7 用户组管理

【用户组管理】用来新建、删除、编辑用户组，设置某个用户组的管理权限。系统默认有四个用户组：monitor、operator、administrator、service。页面如下图所示：

图 5.11 用户组管理

- 编辑用户组：【用户组名】中填写需要修改的用户组名，点击【编辑】进入用户组编辑页面，对该用户组进行权限分配的更改，修改完成后点击【提交】完成修改。
- 新建用户组：点击【新建】进入用户组编辑页面，在【用户组名】中填写新建的用户组名，勾选给予新用户组的权限，然后【提交】。
- 删除用户组：【用户组名】中填写需要删除的用户组名，点击【删除】按钮。注意要删除的用户组不能包含用户在其中。

图 5.12 用户组编辑

5.8 用户管理

【用户管理】模块具有设置用户分级管理功能，方便网络监控及管理。页面如下图所示：

图 5.13 用户管理

- 网络观察员：仅可以查看当前系统状态，无权更改。
- 网络管理员：拥有网络观察员权限，并可变更参数设置。
- 系统管理员：拥有网络管理员权限，并可创建子帐户。
- 授权客户服务：用于远程服务的授权帐户。
- 修改/新建用户名：如需修改某个用户的密码，单机相应用户名后可以直接在用户设置一栏进行设置操作。新建某个用户同样也在用户设置一栏进行新建，方法为输入用户名密码以及授予登录方式和权限后提交即可。

5.9 时间设定

【时间设定】模块提供修改设备时间的功能，页面如下图所示：

图 5.14 时间管理

- 当前时间：指设备当前所显示的时间。
- 启动时间：指系统开机到当前时间一共的时长。
- 设置时间：以当前时间所显示的格式设置系统时间。
- 时区选择：点击选择时区

5.10 SNMP 系统

【SNMP 系统】模块页面，可创建、修改用于 SNMP 服务的系统信息、当前位置以及描述信息。页面如下图图所示：

图 5.15 SNMP 系统

- SNMP 服务：可以禁用以及启用 SNMP 服务。
- 联系信息：默认填写了我们中心金盾的官方网站。
- 物理地址：填写了中新金盾的详细地址。
- 系统描述：说明了当前设备的系统类型。

提示：

当对 SNMP 用户或 SNMP 视图页面修改后，需要在 SNMP 系统页面禁用/启用一次，使更改的配置生效。

5.11 SNMP Trap

【SNMP Trap】是触发某种条件后 SNMP 被管设备主动通知 SNMP 管理器，而不是等待 SNMP 管理器的再次轮询。页面如下图所示：

图 5.16 SNMP Trap 配置

- SNMP Trap 选项：勾选 snmp trap 触发条件。
- 接收主机地址：接收 SNMP 信息的服务器端地址。
- 用户：选择在 SNMP 用户中创建的用户。

5.12 SNMP 用户

【SNMP 用户】模块页面，可创建、修改用于 SNMP 协议的用户名及相应的验证模式。页面如下图所示：

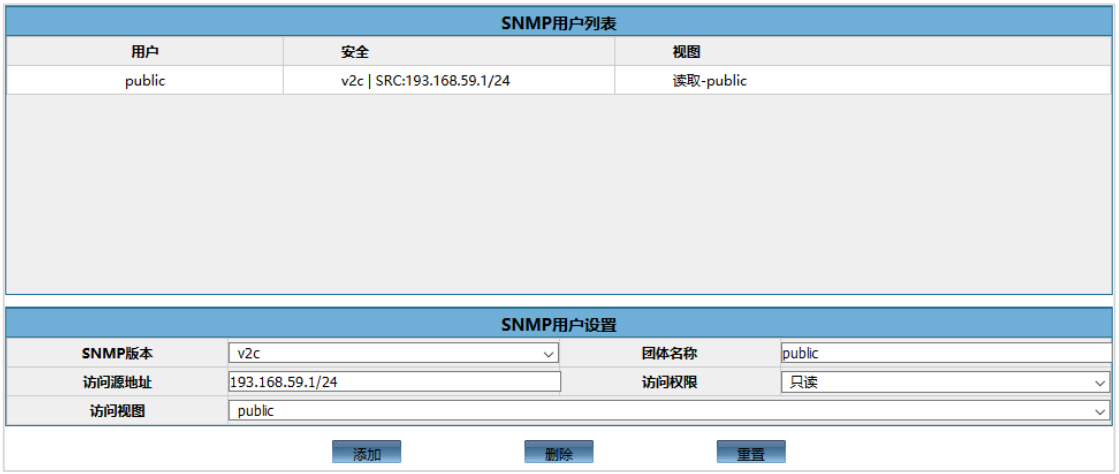


图 5.17 SNMP 用户

1. SNMP 版本

指定该用户适用的 SNMP 查询版本。v1 不需要验证，v2c 使用团体名称作为验证码，v3 则使用强加密方式进行认证。推荐 SNMP v3。

当版本号为 v1 或 v2c 时，如下项可用：

a. 团体名称

用于 SNMP 协议的团体名称。

- 访问源地址：SNMP v1/v2c 模式下，执行 SNMP 操作的源地址范围。可指定单个 IP，或某个网段。如 192.168.1.10，192.168.1.1/24 等。
- 访问权限：SNMP v1/v2c 模式下，对某个视图的访问权限。

当版本号为 v3 时，如下项可用：

- 用户名称：用于 SNMP v3 的用户名。
- 认证算法/认证密码：用于 SNMP v3 的认证方式。密码最小长度为 8。
- 加密算法/加密密码：用于 SNMP v3 的加密方式。密码最小长度为 8。
- 视图：该用户/团体可访问的视图子树。由 SNMP 视图页面创建。

当访问视图为“全视图”时，点击“删除”，则同时删除该用户/团体。否则只将该视图从该用户/团体中删除。

5.13 SNMP 视图

【SNMP 视图】模块页面，可创建、修改用于 SNMP 协议的视图。页面如下图所示：

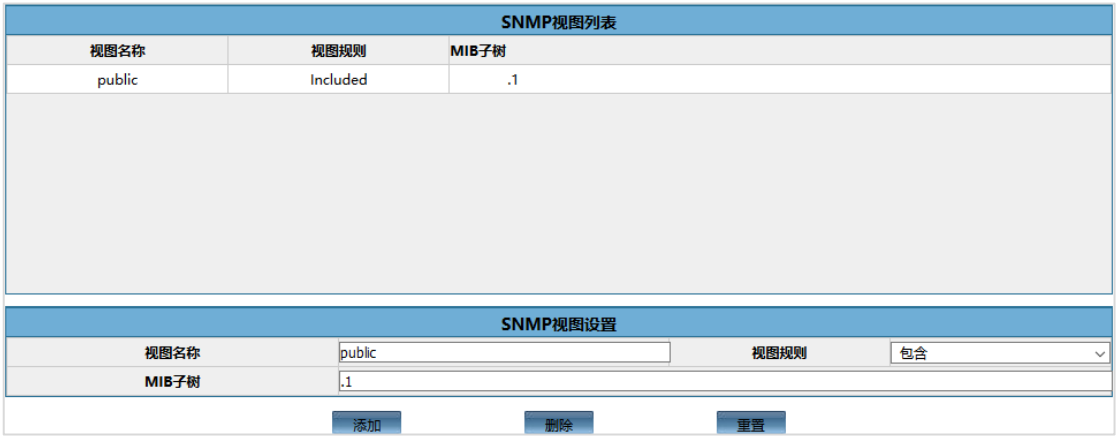


图 5.18 SNMP 视图

1. 视图名称

视图的字符串形式描述。

2. 视图模式

“包含”或“排除”，用于向该视图中包含，或从某个视图中排除某个 MIB 子树。

3. MIB 子树

SNMP 协议中定义的管理信息块。可以是字符串形式，或数字形式。如：1.3.6.1.2.1.25.1.1 或 iso.org.dod.internet.mgmt.mib-2.host.hrSystem.hrSystemUptime。

6 服务与支持

6.1 关于我们

展示我司基本信息

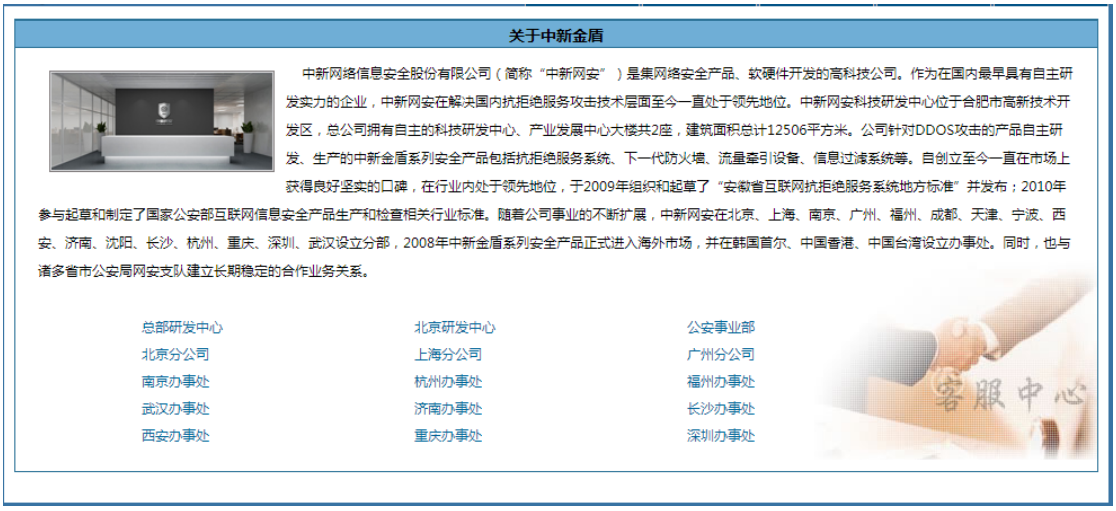


图 6.1 关于我们

6.2 报文捕捉

【报文捕捉】用来抓取经过设备接口的数据报文，分析数据包走向、攻击特征等。

图 6.2 报文捕捉

- 捕捉 MAC 地址：针对特定的 MAC 地址进行捕捉数据包，可以是源 MAC 或是目的 MAC。
- 捕捉 IP 地址：针对特定的 IP 地址进行捕捉数据包，可以是源 ip 或是目的 ip，支持连续多个 IP 抓包如 192.168.2.100-192.168.2.200。
- 捕捉属性：可以选择源地址或是目的地址进行捕捉数据包。
- 协议类型：选择抓取某个协议的报文，比如选择 tcp 类型的。
- 设备接口：针对设备哪个接口进行报文捕捉。
- 捕捉采样比：设置比例，多少个数据包抓取一个。
- 捕捉报文数目：用于指定捕捉数据包的数目，格式为正整数，范围为"1-2147483647"。
- 远程 TFTP 文件：捕捉的数据包发送到指定的 TFTP 服务器，格式为：TFTP 服务器地址:数据包名称
- 捕捉数据大小：显示抓取的数据包大小。24 Bytes 表示未抓取到数据包。