爱快云防火墙解决方案

公司名称:全讯汇聚网络科技（北京）有限公司

公司地址：北京市丰台区南四环西路 186 号汉威国际广场四区 6 号楼 8M 层 11 室

邮政编码：100000

公司网址：www.ikuai8.com

联系电话：400-877-3227

爱快云防火墙使用说明

1. 首页

2. 监控

    系统

    威胁

        概览

        威胁详情

    应用

        概览

        应用详情

    URL

        概览

        URL 详情

    会话

        会话统计

        标准会话

        流量统计

3. 策略

    防火墙

        策略

        策略配置

策略预编译
安全防护
防护策略
攻击防护
入侵防护
Web 防护
威胁情报
病毒防护
IP 黑名单
域名黑名单
白名单
应用控制
应用控制策略
Web 控制策略
关键字
4. 对象
地址对象
地址节点
地址组
域名地址
备份/恢复
服务对象

预定义服务
自定义服务
服务组
应用对象
预定义应用
自定义应用
应用组
URL 分类
预定义 URL 分类
自定义 URL 分类
URL 组
URL 分类查询
备份/恢复
时间对象
绝对时间
周期时间
5. 日志
审计日志
应用控制
Web 控制
安全日志
防火墙策略

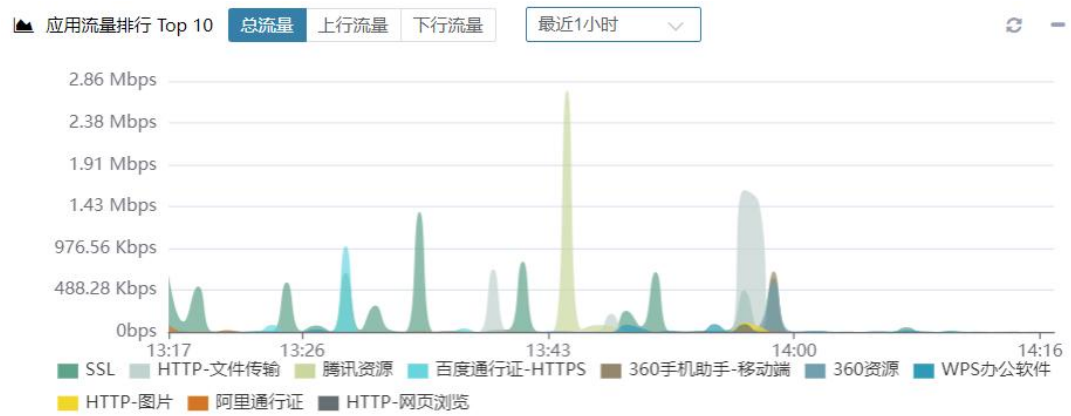
防 Flood 攻击
防扫描
入侵防护
WEB 防护
威胁情报
病毒防护
IP 黑名单
域名黑名单
白名单
流日志
流日志
日志管理
日志过滤
流日志配置
6. 系统
配置
DNS
备份/恢复
设备重启
版本管理
特征库版本
许可管理

首页

页面显示设备当前整体的运行状态，包括应用流量排行 Top10 趋势、设备流量、威胁统计、URL 访问 Top10、高级别日志、连接数、系统信息。

在每个小面板的右上角有 和 两个图标，分别能刷新和展开/折叠当前面板。

应用流量排行 Top10



统计指定时间段内流量排行前 10 的用户（IP）流量速率的变化趋势。

统计内容默认的时间范围是最近 1 小时，按总流量排序；

排序内容可选“总流量/上行流量/下行流量”做为排序标准；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

威胁统计

统计指定时间段内威胁级别和威胁类型的变化趋势。

统计内容默认的时间范围是最近 1 小时；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

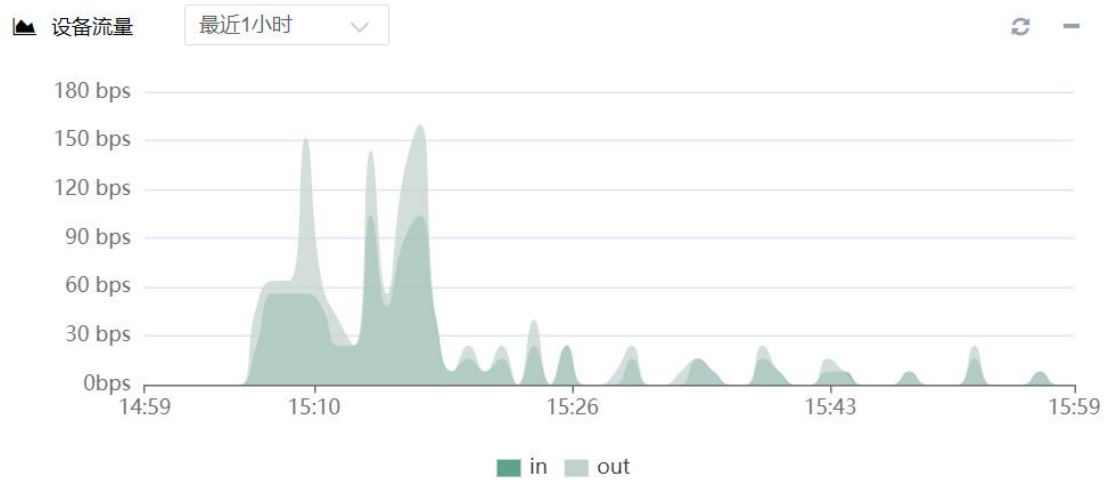
URL 访问 Top10

统计指定时间段内 URL 和 URL 分类访问量的变化趋势。

统计内容默认的时间范围是最近 1 小时；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

设备流量



统计指定时间段内设备整机 in/out 流量速率的变化趋势。

统计内容默认的时间范围是最近 1 小时；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

连接数

统计指定时间段内“并发连接”和“新建连接”的均值变化趋势。

统计内容默认的时间范围是最近 1 小时；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

高级别日志

高级别日志 详情

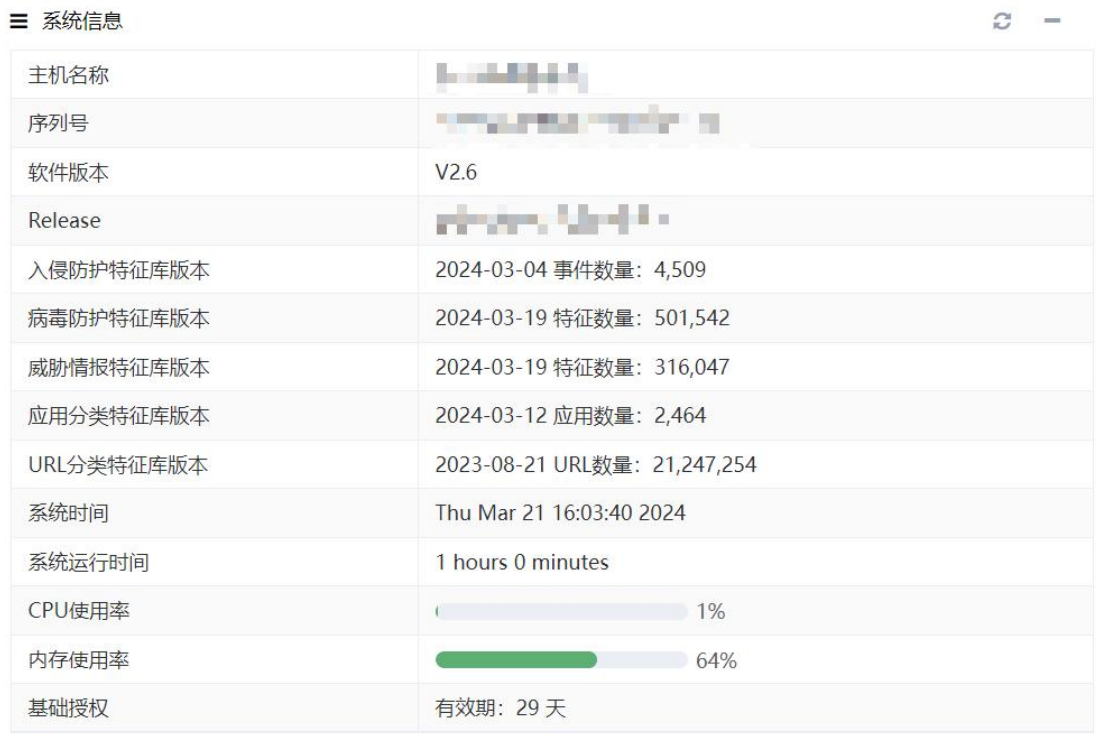
时间	类型	级别	信息
2024-03-27 14:29:12	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.112.233.1 Protocol=TCP SrcPort=54254...
2024-03-27 14:29:12	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.112.233.1 Protocol=TCP SrcPort=40788...
2024-03-27 14:29:12	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.112.233.1 Protocol=TCP SrcPort=40776...
2024-03-27 14:29:12	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.112.233.1 Protocol=TCP SrcPort=40768...
2024-03-27 14:28:07	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.112.233.1 Protocol=TCP SrcPort=41406...
2024-03-27 14:28:07	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.112.233.1 Protocol=TCP SrcPort=41396...
2024-03-27 14:28:07	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.112.233.1 Protocol=TCP SrcPort=41380...
2024-03-27 14:28:07	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.112.233.1 Protocol=TCP SrcPort=55404...
2024-03-27 14:28:01	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.123.207.181 Protocol=TCP SrcPort=551...
2024-03-27 14:27:57	威胁情报	警示	SrcIP=192.168.67.13 DstIP=118.123.207.181 Protocol=TCP SrcPort=429...

查看最新高级别日志数据。

首页的高级别日志列表中，包含了所有类型日志里的高级别记录；

点击“详情”连接，可跳转到日志菜单下，即可浏览各类型日志的详细内容。

系统信息



系统信息

主机名称	
序列号	
软件版本	V2.6
Release	
入侵防护特征库版本	2024-03-04 事件数量：4,509
病毒防护特征库版本	2024-03-19 特征数量：501,542
威胁情报特征库版本	2024-03-19 特征数量：316,047
应用分类特征库版本	2024-03-12 应用数量：2,464
URL分类特征库版本	2023-08-21 URL数量：21,247,254
系统时间	Thu Mar 21 16:03:40 2024
系统运行时间	1 hours 0 minutes
CPU使用率	1%
内存使用率	64%
基础授权	有效期：29 天

查看设备基本信息。

主机名称：可以由管理员用户配置，可以通过主机名称区分设备。

序列号：当前设备的唯一标识。

软件版本：当前设备运行的系统软件的版本号。

Release：售后服务时使用的编码。

入侵防护特征库版本：最新入侵防护特征库更新时间和特征数量。

病毒防护特征库版本：最新病毒防护特征库更新时间和特征数量。

应用分类特征库版本：最新应用分类特征库更新时间和特征数量。

URL 分类特征库版本：最新 URL 分类特征库更新时间和特征数量。

系统时间：当前系统时间。

系统运行时间：系统从上次启动到现在已经运行的时间。

CPU 使用率：当前设备 CPU 使用率。

内存使用率：当前设备内存使用率。

基础授权：设备基础授权时间。

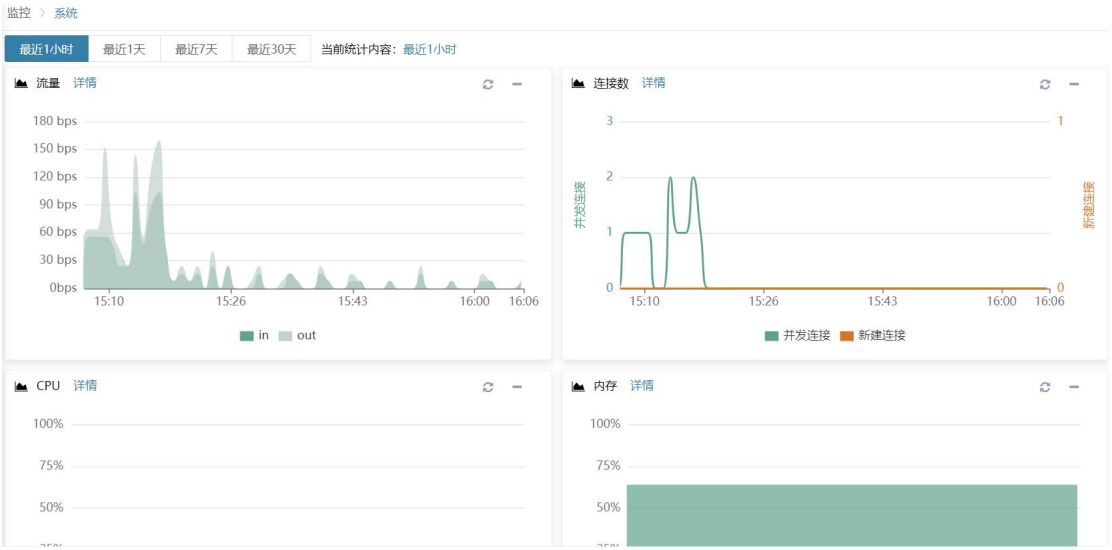
监控

系统

系统监控概述

通过系统监控功能，可监控下一代安全防护平台设备的整机流量速率、并发连接与新建连接、CPU 与内存利用率等信息。并可以调整最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期。

点击**监控>系统**，进入系统监控页面，可以查看下一代安全防护平台设备，最近 1 小时、最近 1 天、最近 7 天、最近 30 天的流量、连接数、CPU、内存利用率信息。



点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

威胁

概览

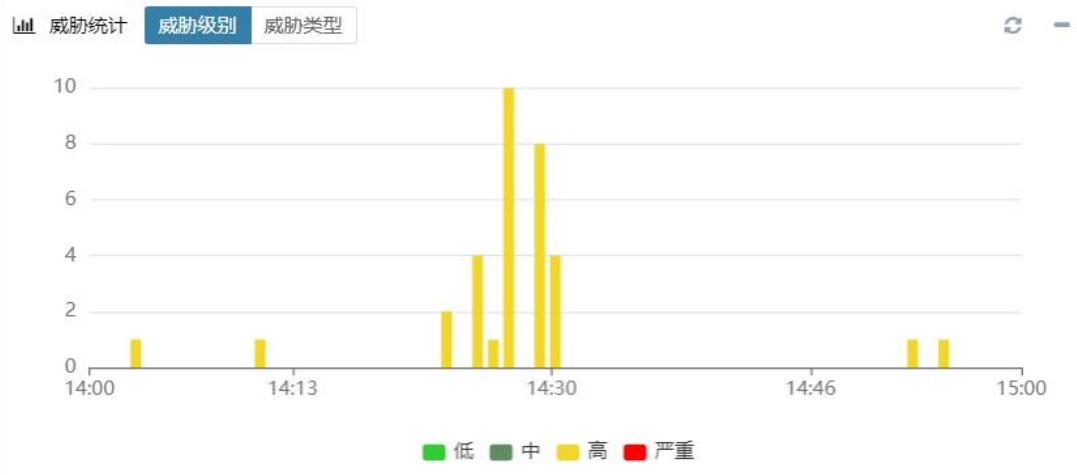
威胁监控概述

通过威胁监控功能，可监控用户受到威胁的信息。根据最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期，监控周期内用户受到威胁的信息，并对攻击信息的级别、类型、事件以及地理分布做了全方位的分析检测，以图表和分布图的方式更直观让用户对威胁源头有了了解。

威胁概览

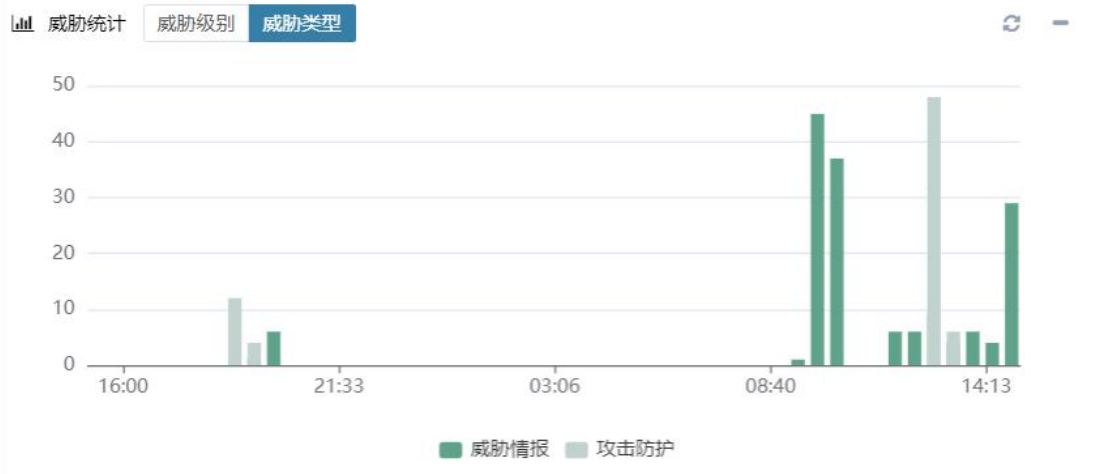
点击**监控>威胁>概览**，进入用户概览页面，可以查看最近 1 小时、最近 1 天、最近 7 天、最近 30 天的威胁统计、威胁地图、威胁主机 Top10 和威胁 Top10 的统计信息，其中包含威胁级别、类型、事件、以及中国地图、世界地图的威胁分布。

威胁级别统计：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

威胁类型统计：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击**威胁级别**、**威胁类型**，切换统计内容。

威胁主机 Top10 表格展示方式：

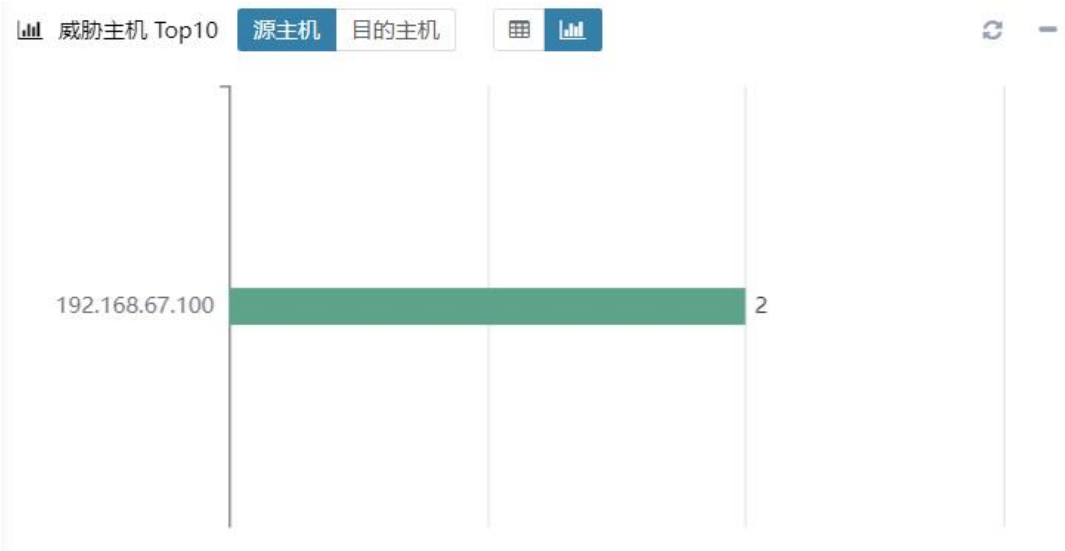
IP	国家/城市	攻击数
[redacted]	保留	83
[redacted]	保留	53
[redacted]	保留	50
[redacted]	保留	17
[redacted]	保留	8
[redacted]	保留	8
[redacted]	保留	3
[redacted]	保留	2

点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击源主机、目的主机，切换攻击主机和被攻击主机的统计。

表/图按钮可切换统计展示方式。

威胁主机 Top10 柱形图展示方式：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击源主机、目的主机，切换攻击主机和被攻击主机的统计。

表/图按钮可切换统计展示方式。

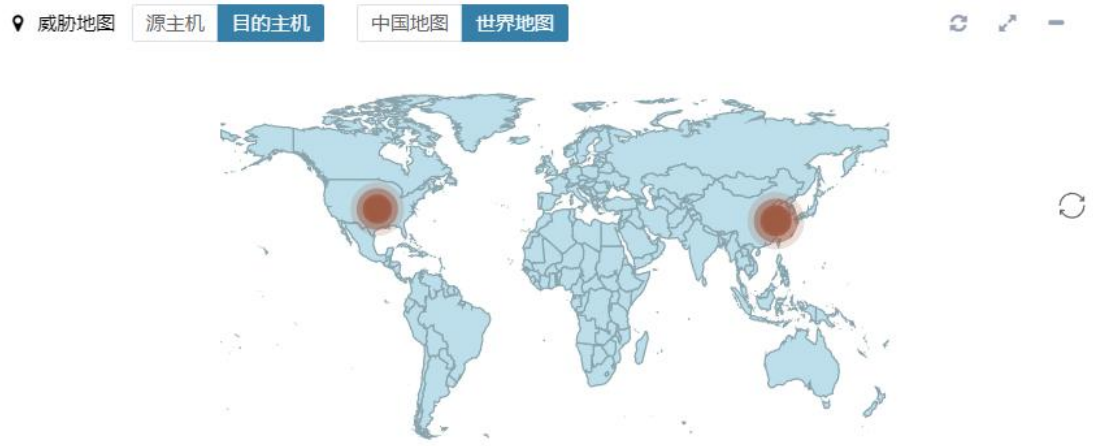
威胁地图目的主机分布：

点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击源主机、目的主机，切换攻击主机和被攻击主机的统计。

中国地图、世界地图页签切换可从不同的地理范围查看攻击情况。

世界地图威胁目的主机分布：

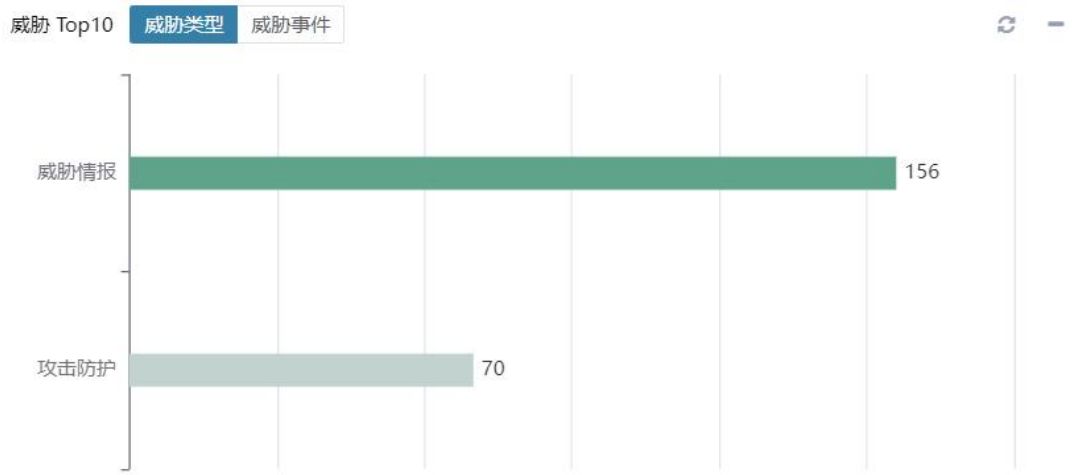


点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击源主机、目的主机，切换攻击主机和被攻击主机的统计。

中国地图、世界地图页签切换可从不同的地理范围查看攻击情况。

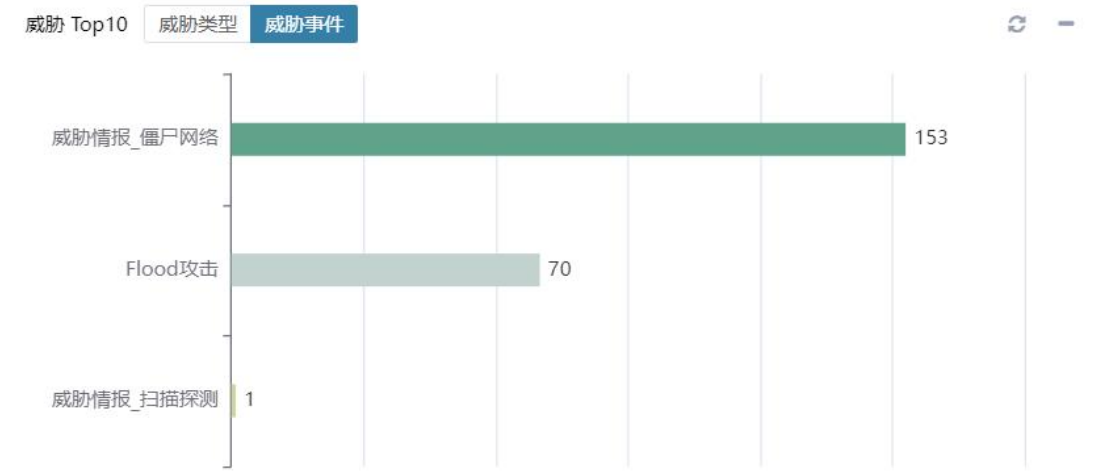
威胁类型 Top10：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

威胁类型、威胁事件页签切换可切换统计内容。

威胁事件 Top10：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

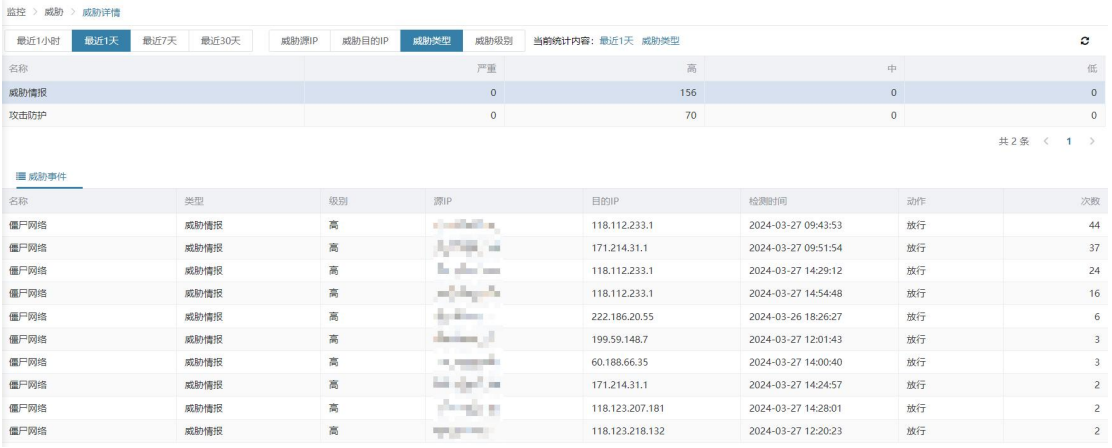
威胁类型、威胁事件页签切换可切换统计内容。

威胁详情

点击**监控>威胁>威胁详情**，进入**威胁**详情页面，可以查看威胁详细信息。

威胁详情统计：

上图是威胁 IP 统计，可以看到威胁 IP 所在地理位置，和威胁级别分布情况。



上图是威胁类型统计，可以看到威胁类型的威胁级别分布情况。

上图是威胁级别统计，可分别查看各威胁级别的威胁总数。

除此之外，点击以上各统计项，在下方都可以查看到符合该统计具体的威胁事件。

威胁事件详情：

上述统计中可查看到，威胁事件所属类型，威胁级别，源 IP，目的 IP 以及检测到威胁的时间，还有这次检测同时检测到的同类事件的次数。

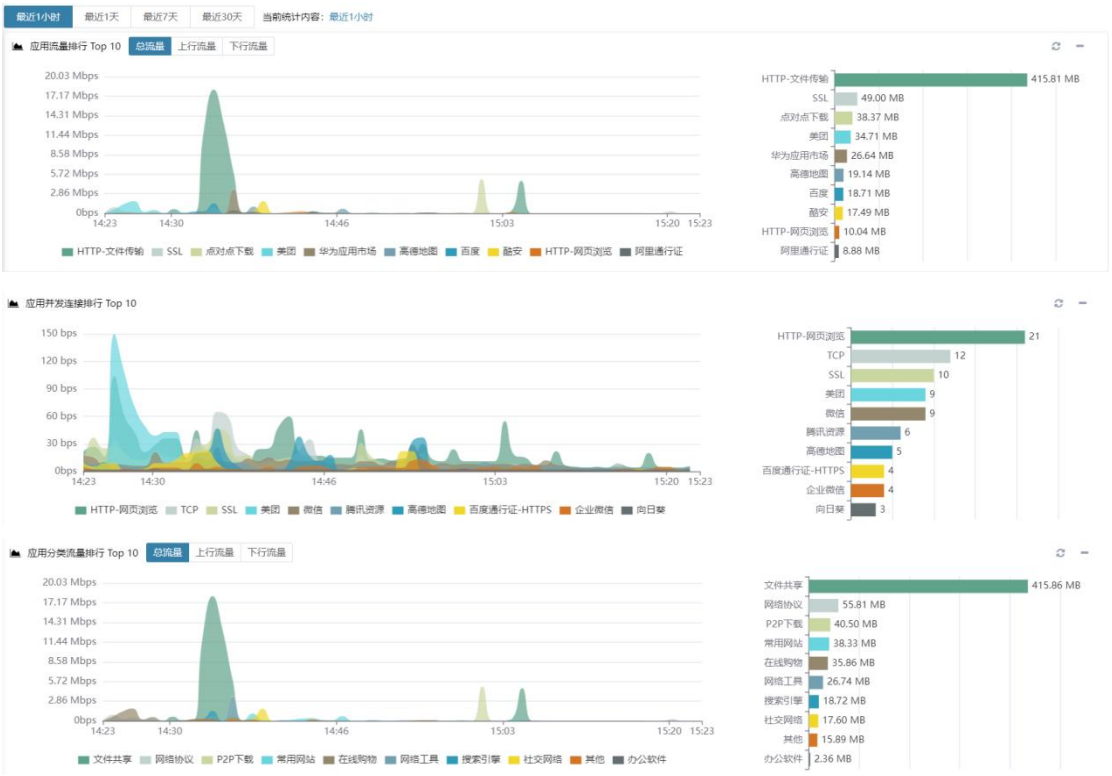
应用

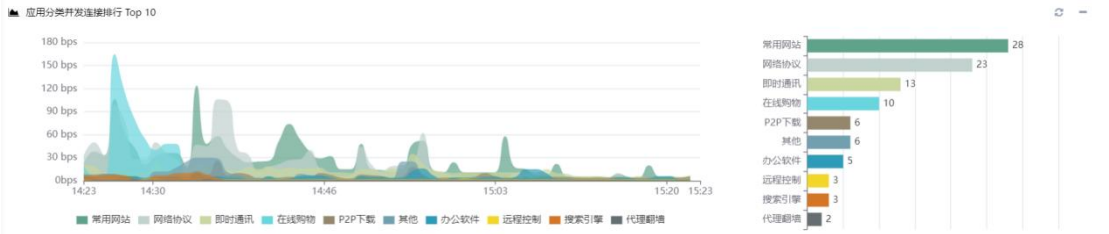
概览

通过应用监控功能，可监控统计通过下一代安全防护平台设备应用的流量信息。根据最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期，监控周期内应用流量排行 Top10 、应用并发连接排行 Top10 ，并可以分别查看总流量、上行流量、下行流量的 Top10 应用，以及应用分类并发连接排行 Top10 信息。

应用监控概览

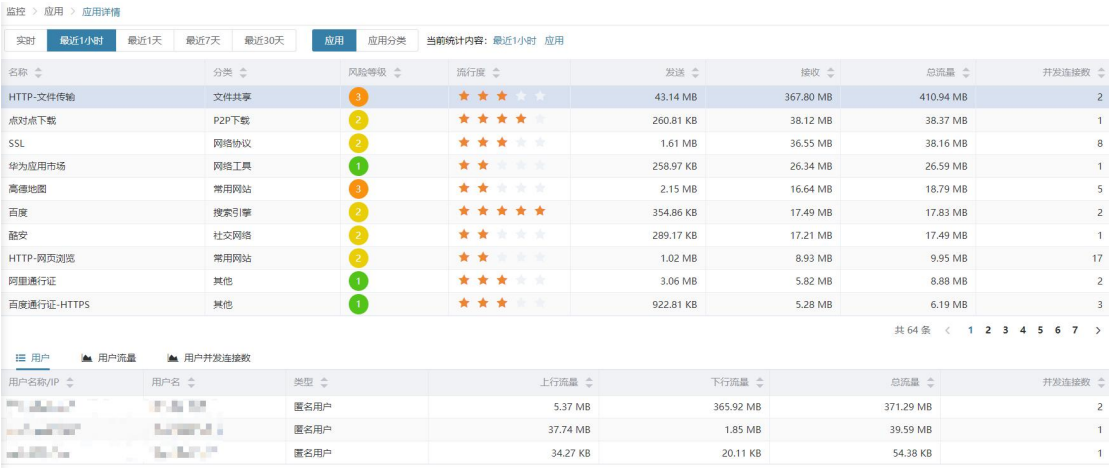
进入应用监控概览页面，该页面可分别查看应用和应用分类的流量排行和并发连接数排行，可查看最近 1 小时、最近 1 天、最近 7 天、最近 30 天的统计结果。曲线图表示监控周期内的应用的总流量、发送流量、接收流量速率，柱状图表示应用总流量、发送流量、接收流量排行。





应用详情

点击**监控>应用>应用详情**，进入应用统计详情页面，该页面可查看应用和应用分类最近 1 小时、最近 1 天、最近 7 天、最近 30 天的统计结果以及实时的流量和并发连接数情况。



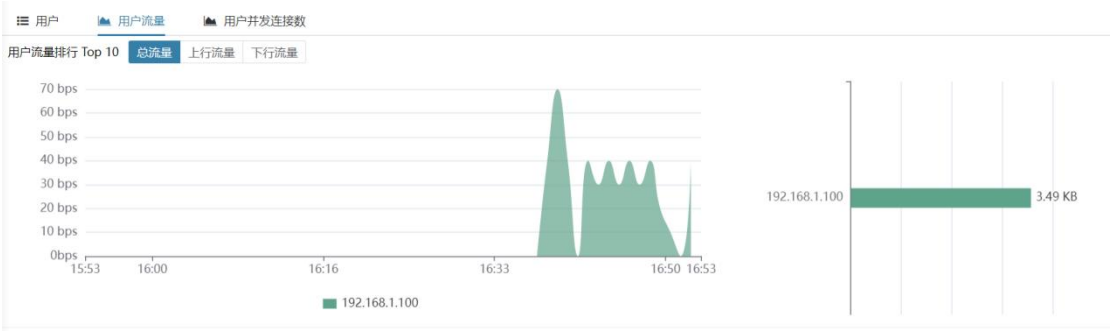
选择类型：包括应用和应用分类。

选择统计时间间隔，其中包括最近 1 小时、最近 1 天、最近 7 天、最近 30 天。

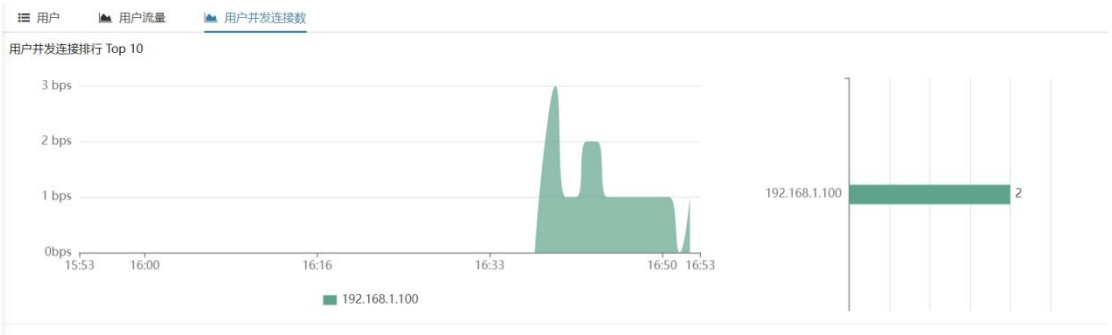
选择具体应用进行查询：在应用或者应用分类的流量排行列表中，点击某应用，在下方将会显示该应用的流量在所有用户 IP 上的分布情况。

用户列表：

用户流量曲线图和柱形图：



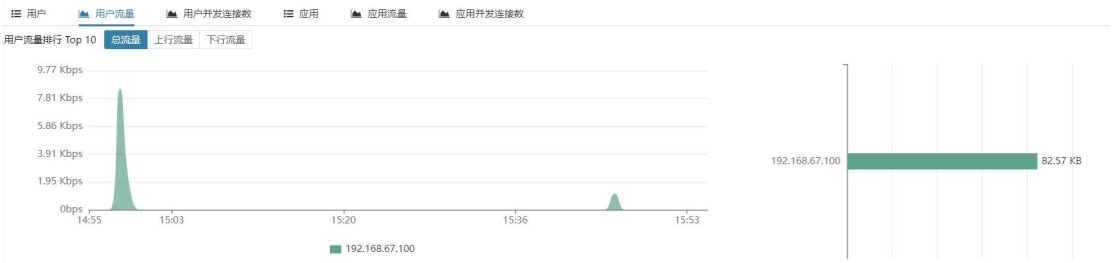
用户并发连接数曲线图和柱形图：



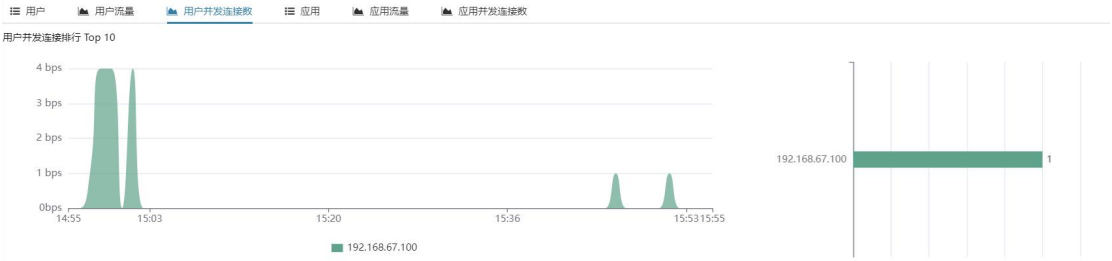
选择具体应用分类进行查询：在应用分类的流量排行列表中，点击某应用分类，在下方将会显示该应用分类的流量和并发连接数分别在所有用户 IP 和该应用分类下具体应用上的分布情况。

用户流量列表：

用户流量曲线图和柱形图：

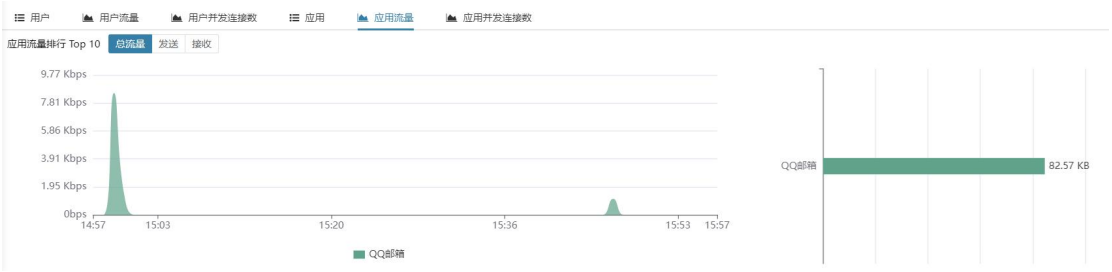


用户并发连接数曲线图和柱形图：



应用流量列表：

应用流量曲线图和柱形图：



应用并发连接数曲线图和柱形图：

查看应用流量实时信息。在应用详情中选择“实时”，将进入应用流量实时显示页面。该页面显示的是应用或者应用分类的实时流量和并发连接数。

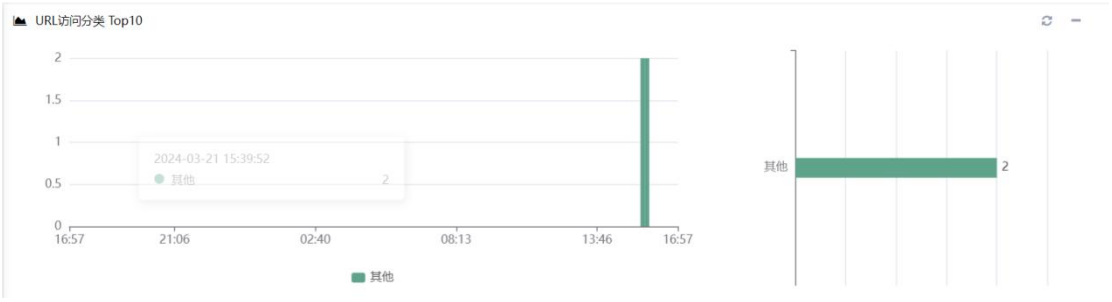
URL

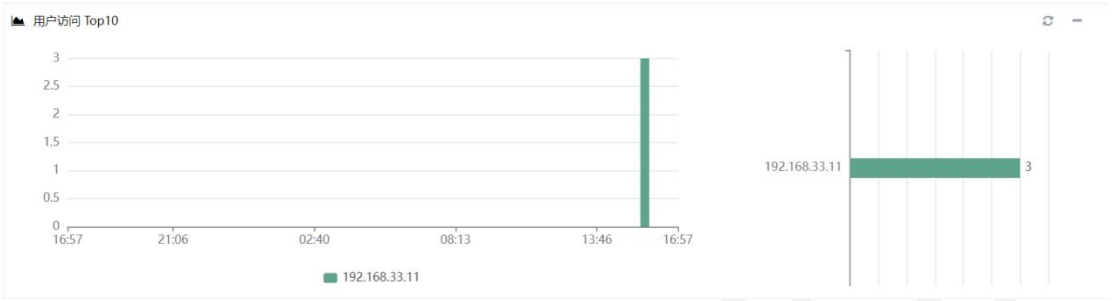
概览

通过 URL 监控功能，可监控统计通过下一代安全防护平台设备访问 URL 的信息。根据最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期，监控周期内总访问量 top10 的 URL 和 URL 分类，并可以分别监控 URL、URL 分类、用户访问量 top100 信息。

URL 监控概览

进入 URL 监控概览页面，该页面可分别查看 URL、URL 分类和用户的 URL 访问排行，可查看最近 1 小时、最近 1 天、最近 7 天、最近 30 天的统计结果。直方图表示监控周期内的 URL 的访问情况，柱状图表示 URL 访问量排行。





URL 详情

点击**监控>URL>URL 详情**，进入 URL 统计详情页面，该页面可查看 URL、URL 分类和用户的 URL 访问最近 1 小时、最近 1 天、最近 7 天、最近 30 天的统计结果。

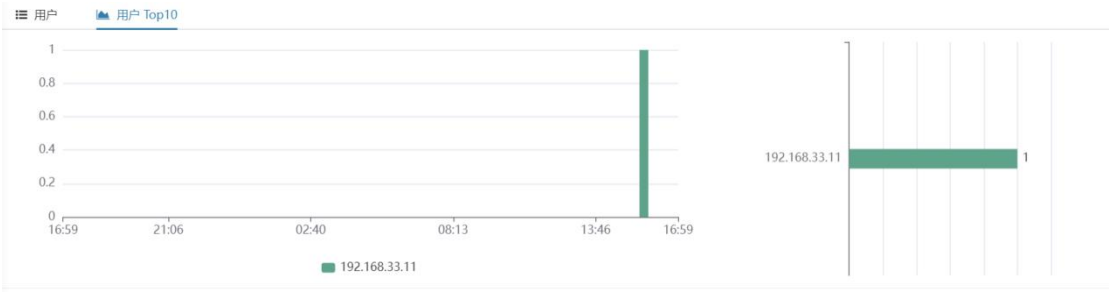
选择类型：包括 URL、URL 分类和用户。

选择统计时间间隔，其中包括最近 1 小时、最近 1 天、最近 7 天、最近 30 天。

选择具体 URL 进行查询：在 URL 的访问量排行列表中，点击某 URL，在下方将会显示该 URL 的访问量在所有用户 IP 上的分布情况。

用户访问量列表：

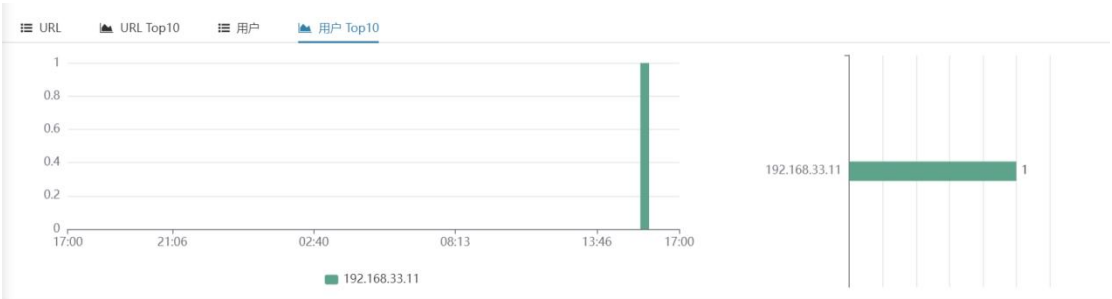
用户访问量直方图和柱形图：



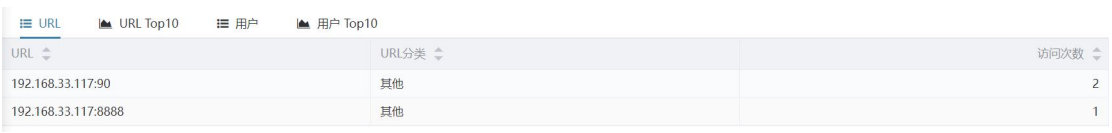
选择具体 URL 分类进行查询：在 URL 分类的访问量排行列表中，点击某 URL 分类，在下方将会显示该 URL 分类的访问量分别在所有用户 IP 和该 URL 分类下具体 URL 上的分布情况。

用户访问量列表：

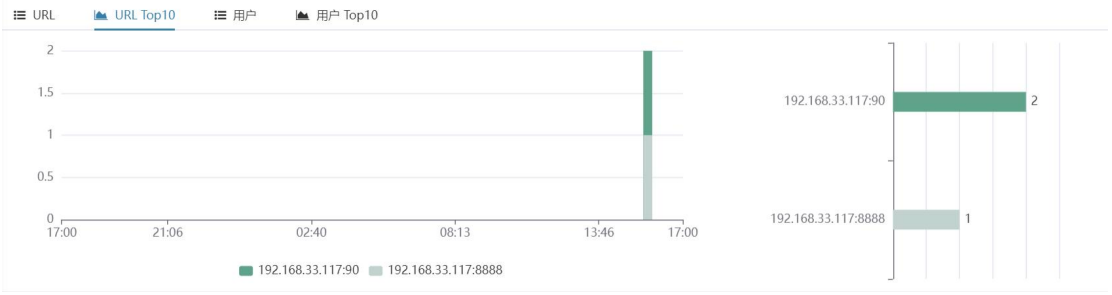
用户访问量直方图和柱形图：



URL 访问量列表：

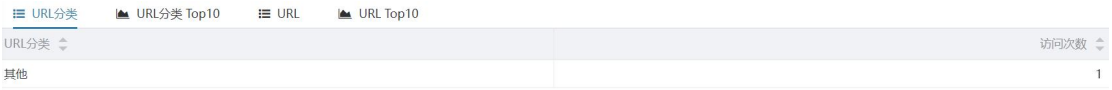


URL 访问量直方图和柱形图：

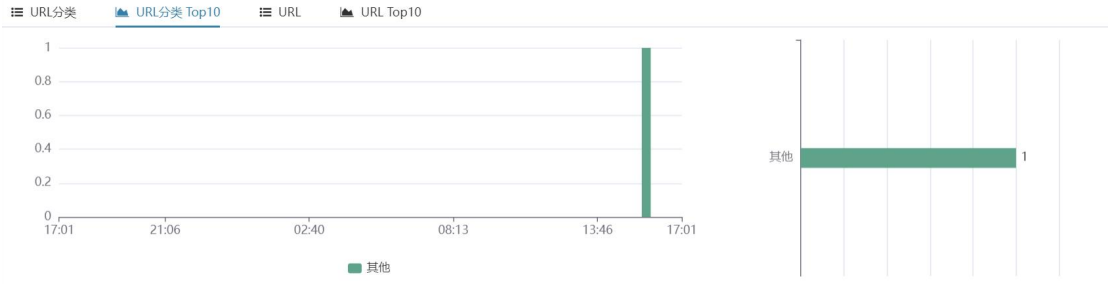


选择具体用户进行查询：在用户的访问量排行列表中，点击某用户，在下方将会显示该用户的访问量分别在 URL 和 URL 分类上的分布情况。

URL 分类访问量列表：

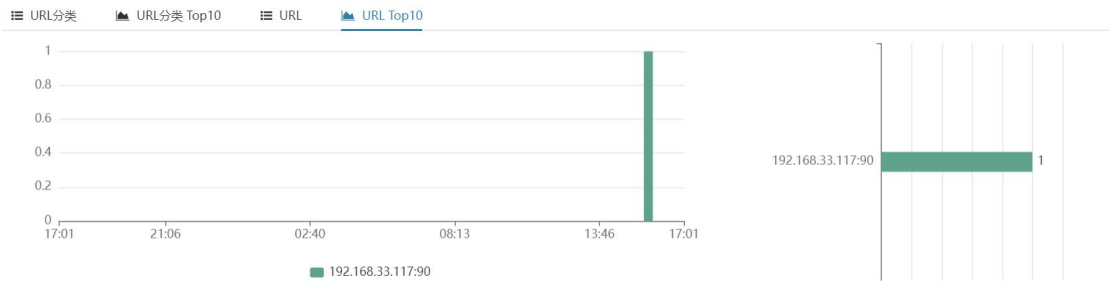


URL 分类访问量直方图和柱形图：



URL 访问量列表：

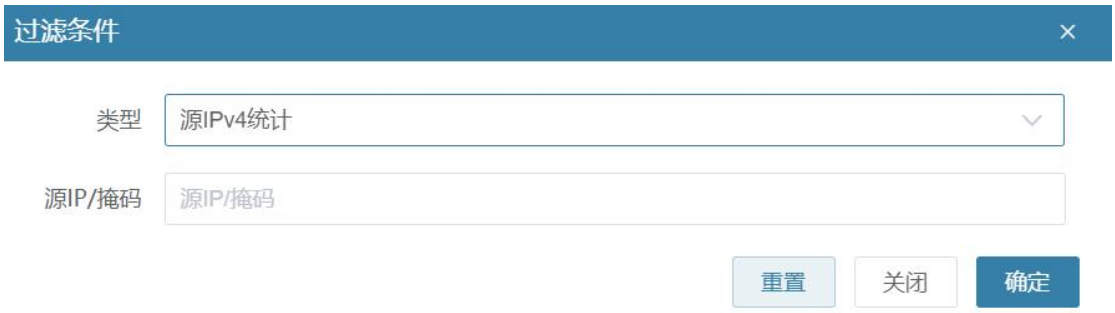
URL 访问量直方图和柱形图：



会话

会话统计

点击**监控>会话>会话统计**，进入会话统计页面，该页面根据下拉菜单中的选项统计系统当前连接数，可根据**源 IPv4 统计、源 IPv6 统计、目的 IPv4 统计、目的 IPv6 统计、目的端口统计**，还可指定详细条件，统计出的连接数按数量降序排列。

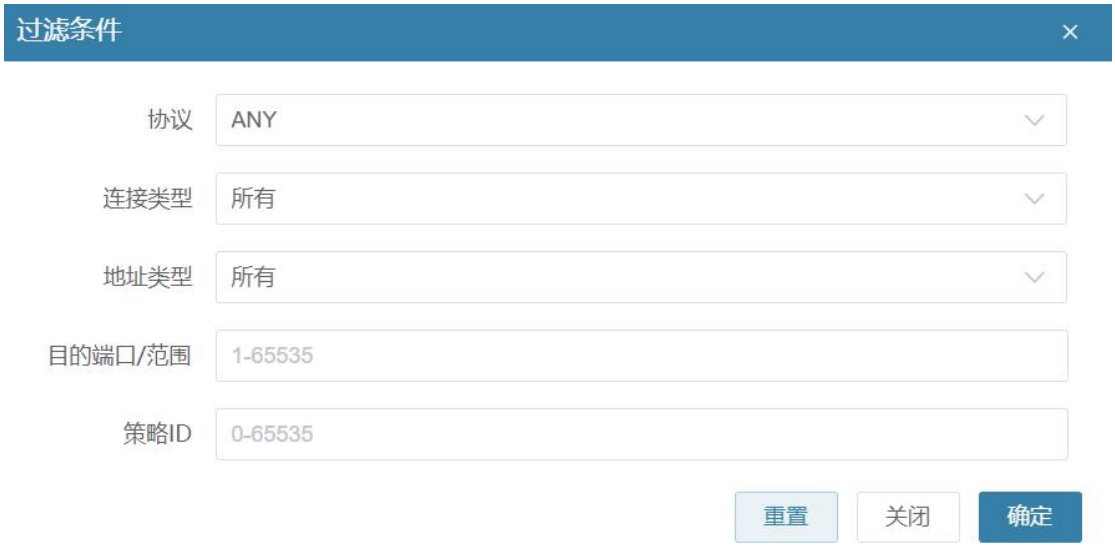


在类型下拉菜单中选择排序条件：**源 IPv4 统计、源 IPv6 统计、目的 IPv4 统计、目的 IPv6 统计、目的端口统计**，默认为按源 IPv4 统计。

在输入框中填写详细的**端口**或 **IP** 匹配条件，可输入 IP 地址/范围/掩码或端口号/范围，如果不输入，默认为全部统计。

标准会话

进入**标准会话**页面，该页面根据输入的协议、连接类型、地址类型、目的端口/范围等条件进行组合查询，显示匹配条件的连接。



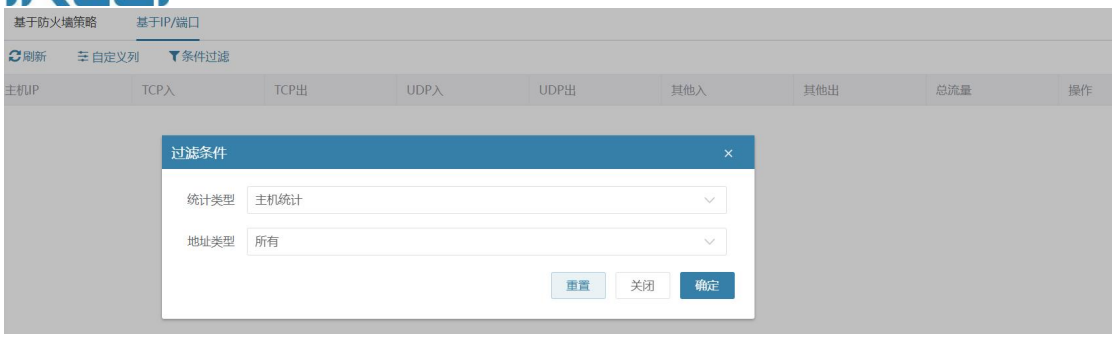
在下拉菜单中选择想要监控连接的类型和协议，输入源 IP，目的 IP，业务端口等条件，默认为所有。

流量统计

基于 IP/端口流量统计查询

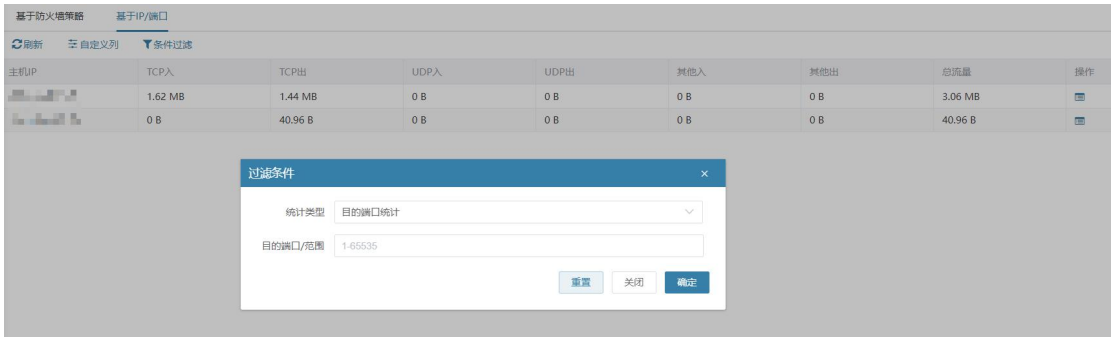
通过 IP/端口，检索查看流量统计。显示结果为基于源 IP 的流量大小排名。

进入**监控>会话>流量统计**，可看到如下界面。输入检索条件，查询流量统计结果。



统计类型：包括主机统计和目的端口统计

地址类型：**IPv4/IPv6** 地址



目的端口或范围：统计的目的端口或者端口范围，如 100-2410

列表显示关键字释义：

主机 IP：统计的主机地址

TCP 入：TCP 协议流量，反向流量

TCP 出：TCP 协议流量，正向流量

UDP 入：UDP 协议流量，反向流量

UDP 出：UDP 协议流量，正向流量

其他入：其他协议流量，反向流量

其他出：其他协议流量，正向流量

总流量：所有协议双方向流量总和

策略

防火墙

策略

配置策略组，对防火墙策略进行分组管理，在添加防火墙策略时可以设置策略所属的组，内置的策略组为“default”，可以添加新的策略组。

配置步骤：

进入**策略>防火墙>策略**，选择 IPV4 或 IPV6，点击**新建策略组**， 如下图：

参数说明：

名称：策略组的名称，名称不能重复。

配置完毕后，点击**确定**。

启用策略组

策略组的启用，对应的策略组下所有策略的启用。

配置步骤：

进入**策略>防火墙>策略**，如下图：

勾选**启用**，可以启用一个策略组下的所有策略，取消勾选，策略组下所有策略都将不启用。

删除策略组

配置步骤：

进入**策略>防火墙>策略**，如下图：

点击 选择删除方式，删除策略组。

选项说明：

同步删除组内策略：策略组和组内所有策略都删除。

组内策略移到默认组：策略组被删除，组内策略不被删除，移动到默认组。

移动策略组

可以通过移动策略组的顺序，改变策略的匹配顺序，default 策略组不能被移动。

配置步骤：

进入**策略>防火墙>策略**，如下图：

点击 移动策略组。

参数说明：

名称 ：需要被移动的策略组。

移动到：参考的策略组。

之前：移动策略组到参考策略组之前。

之后：移动策略组到参考策略组之后。

配置完毕后，点击**确定**。

插入策略组

配置步骤：

进入**策略>防火墙>策略**，如下图：

点击 插入新的策略组，新插入的策略组将放置于被插入策略组之前。

配置完毕后，点击**确定。**

重命名策略组

配置步骤：

进入**策略>防火墙>策略**，如下图：

点击 将策略组重新命名。

配置完毕后，点击**提交。**

策略组内策略迁移

配置步骤：

进入**策略>防火墙>策略**，如下图：

点击 将策略组内所有的策略移动到另一个策略组内。

参数说明：

名称：将被移动策略的策略组名称。

策略组：策略将移动进入的策略组的名称。

配置完毕后，点击**确定。**

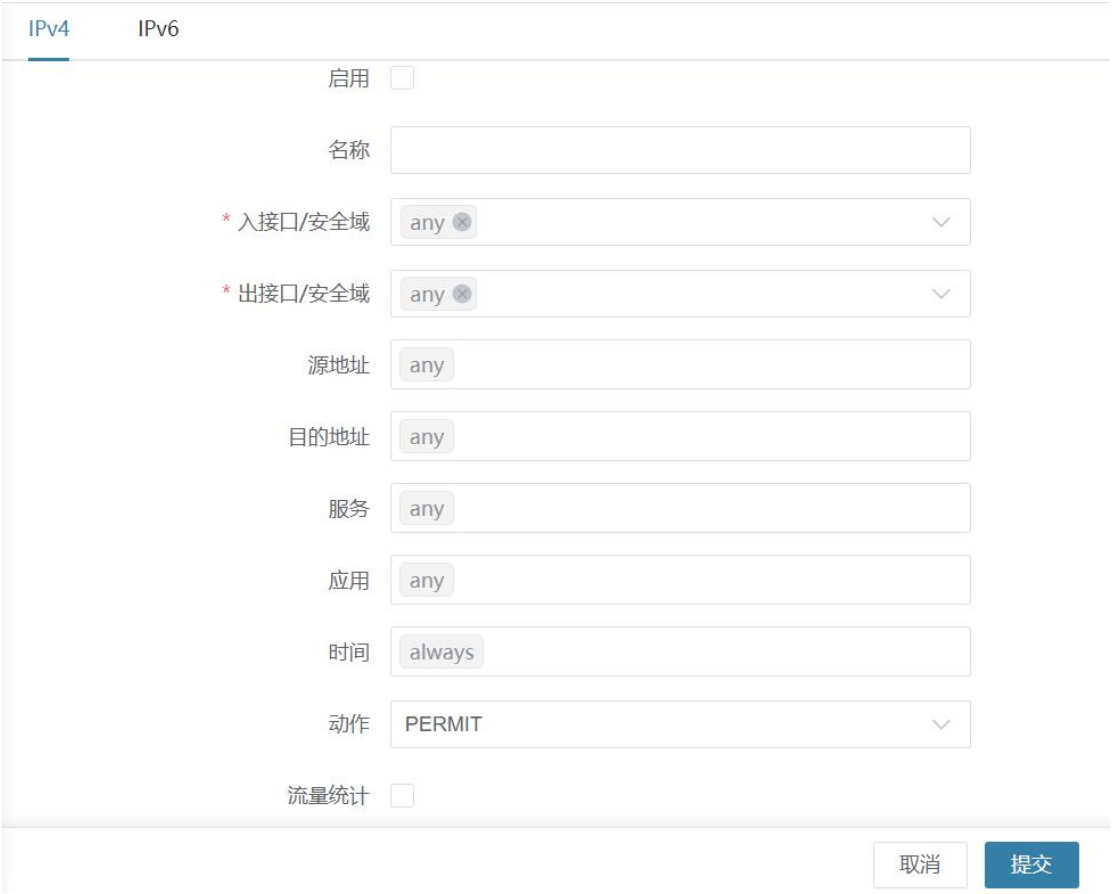
配置防火墙**策略**

配置策略的基本要素

防火墙策略的基本要素是匹配条件和动作。匹配条件包括数据流的方向、源地址、目的地址、服务、用户、应用和策略生效的时间范围。其中，数据流的方向通过指定入接口、出接口、源地址、目的地址来确定，服务、用户、应用和时间范围都可以直接引用已定义的对象。策略的动作有 PERMIT，DENY，不同的动作下又有不同的可选配置，从而决定对符合匹配条件的数据流实现哪些业务。

配置步骤：

进入**策略>防火墙>策略**，选择 IPV4 或 IPV6，点击**新建策略**，如下图：



参数说明：

名称：防火墙策略的名称，名称不可配置，若指定了名称，则不同策略的名称不能重复。

入接口/安全域：数据流的流入方向，可以指定某个特定接口，也可以指定多个接口，any 表示所有接口。

出接口/安全域：数据流的流出方向，可以指定某个特定接口，也可以指定多个接口，any 表示所有接口。

源地址：数据流的源地址，可以引用已定义的某个或者多个地址对象或对象组，any 表示可以源地址可以匹配所有对象。

目的地址：数据流的目的地址，可以引用已定义的某个或者多个地址对象或地址对象组，any 表示目的地址可以匹配所有对象。

服务：数据流的服务属性，包括协议，源端口和目的端口，可以引用某个或者多个系统预定义服务、自定义的服务对象或服务对象组，any 表示服务可以匹配所有对象。

应用：数据流的应用属性，可以引用某个或者多个系统预定义应用、自定义的应用对象或应用对象组，any 表示可以匹配所有应用。

时间：策略生效的时间，可以引用某个或者多个已配置的时间对象，always 表示所有时间。

动作：对符合匹配条件的数据流执行的动作，PERMIT 为允许，DENY 为拒绝。

流量统计：只有当策略动作为允许时才可配置，用于统计匹配该策略的流量。

日志：启用日志功能，当策略动作为允许时，可以选择记录会话开始和会话结束的日志，当策略动作为拒绝时，可以记录匹配该拒绝动作的日志。

会话超时时间：匹配该策略的会话超时时间，不配置时，会话宝石系统默认的协议的超过时间。

策略组：策略所属的策略组。

描述：防火墙策略的描述。

配置完毕后，点击**提交**。

配置 DENY 策略

配置步骤：

进入**策略>防火墙>策略**，点击**新建策略**，在**动作**下拉框中选择 **DENY**，如下图：

参数说明：

日志：启用日志功能，匹配该策略的数据流被阻断的信息会被发往 syslog 服务器或者产生设备本地日志，日志的优先级为信息级别。

配置完毕后，点击**确定**。

配置 PERMIT 策略

配置步骤：

进入**策略>防火墙>策略**，点击**新建策略**，在**动作**下拉框中选择 **PERMIT**，如下图：

参数说明：

日志：启用日志功能，匹配该策略的数据流创建和拆除的信息会被发往 syslog 服务器或者产生设备本地日志，日志的优先级为信息级别。

流量统计：统计匹配该策略的流量，可在监控->会话->流量统计->基于防火墙策略中进行查看。

会话超时时间：匹配该策略的会话的超时时间，不配置时，会话保持系统默认的协议的超时时间。

配置完毕后，点击**确定**。

启用防火墙策略

配置好的防火墙策略必须启用才能使其生效。

配置步骤：

进入**策略>防火墙>策略**，如下图：

勾选**启用**，可以启用一条策略。

可以对防火墙策略里面的内容进行编辑修改，修改完毕后点击**确定**。

策略配置

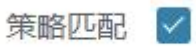
策略配置模块

在策略配置模块可以开启或者关闭整个策略匹配模块，也可以设置策略全部不匹配时执行的默认动作。

配置步骤：

进入**策略>防火墙>策略配置**，如下图：

勾选或者取消**策略匹配**的复选框，实现整个策略匹配模块的开启和关闭。



若勾选则开启策略匹配模块，经过系统的数据包都要经过防火墙策略的匹配；否则为关闭策略匹配模块，经过系统的数据包都不进行防火墙策略的匹配。

在下拉框里选择**策略默认动作**，可选择 permit 或者 deny，此动作为匹配不到防火墙策略时的默认动作。

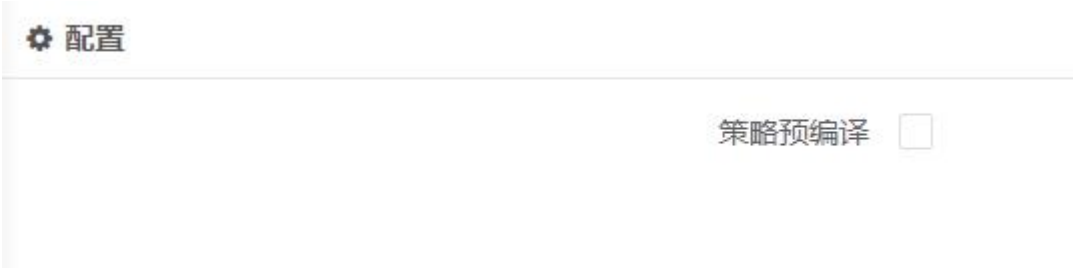
策略预编译

策略预编译模块

在策略预编译模块可以开启或者关闭防火墙策略预编译匹配功能，默认关闭。在大量防火墙策略配置情况下，开启策略预编译可以提高策略的匹配性能。

配置步骤：

进入**策略>防火墙>策略预编译**，如下图：



勾选或者取消策略预编译的复选框，若勾选则开启策略预编译功能。

点击开始按钮，对当前防火墙策略配置进行预编译；

点击停止按钮，释放当前编译的策略配置，会切换成默认匹配方式。

安全防护

防护策略

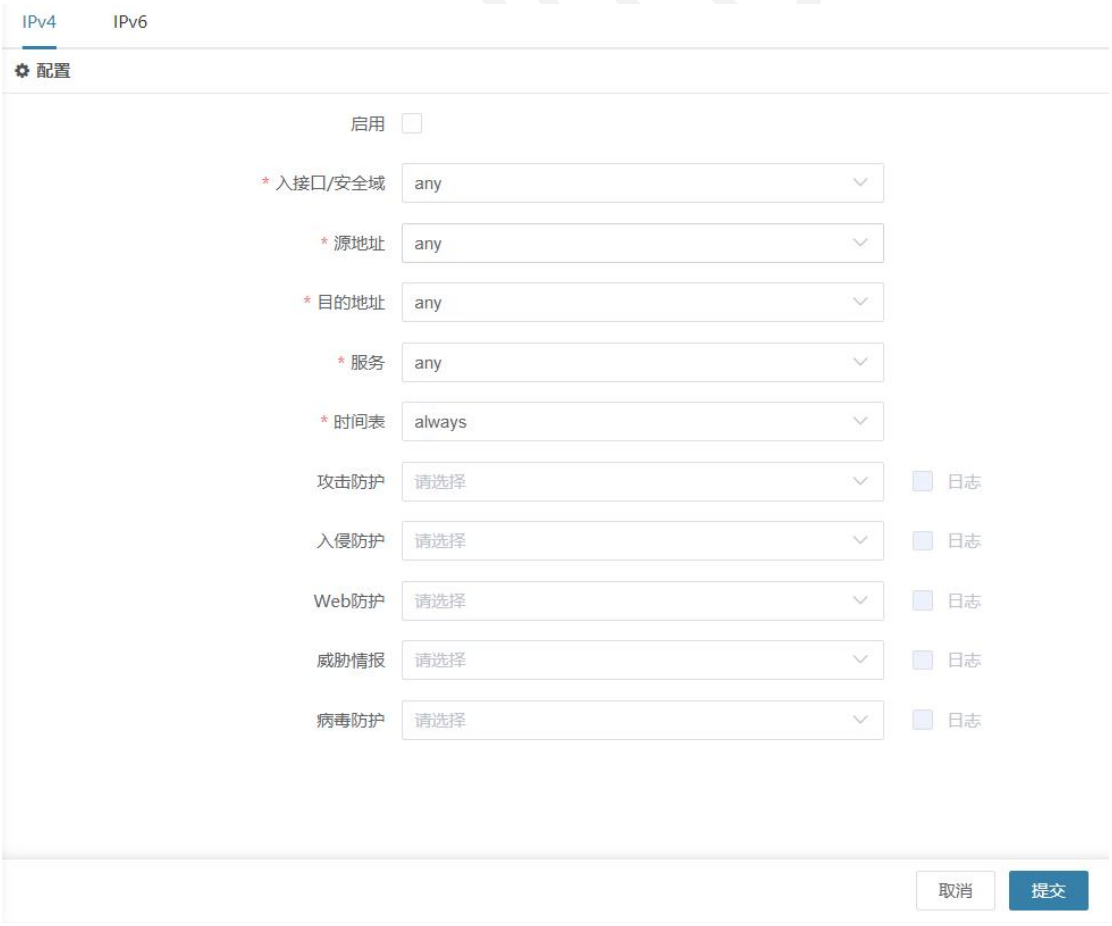
配置安全防护策略

配置策略的基本要素

安全防护策略的基本要素是匹配条件和动作。匹配条件包括数据流的入接口、源地址、目的地址、服务和策略生效的时间范围。其中，数据流的方向通过指定入接口、源地址、目的地址来确定，服务和时间范围都可以直接引用已定义的对象。

配置步骤：

进入**策略>安全防护>防护策略**，点击新建。



参数说明：

地址类型：安全策略分为 IPv4 和 IPv6 两种类型，数据包匹配相应协议类型的安全策略。

入接口：数据流的流入方向，可以指定某个特定接口，any 表示所有接口。

源地址：数据流的源地址，可以引用已定义的某个地址对象或地址对象组，any 表示源地址为任意。

目的地址：数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any 表示目的地址为任意。

服务：数据流的服务属性，包括协议、源端口和目的端口，可以引用系统预定义服务、自定义的服务对象或服务对象组，any 表示服务为任意。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

攻击防护：开启攻击防护，对匹配的报文进行控制，防止 FLOOD 攻击和防扫描。

入侵防护：入侵防御可以检测到特定的网络行为，并可以选择放行、阻断、阻断源 ip 等动作，以达到保护网络的功能。

web 防护：web 防护主要针对 XSS 攻击和 SQL 注入攻击进行防御。并根据预设的动作进行阻断或者放行。

威胁情报：根据配置策略对网络中威胁情报进行扫描。

病毒防护：针对内外网入口处进行实时的病毒扫描，实现工作站被动防御病毒之外的主动病毒防御，并还提供文件扫描功能。

日志：配置安全防护策略中各防护模块的日志过滤，支持日志信息在本地内存、syslog 服务器(日志控制中心)及 Email 这三种方式进行记录，每种方式都可以配置过滤的等级，当产生的日志高于或等于配置的过滤等级时，才会输出日志信息。

配置完毕后，点击**提交**。

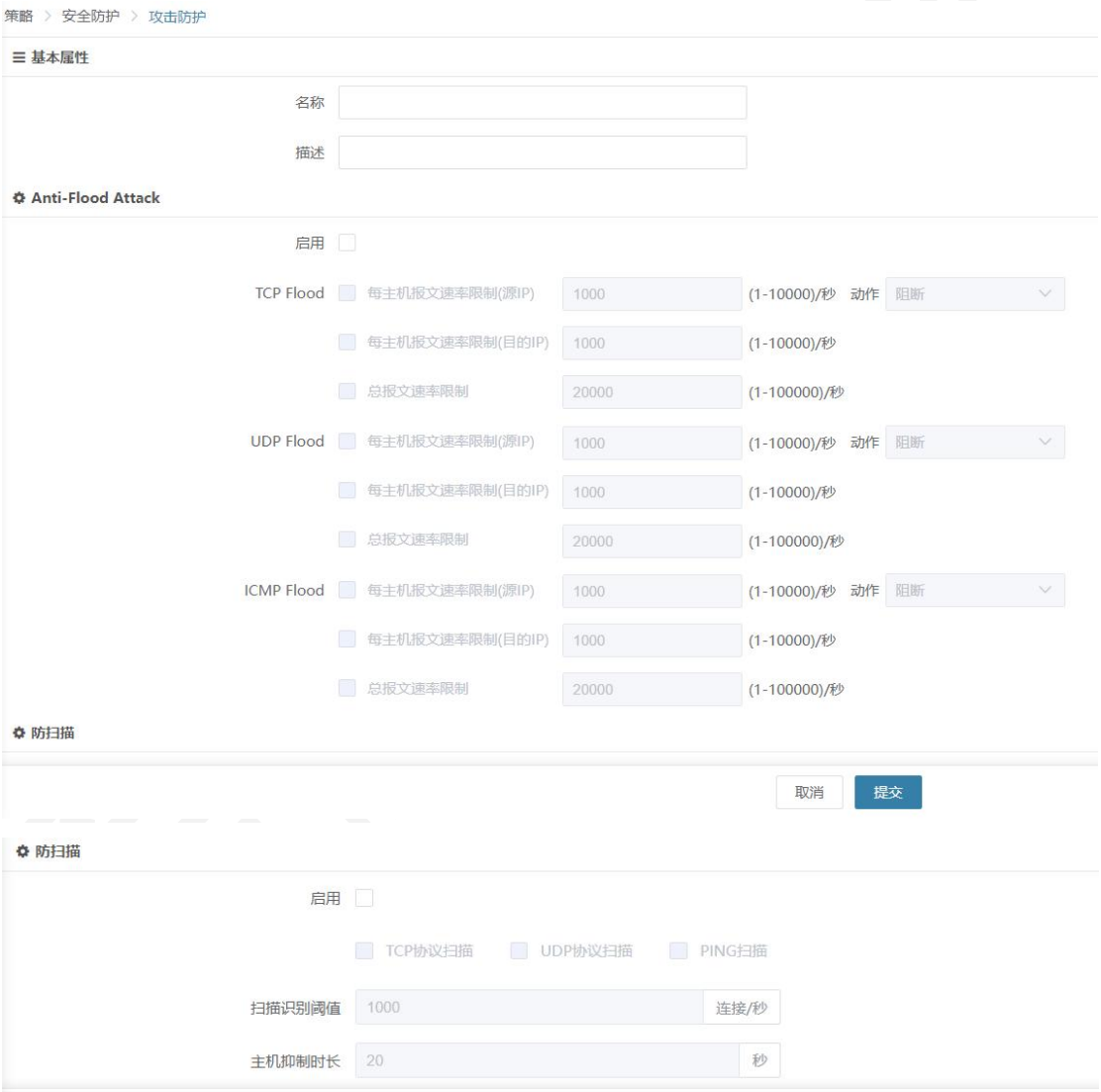
攻击防护

配置攻击防护

创建攻击防护

配置步骤：

进入**策略>安全防护>攻击防护**，点击**新建。**



名称：攻击防护名称，支持中文名称。

描述：攻击防护的简单描述信息。

Anti-Flood Attack：配置是否启用防 **Flood** 攻击。

TCP Flood：选择启用 **TCP** 协议的防 **Flood** 攻击功能。**TCP Flood** 即 **SYN Flood** 攻击，是众多攻击形式的一种方式。**SYN Flood** 利用 **TCP** 协议的缺陷，向服务器端发送大量伪造的 **TCP** 连接请求之后，自身不再做出应答，使得服务器端的资源迅速耗尽，从而无法及时处理其它正常的服务请求，严重的时候甚至会导致服务器系统的崩溃。

识别门限：配置 syn 报文个数的阈值，即防 **TCP Flood** 攻击的启动门限。

动作：阻断、警告、**syncookie**。

UDP Flood：选择启用 **UDP** 协议的防 **Flood** 攻击功能。

识别门限：配置 **UDP** 报文个数的阈值，即防 UDP Flood 攻击的启动门限。

动 作：阻断、警告。

ICMP Flood：选择启用 **ICMP** 协议的防 **Flood** 攻击功能。

识别门限：配置 **ICMP** 报文个数的阈值，即防 **ICMP Flood** 攻击的启动门限。

动作：阻断、警告。

防扫描：配置是否启用防扫描攻击。

TCP 协议扫描：根据实际网络情况，当受到 **TCP** 扫描攻击时，可以配置防 **TCP** 扫描。当一个源 IP 地址在 1 秒内将含有 **TCP SYN** 片段的 **IP** 封包发送给位于相同目标 **IP** 地址的不同端口（或者不同目标地址的相同端口）数量大于配置的阈值时，即认为其进行了一次 **TCP** 扫描，系统将其标记为 **TCP SCAN**，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 **TCP SYN** 包。启用防 **TCP** 扫描，可能会占用比较多的内存。

UDP 协议扫描：根据实际网络情况，当受到 **UDP** 扫描攻击时，可以配置防 **UDP SCAN** 扫描。当一个源 **IP** 地址在 **1** 秒内将含有 **UDP** 的 **IP** 封包发送给位于相同目标 **IP** 地址的不同端口（或者不同目标地址的相同端口）数量大于配置的阈值时，即进行了一次 **UDP** 扫描，

系统将其标记为 **UDP SCAN**，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 **UDP** 包。启用防 **UDP** 扫描，可能会占用比较多的内存。

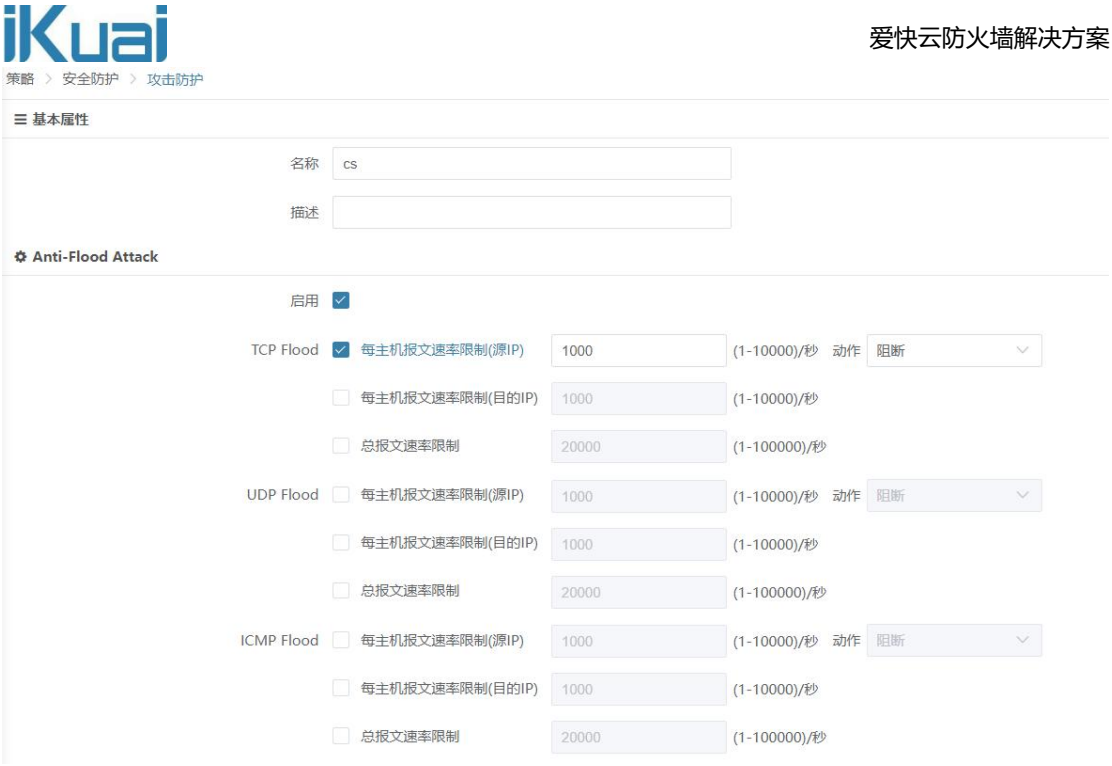
PING 扫描：根据实际网络情况，当受到 **PING** 扫描攻击时，可以配置防 **PING** 扫描。当一个源 **IP** 地址在 **1** 秒内发送给不同主机的 **ICMP** 封包超过门限值时，即进行了一次地址扫描。此方案的目的是将 **ICMP** 封包（ 通常是应答请求）发送给各个主机，以期获得至少一个回复，从而查明目标地址。下一代安全防护平台设备在内部记录从某一远程源地点发往不同地址的 **ICMP** 封包数目。

当某个源 **IP** 被标记为地址扫描攻击，则系统在配置的阻断时间内拒绝来自该主机的其它更多 **ICMP** 封包。启用防 **PING** 扫描，可能会占用比较多的内存。

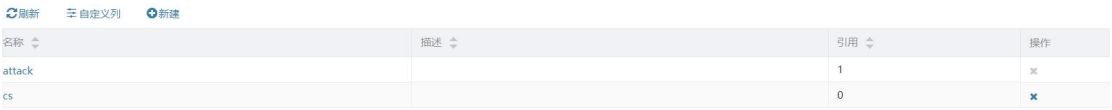
主机抑制时长：设置防扫描功能的阻断时间，当系统检测到扫描攻击时，在配置的时长内拒绝来自于该台源主机的所有其它攻击包，缺省配置为 **20** 秒。

扫描识别阈值：防扫描功能的扫描识别门限，超过阈值时，该源 **IP** 被标记为扫描攻击，来自于该台源主机的所有其它攻击包都被阻断，缺省配置为 **1000**。

输入攻击防护**名称**和**描述**，配置好各项功能：



点击**提交**，完成对攻击防护的配置，显示如下页面：



入侵防护

配置事件集

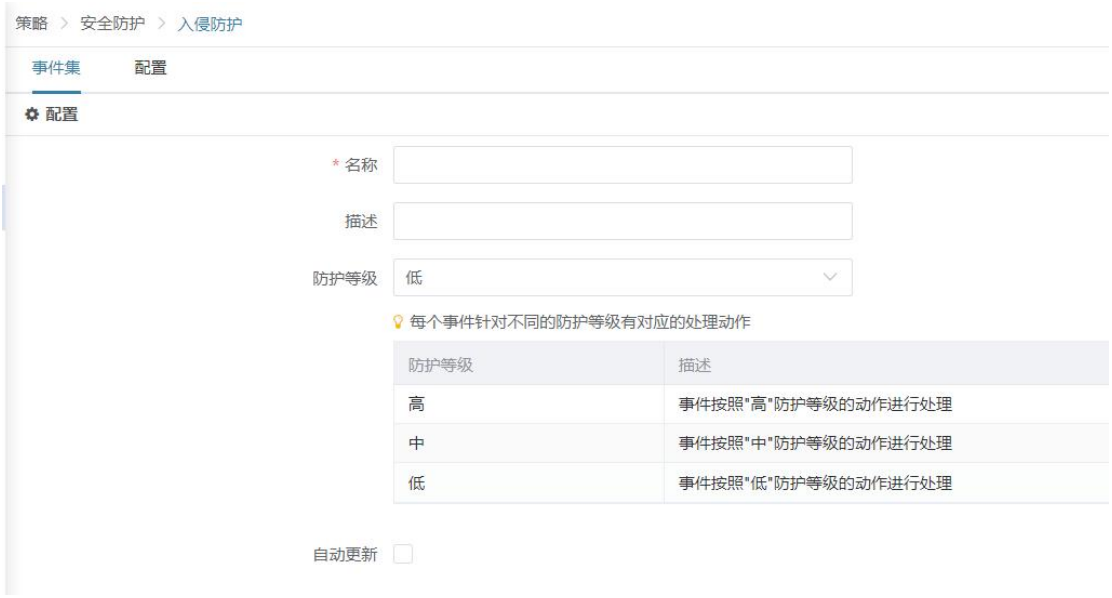
新建事件集

配置步骤：

1．进入**策略>安全防护>入侵防护**，如下图：

由粗体显示的事件集名称，是系统预定义的事件集。

2．点击**新建，**创建事件集，如下图：



参数说明：

名称：事件集名称。

描述：事件集的描述。

防护等级：事件集的防护等级。

3．配置完毕后，点击**提交**。

WEB 防护

配置 Web 防护

配置策略的基本要素

Web 防护策略的基本要素是名称和 SQL 注入防护开关和 XSS 攻击防护开关。建立好模板策略的两种攻击动作有“放行”，“拒绝”。

配置步骤：

进入**策略>安全防护>Web 防护**，点击新建。

参数说明：

名称：该策略的名称。

SQL 注入：SQL 注入攻击防护的开关。

动作：放行或阻断。

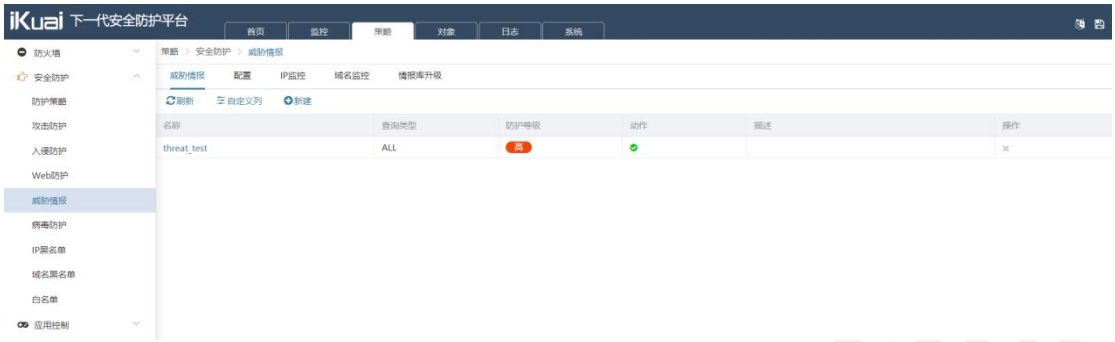
XSS 攻击：XSS 攻击防护的开关。

动作：放行或阻断。

配置完毕后，点击**提交**。

威胁情报

系统默认生成一条 threat_test 威胁情报防护策略，对网络中 IP/域名进行防护。



点击 threat_test 可查看/修改防护配置。

名称：查看威胁情报策略名称。

描述：对本条策略描述。

威胁类型：威胁类型默认是 any，表示生效所有威胁类型。威胁类型包含：勒索软件、挖矿软件、网银木马、窃密木马、黑客工具、后门软件。

查询类型：默认为 all，包含查询 IP、域名，可指定查询类型。

防护等级：防护等级分为低、中、高三个选项，默认防护等级为高。

动作：动作可根据需求设置放行或阻断。

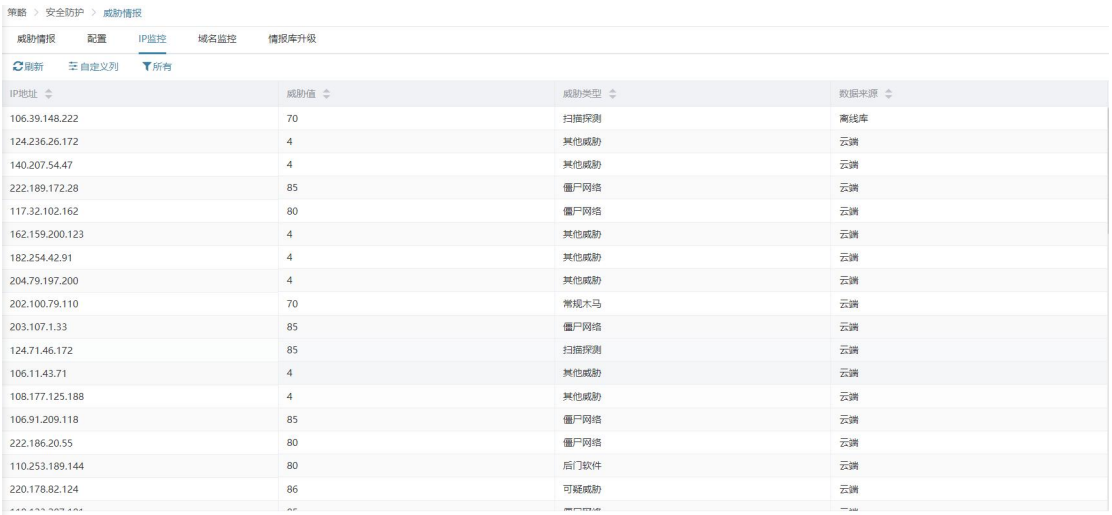
威胁情报防护等级配置：

防护等级：对防护等级高、中、低设置设置威胁值。

云端查询：开启后需要配置 DNS 服务器，指定云端服务器查询。

IP 监控：

查看监控到的威胁 IP，数据来源，威胁的类型。可自定义筛选 IPv4 或 IPv6 地址。



IP地址	威胁值	威胁类型	数据来源
106.39.148.222	70	扫描探测	离线库
124.236.26.172	4	其他威胁	云端
140.207.54.47	4	其他威胁	云端
222.189.172.28	85	僵尸网络	云端
117.32.102.162	80	僵尸网络	云端
162.159.200.123	4	其他威胁	云端
182.254.42.91	4	其他威胁	云端
204.79.197.200	4	其他威胁	云端
202.100.79.110	70	常规木马	云端
203.107.1.33	85	僵尸网络	云端
124.71.46.172	85	扫描探测	云端
106.11.43.71	4	其他威胁	云端
108.177.125.188	4	其他威胁	云端
106.91.209.118	85	僵尸网络	云端
222.186.20.55	80	僵尸网络	云端
110.253.189.144	80	后门软件	云端
220.178.82.124	86	可疑威胁	云端

域名监控：

监控网络中威胁域名，显示域名、威胁值、威胁类型、数据来源。

情报库升级：

对情报库升级，支持上传升级文件离线升级情报库，定时对情报库升级、立即升级。查看最近升级时间、状态。

病毒防护

病毒防护概述

针对内外网入口处进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防御。同时还提供文件扫描功能，可以对特定的文件类型进行扫描。我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 等应用协议时进行文件扫描。

配置病毒防护

新建病毒防护模板

配置步骤：

1.进入**策略>安全防护>病毒防护**，点击**新建。**

参数说明：

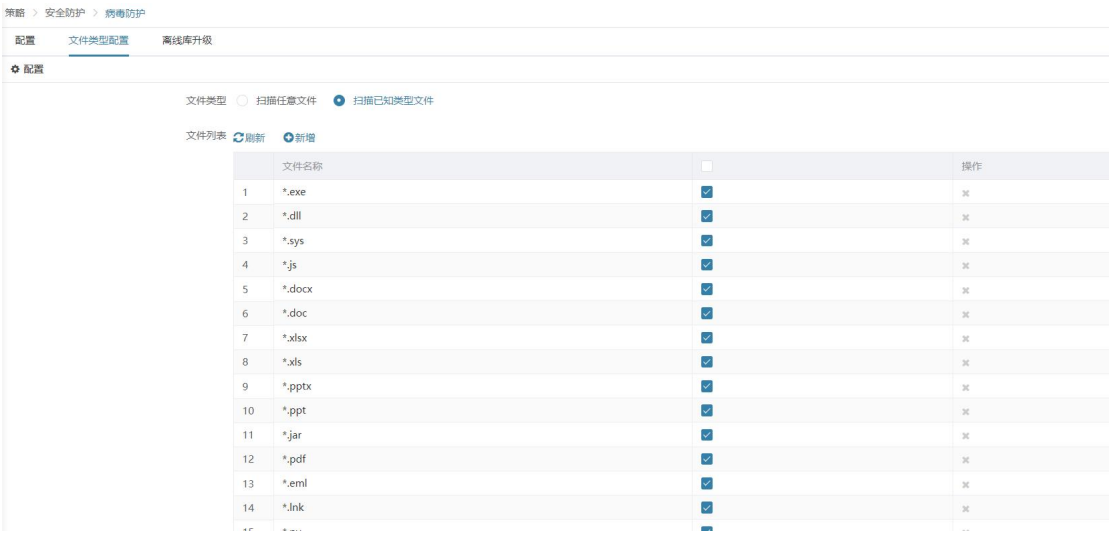
名称：病毒防护模板名称。

协议：数据流的应用协议，至少选择一个。

行为：对符合匹配条件的数据流执行的动作，放行或者阻断。

文件类型配置：

对病毒文件类型进行配置。



文件类型：可选扫描任意文件、扫描已知类型文件。

文件列表：显示支持扫描的文件后缀名，列表中没有的后缀名可点击新增进行添加。

IP 黑名单

设置云防火墙 IP 黑名单。

点击新建，添加 IP 黑名单。

类型：可选择添加黑名单 IP 的类型，支持添加 IPv4、IPv6、用户区域黑名单。

源 IP：选择对应类型后填写对应 IP 地址。

超时：超时时间可选有效时间、绝对时间，设置时间值，单位可选分钟、天、月。

加入分组：选择所属分组。

IP 黑名单组：

默认有两个分组，支持自定义分组。

点击新建，配置分组。

名称：设置分组名称。

启动：是否启用分组。

超时：设置分组超时时间，可选有效时间、绝对时间、无，超时时间单位可选分钟、天、月。

阻断方向配置：

黑名单阻断方向：可选从源 IP 方向阻断、源或目的 IP 方向阻断。

导入：

配置超时时间、选择所属分组、导入 IP 地址文件。

导出：

支持导出全部黑名单配置、导出永久黑名单配置、导出指定分组黑名单。

域名黑名单

添加网络中黑名单域名。

新建域名：

设置请求域名地址、时间表。

白名单

添加白名单 IP 地址。

点击新建，根据需求新建白名单 IPv4、IPv6 地址、用户区域。设置超时时间。

设置白名单匹配方向，可选从源 IP 匹配、源或目的 IP 匹配。

应用控制

应用控制策略

配置应用控制策略

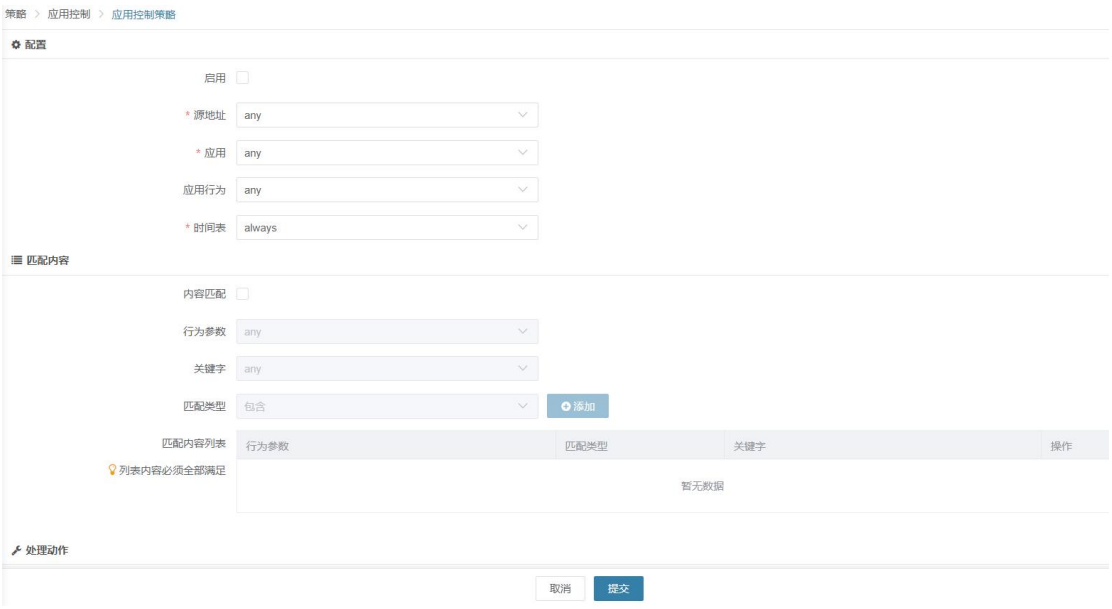
配置策略的基本要素

应用控制策略的基本要素是匹配条件和动作。匹配条件包括地址对象、应用对象、应用行为、行为参数、关键字匹配、策略生效的时间范围。

其中，地址对象、时间范围对象、关键字对象都都需要先建立好模板，策略的动作有“允许”，“拒绝”。

配置步骤：

1.进入**策略>应用控制>应用控制策略**，点击新建。



参数说明：

启用：是否启用该策略。

源地址：源地址节点或源地址对象组，支持添加 IPv4 地址、IPv6 地址。

应用：默认为 any，可根据需求搜索应用控制协议名称。

应用行为：应用特征库库可以识别的动作，any 表示所有应用行为。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

内容匹配：没有启用则匹配内容列表不生效，启用则匹配内容列表生效。

行为参数：以上配置的应用行为所支持审计的参数。any 表示应用行为的所有参数。

关键字：引用建立好的关键字模板。当行为参数获取到的内容包含关键字内容，则匹配成功。any 代表匹配任何内容。

匹配类型：匹配类型分别包含和不包含两种。

匹配内容列表：根据行为参数+关键字+匹配类型的组合为一组，匹配时只有都满足这些组合才算匹配成功。

处理动作：对符合匹配条件的数据流执行的动作。

日志：日志开关，该日志开关和日志模块的日志开关都开启后才生效。

配置完毕后，点击**提交**。

WEB 控制策略

配置 Web 控制策略

配置策略的基本要素

Web 控制策略的基本要素是匹配条件和动作。

匹配条件包括源地址、入接口、用户、URL 分类、文件类型、行为参数、关键字匹配、策略生效的时间范围。其中，地址对象、时间范围对象、关键字对象都需要先建立好。模板策略的动作有“允许”，“拒绝”。

配置步骤：

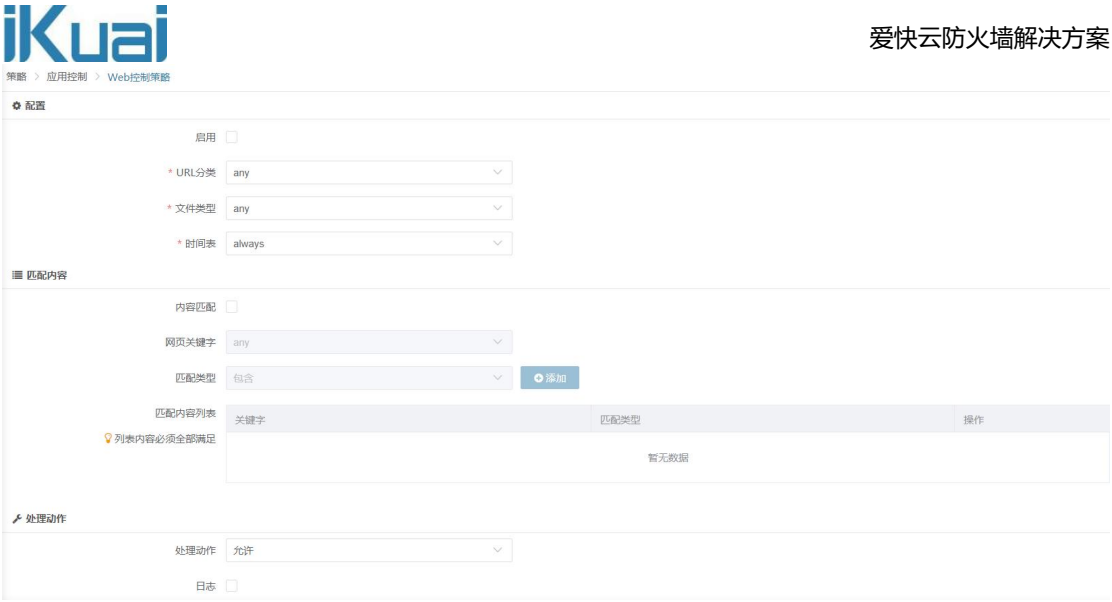
1.进入**策略>应用控制>Web 控制策略**，点击新建。

参数说明：

启用：是否启用该策略。

源地址：源地址对象或源地址对象组（目前只适用于 IPv4）。

2.进入**策略>应用控制>Web 控制策略>控制规则列表**，点击新建。



参数说明：

启用：是否启用该策略的规则。

URL 分类：引用下拉框支持模糊搜索 URL 类型，any 表示所有 URL 分类。

文件类型：引用建立好的关键字模板。当行为参数获取到的内容包含关键字内容，则匹配成功。any 代表匹配任何内容。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

内容匹配：没有启用则匹配内容列表不生效，启用则匹配内容列表生效。

网页关键字：引用建立好的关键字模板。当行为参数获取到的内容包含关键字内容，则匹配成功。

匹配类型：匹配类型分别包含和不包含两种。

匹配内容列表：根据行为关键字+匹配类型+操作的组合为一组，匹配时只有都满足这些组合才算匹配成功。

处理动作：对符合匹配条件的数据流执行的动作，允许或拒绝。

日志：日志开关，该日志开关和日志模块的日志开关都开启后才生效。

3.配置完毕后，点击**提交**。

关键字

关键字配置

关键字可以在应用控制策略、Web 控制策略里的关键字下拉菜单里直接新建引用。也可以在此功能中先创建。

配置步骤：

进入**策略>应用控制>关键字**，如下图：

参数说明：

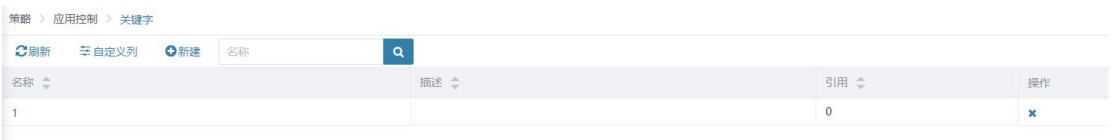
名称：关键字模板的名字。

描述：用户可以配置对关键字的描述信息。

关键字：要进行匹配的关键字。

关键字列表：匹配时只要满足一条关键字即算匹配成功。

配置完毕后，点击**提交**。



对象

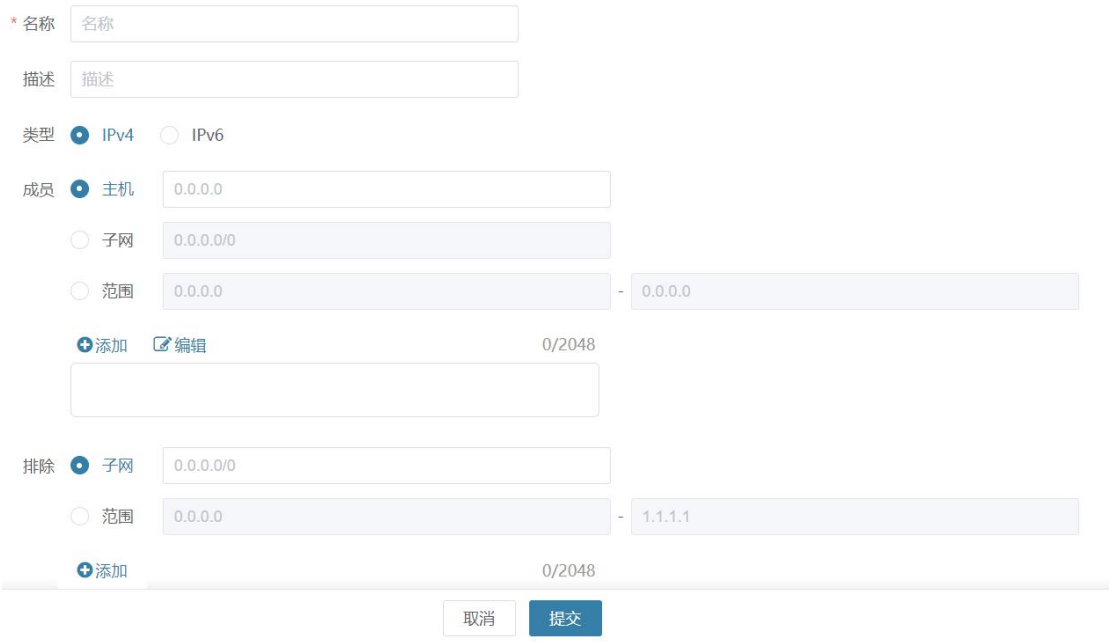
地址对象

地址节点

地址对象分为地址节点和地址组，地址组是地址节点的集合。在其它功能的配置中（如防火墙策略、NAT 规则，路由策略），可以引用地址对象来定义配置生效的条件。

地址节点分为 IPv4 类型，IPv6 类型。

进入**对象->地址对象>地址节点**，点击**新建**，如下图：



名称：为新建地址节点设置名称。

描述：对新建地址节点做描述。

类型：地址节点可分为 IPv4 类型，IPv6 类型。

地址节点：

成员：该地址节点中包含的成员。

IPv4 类型地址节点的内容包含：

主机：主机 IPv4 地址。

子网： IPv4 网段地址。

范围： IPv4 地址池范围。

IPv4 的 ISP 地址库。

IPv6 类型地址节点的内容包括：

主机：主机 IPv6 地址。

子网：IPv6 网络地址。

范围：IPv6 地址范围。

排除：该地址节点中排除的成员。

IPv4 类型地址节点：

子网： IPv4 网段地址。

范围： IPv4 地址池范围。

点击**提交**。

批量删除地址节点

可对未被引用的地址节点进行批量删除操作。

进入**对象->地址对象->地址节点**，在地址节点首列选中可勾选所要批量删除的地址节点，

如下图：

地址组

地址组是地址节点的集合，可以使用地址组方便的管理和地址相关的规则。

配置步骤：

进入**对象->地址对象>地址组，**点击**新建，**如下图：

名称：为新建地址组设置名称，不得超过 63 个字符。

描述：对新建地址组做描述，不得超过 127 个字符。

可用地址和地址组：已经定义好的地址节点和地址组信息。

成员：地址组成员。

点击**提交**。

批量删除地址组

可对未被引用的地址组进行批量删除操作。

进入**对象->地址对象->地址组**，在地址组首列选中可勾选所要批量删除

的地址组，如下图：

点击  ，批量删除完成。

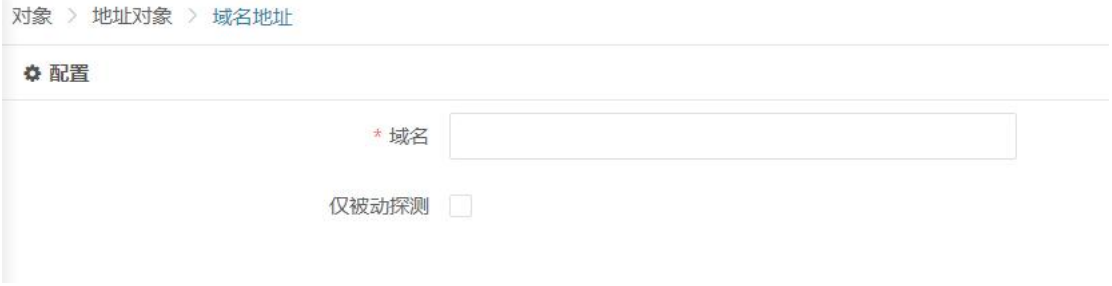
域名地址

域名地址是一种特殊的地址对象，对象名称定义为域名地址，对象成员是系统从 DNS 服

务器解析到的 IP 地址集合。

配置步骤：

进入**对象->地址对象>域名地址**，点击**新建**，如下图：



域名：设置需要解析的域名，不得超过 63 个字符。

仅被动探测：是否开启仅被动探测。

点击**提交**。

备份/恢复

点击**对象->地址对象>备份恢复**，如下图：

参数说明：

恢复：可导入包含地址对象配置的文本文件，系统会读取文件中的配置并执行下发。

备份：可将地址对象的配置导出至一个文本文件中。

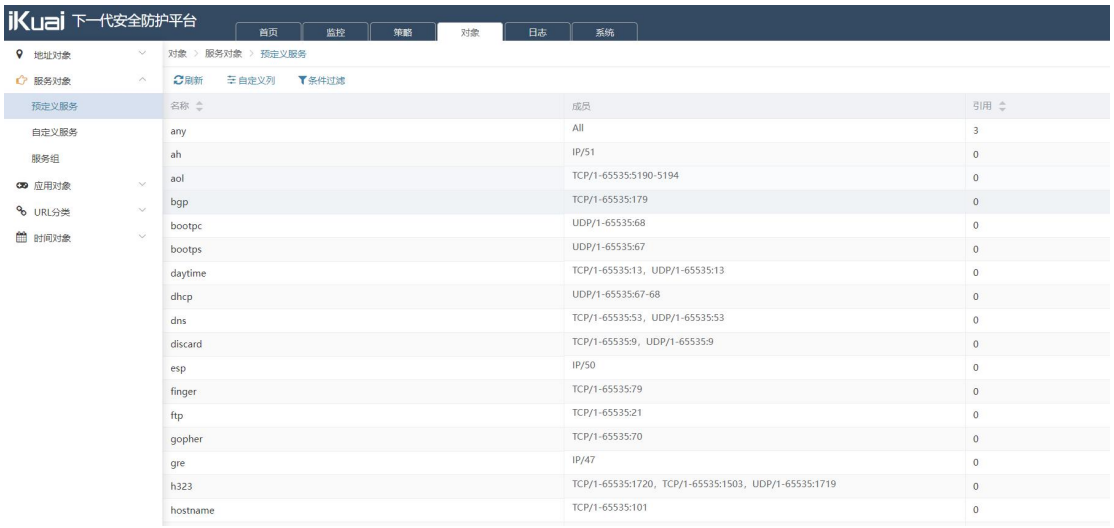
服务对象

预定义服务

预定义服务：系统预先添加服务，用户不可编辑或删除。

进入**对象>服务对象>预定义服务**，可查看预定义配置：

下图是部分系统预定义服务。

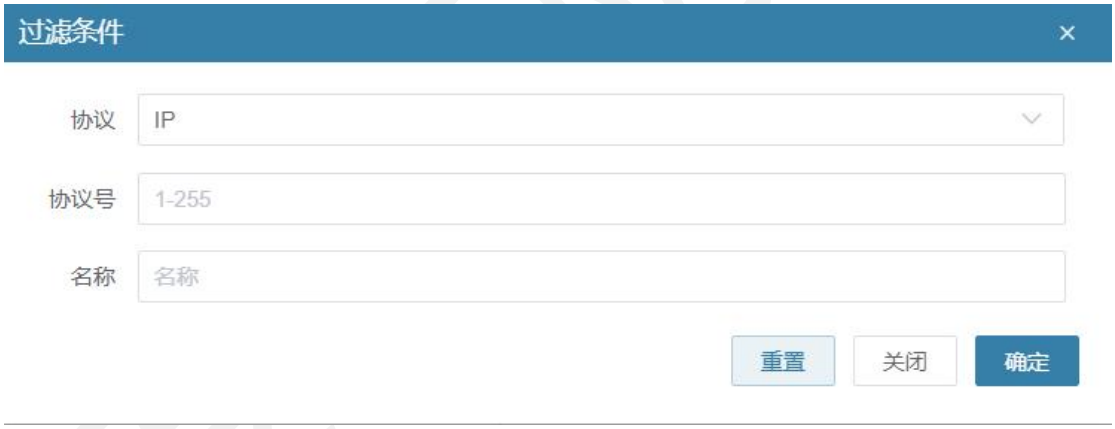


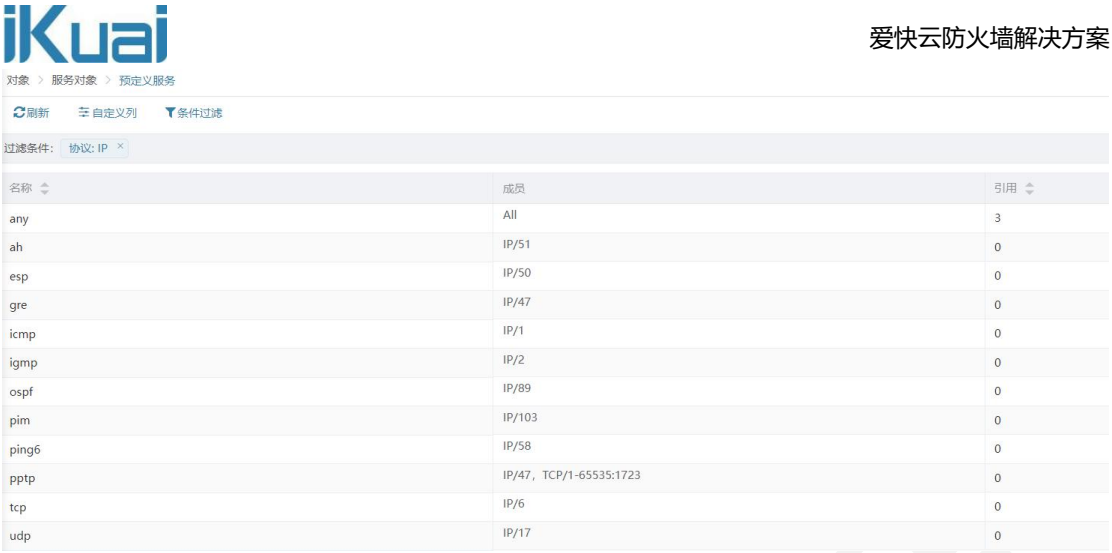
查看预定义服务

进入**对象->服务对象>预定义服务**，如下图：

协议查找：

在条件过滤处输入(TCP/UDP/ICMP/IP)其中一种，点击可以查看匹配项如下：





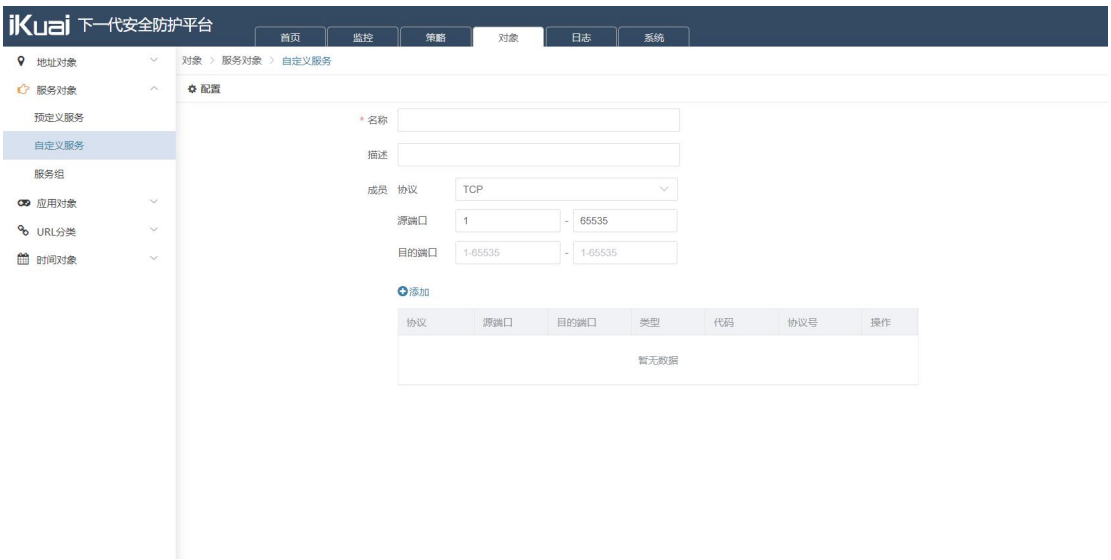
名称	成员	引用
any	All	3
ah	IP/51	0
esp	IP/50	0
gre	IP/47	0
icmp	IP/1	0
igmp	IP/2	0
ospf	IP/89	0
pim	IP/103	0
ping6	IP/58	0
pptp	IP/47，TCP/1-65535:1723	0
tcp	IP/6	0
udp	IP/17	0

自定义服务

自定义服务：需要用户自行配置添加。

配置步骤：

进入**对象->服务对象>自定义服务**，点击**新建**，如下图



名称：为新建自定义服务设置名称。

描述：对新建自定义服务做描述。

协议：可以自定义的服务协议（TCP,UDP,ICMP,IP）。

源端口：协议源端口号。

目的端口：协议目标端口号。

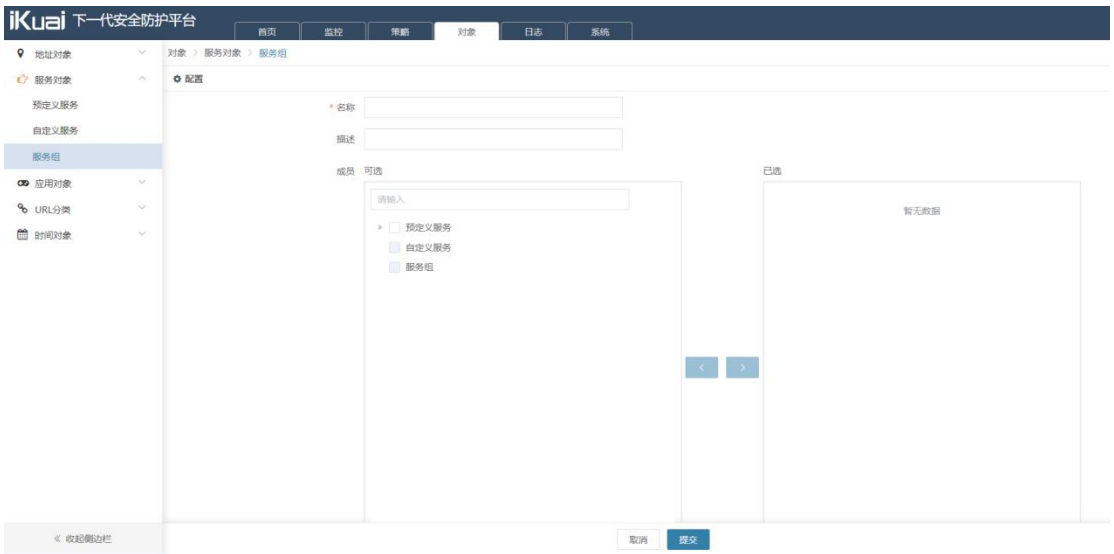
点击**提交**。

服务组

服务组：服务组是服务的集合。

配置步骤：

进入**对象->服务对象>服务组**，点击**新建**，如下图：



名称：为新建服务组设置名称。

描述：对新建服务组做描述。

可用服务和服务组：显示已有的服务对象，可从中选择预定义服务与自定义服务添加到服务组中。

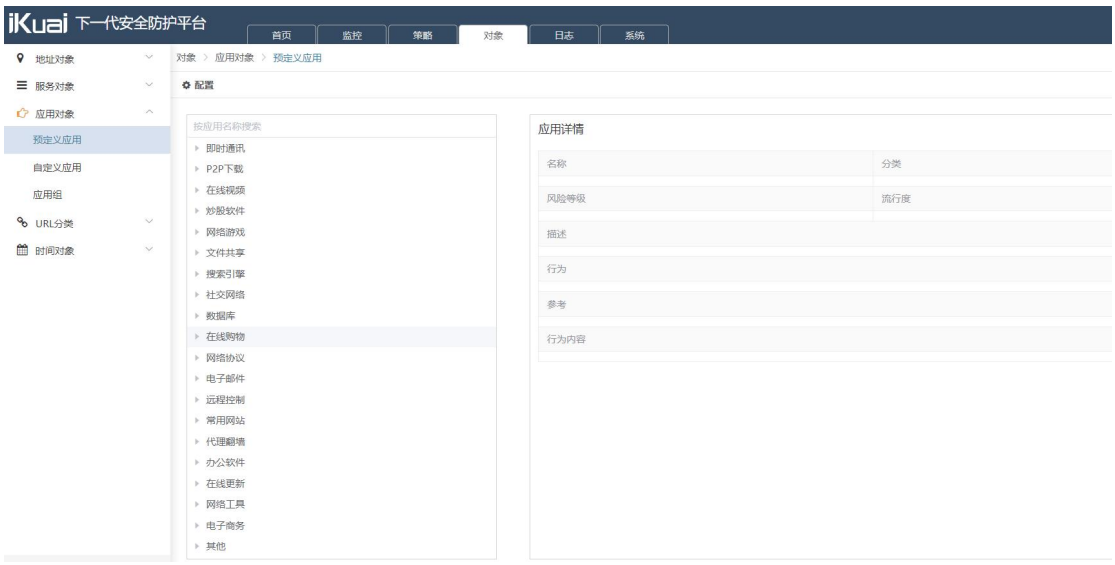
点击**提交**。

应用对象

预定义应用

预定义应用：具体的用户应用，如 P2P 下载、即时通讯软件，目前有 20 大类 1000 多种应用，通过应用于特征库更新，不需要用户配置。

进入**对象>应用对象>预定义应用**，通过左侧树状目录中选择应用，如下：



自定义应用

自定义应用：需要用户自行配置。

配置步骤：

1.进入**对象>应用对象>自定义应用**

该界面显示已配置的自定义应用。

2.点击**新建**，进入自定义应用配置页面。

名称：为新建自定义应用的名称。

协议类型：选择协议类型，可配置为 TCP 或 UDP。

源地址：应用的源地址，可以引用已定义的某个地址对象或地址对象组，any 表示源地址为任意。

源端口：应用的源端口，端口号允许的范围为 1~65535。

目的地址：应用的目的地址，可以引用已定义的某个地址对象或地址对象组，any 表示目的地址为任意。

目的端口：应用的目的端口，端口号允许的范围为 1~65535。。

3.点击**提交**。

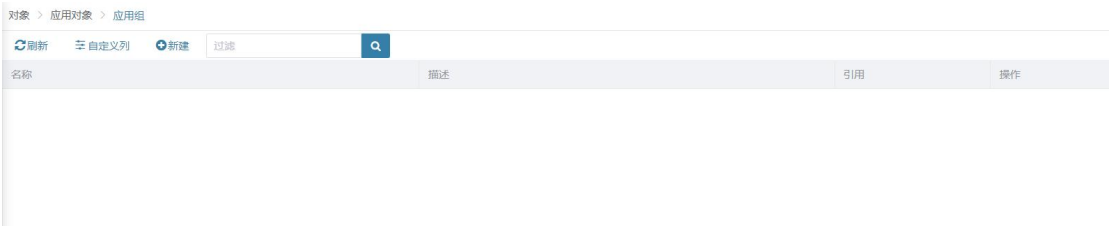
应用组

应用组：需要用户自行配置，可引用预定义应用和自定义应用。

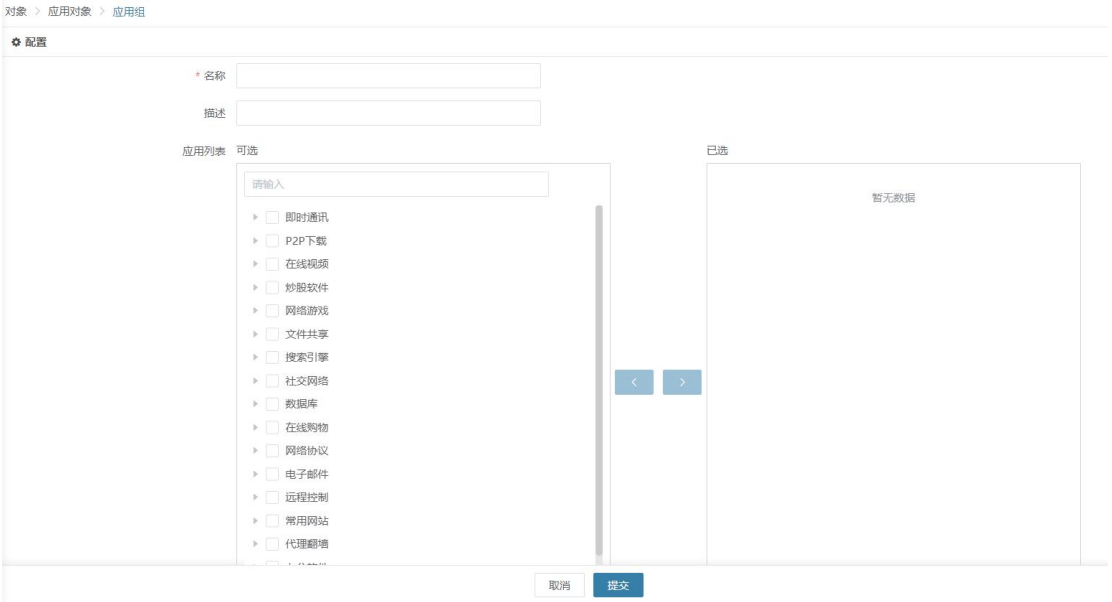
配置步骤：

1.进入**对象>应用对象>应用组**

该界面显示已配置的应用组。



2.点击**新建**，进入应用组配置页面



名称：为新建应用组的名称。

描述：为新建应用组的描述。

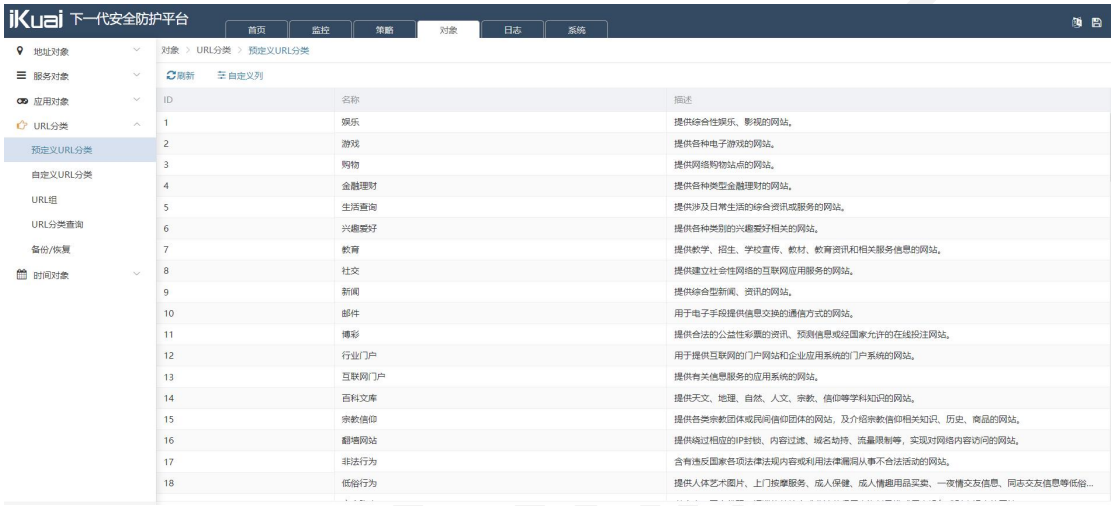
应用列表：为系统所支持的所有应用列表。如上图所示。

选中所想要的应用，点击**提交**。

URL 分类

预定义 URL 分类

预定义 URL 分类:将常见的 URL 进行分类,例如娱乐、金融理财、互联网门户等,通过 URL 特征库更新，不需要用户配置。



自定义 URL 分类

自定义 URL 分类：需要用户自行配置 URL 分类。

配置步骤:

1.进入**对象>URL 分类>自定义 URL 分类**

该界面显示已配置的自定义 URL 分类。

点击新建，自定义 URL 分类。

名称：给策略定义一个名称。

描述：对此条策略做描述。

URL：添加自定义的 URL 条目。

URL 列表：添加的 URL 或显示到 URL 列表中，每条策略最多可添加 1000 条 URL。

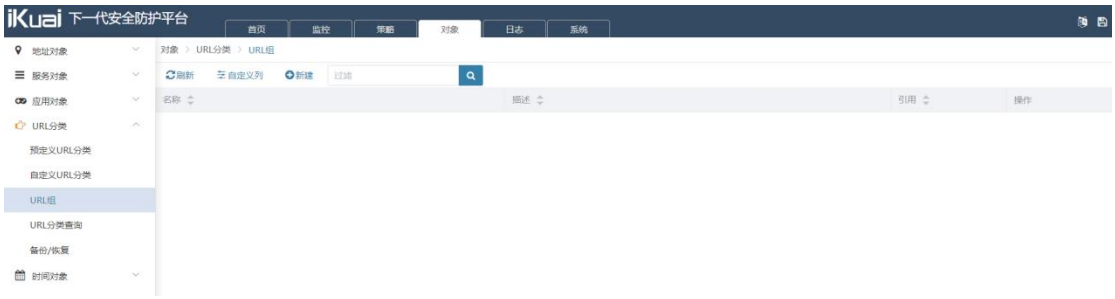
URL 组

URL 组：需要用户自行配置，可引用预定义 URL 分类和自定义 URL 分类。

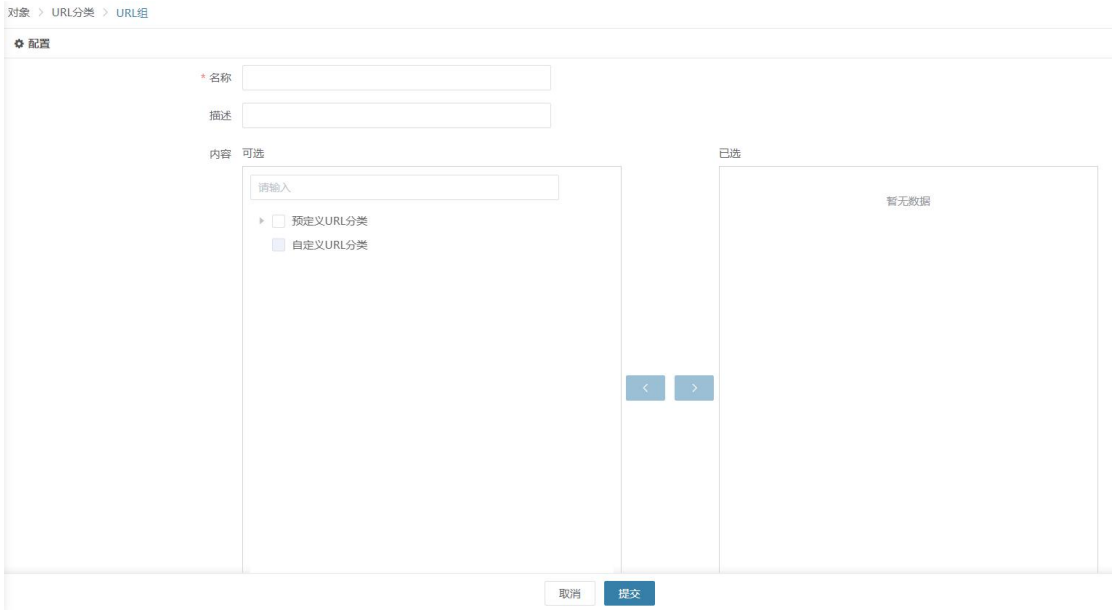
配置步骤：

1.进入**对象>URL 分类>URL 组**

该界面显示已配置的 URL 组。



2.点击**新建**，进入 URL 组配置页面



名称：为新建 URL 组的名称。

描述：为新建 URL 组的描述。

内容：为设备上已配置的自定义 URL 分类和所有预定义 URL 分类。

选中所想要的 URL 分类，点击**提交**。

URL 分类查询

对 URL 的分类进行查询。

进入**对象>URL 分类>URL 分类查询**，如下：

URL：输入 URL，点击查询，查看 URL 所属分类。

备份/恢复

对自定义 URL 分类进行导入导出、恢复备份。

进入**对象>URL 分类>备份恢复**

系统配置导入: 选择配置文件导入到设备中。

系统配置导出: 将设备中的配置文件导出。

时间对象

绝对时间

绝对时间：配置服务在指定的时间内生效。

绝对时间中只能配置一个有效时间范围。

进入**对象>时间对象>绝对时间**，点击**新建**，如下图：

名称：为新建绝对时间设置名称。

描述：对新建绝对时间做描述。

开始时间：绝对时间的起始时间（年，月，日，时，分）。

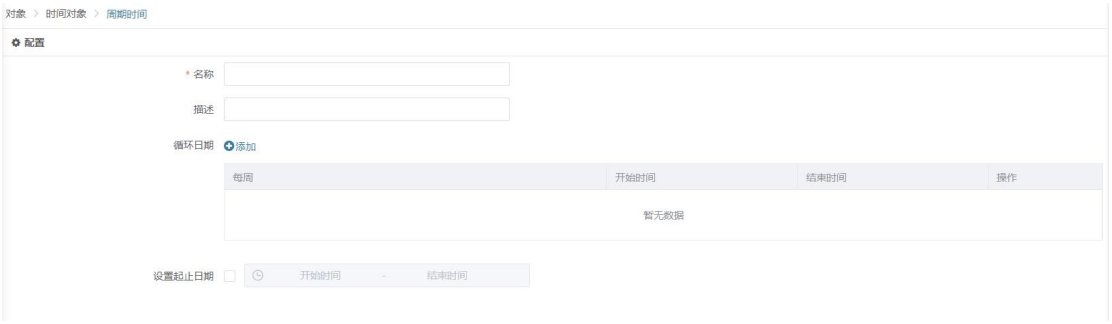
结束时间：绝对时间的终止时间（年，月，日，时，分）。

点击**提交。**

周期时间

周期时间中可以定义有效时间范围和有效时间段。有效时间范围只能有一个，而有效时间段可以有多个。有效时间段之间是或的关系，满足其中一个即可；有效时间范围和有效时间段之间是与的关系，都满足才生效。

进入**对象->时间对象>周期时间**，点击**新建**，如下图



名称：为新建周期时间设置名称。

描述：对新建周期时间做描述。

开始时间：有效时间范围的起始时间（年，月，日，时，分）。

结束时间：有效时间范围的终止时间（年，月，日，时，分）。

循环日期：点击添加按钮可以添加日期设置有效时间段，如下图：

设置起止时间：设置本条策略的起止时间。

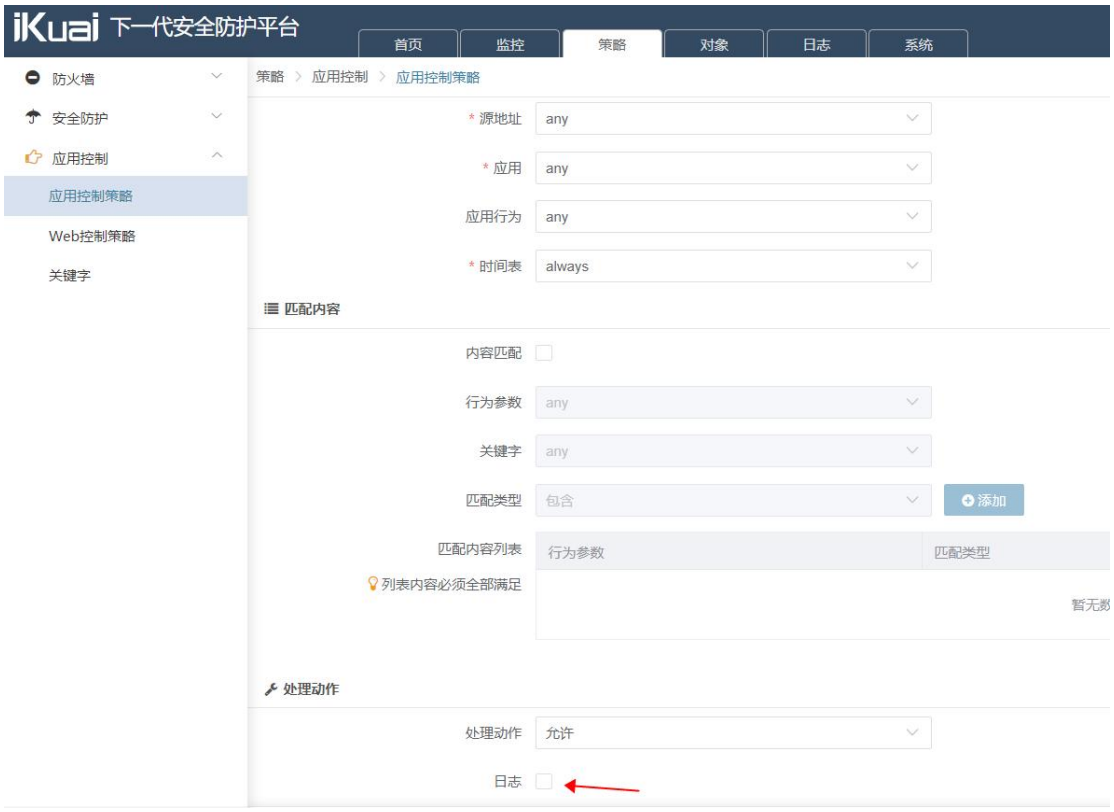
点击**提交**。

日志

审计日志

应用控制

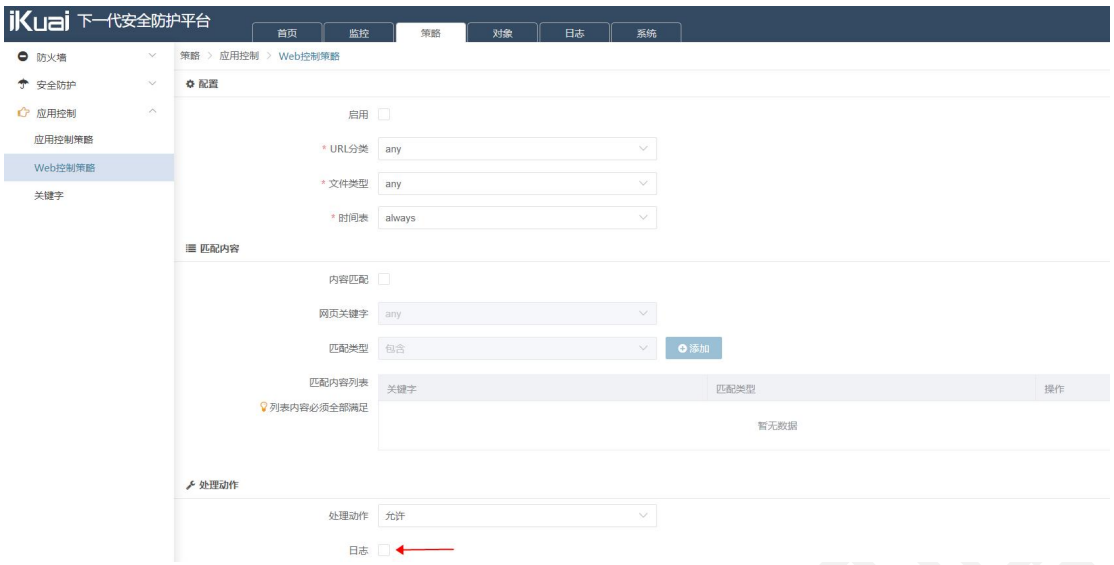
应用控制：需要在具体的应用控制策略配置中开启日志，才能上报到此页面。



在应用控制页面查看日志详情，可根据需求对日志类型、级别、源 IP、目的 IP 等条件进行筛选查看。

WEB 控制

WEB 控制：需要在具体的 WEB 控制策略配置中开启日志，如下图



在 Web 控制页面查看日志详情，可根据需求对日志类型、级别、源 IP、目的 IP 等条件进行筛选查看。

安全日志

防火墙策略

防火墙策略：显示防火墙日志策略信息。

参数说明：

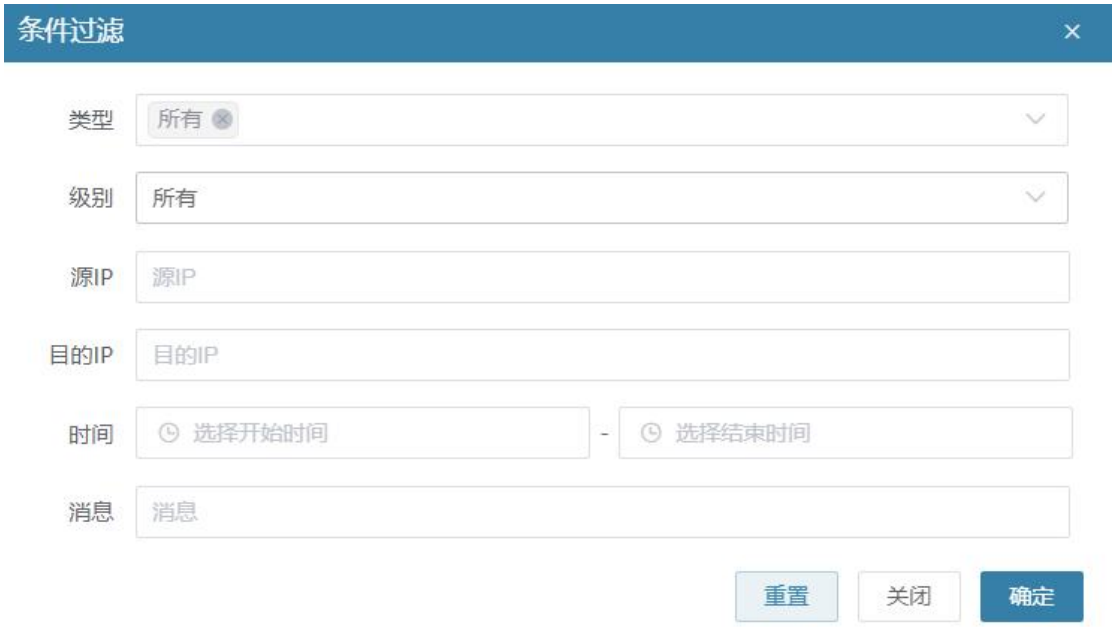
时间：该日志消息的产生时间。

级别：该日志消息的级别。

类型：该日志消息的模块类型。

消息：该日志消息的具体内容。

过滤条件



类型：选择防火墙策略。

级别：可选所有、紧急、告警、严重、错误、警示、通知、信息。

源 IP：填写要进行筛选的 IP。

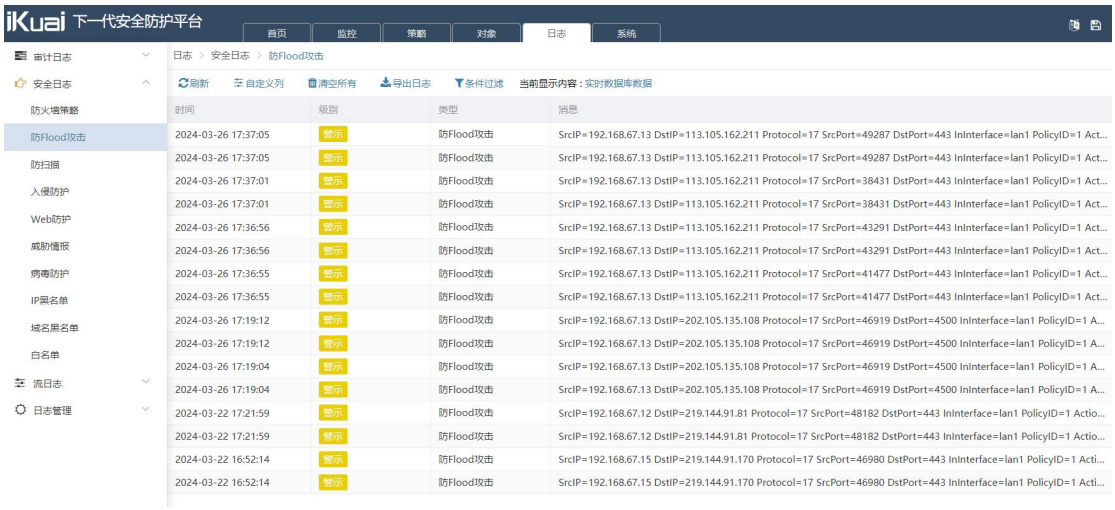
目的地址：填写筛选的目的 IP。

时间：填写筛选的时间。

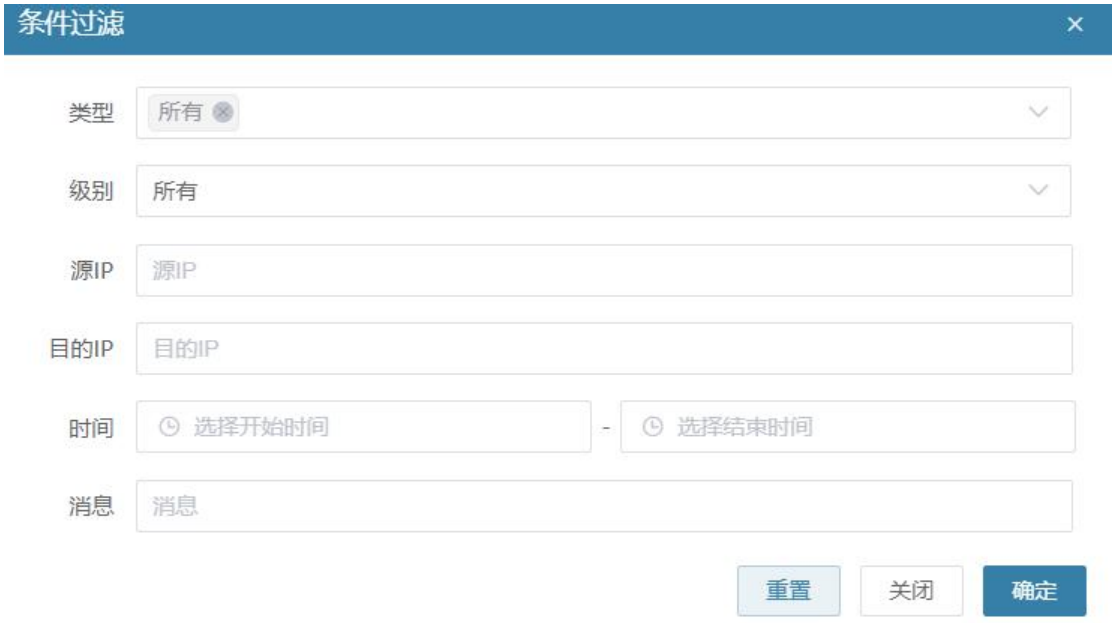
消息：填写筛选消息的详细内容。

防 Flood 攻击

防 Flood 攻击：记录 TCP、UDP、ICMP Flood 攻击攻击信息，需要在安全防护>攻击防护策略中启用防护攻击设置才能有记录信息。



可通过条件过滤，筛选具体的的日志信息。



防扫描

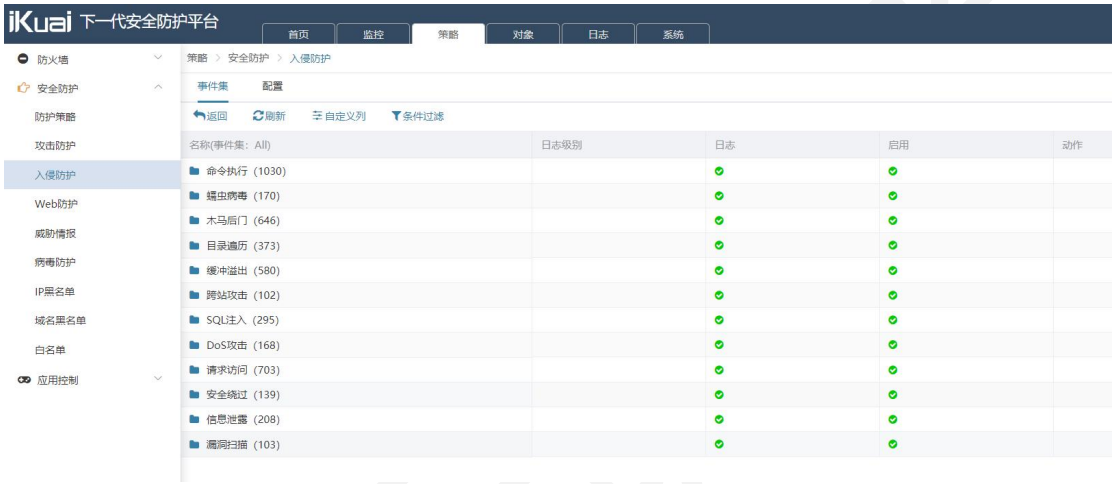
防扫描：在策略>安全防护>攻击防护中配置启用防扫描攻击后记录防扫描日志。

通过条件过滤，筛选具体的日志信息。

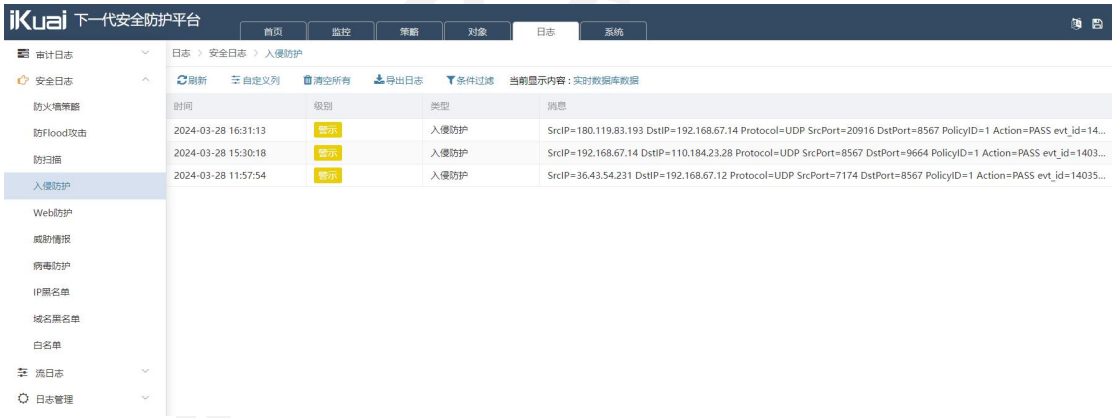
入侵防护

入侵防护利用事件特征可以检测到特定的网络行为，并可以选择放行、阻断、阻断源 ip 等动作，以达到保护网络的目的。 下一代安全防护平台设备入侵防御的事件特征库可以在某的网站上进行动态升级，以实时跟踪最新的网络威胁，保护网络的安全。

默认事件集中已开启入侵防护日志。



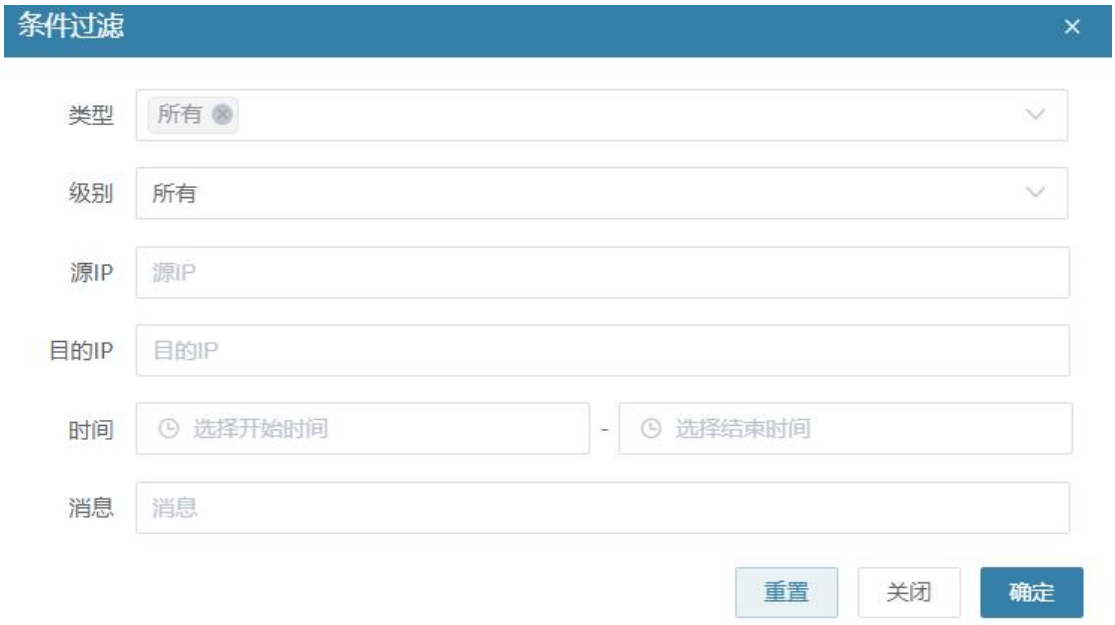
在入侵防护日志中，可查看具体的消息、基本、类型。



Web 防护

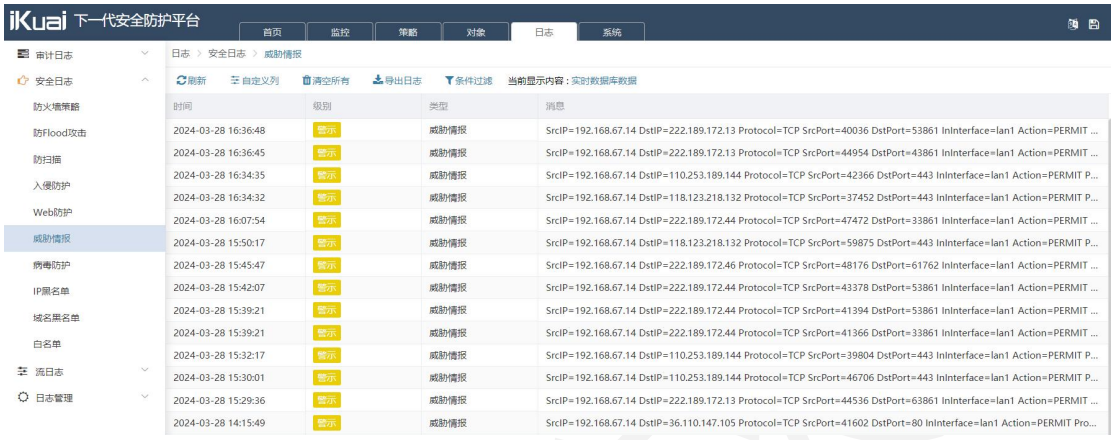
Web 防护策略防护的攻击有两种，分别是 XSS 攻击和 SQL 注入攻击。XSS 是一种经常出现在 web 应用中的计算机安全漏洞，它允许恶意 web 用户将代码植入到提供给其它用户使用的页面中，这些代码包括 HTML 代码和客户端脚本。

点击条件过滤，可对 web 防护日志进行筛选，根据需求查询所需日志。

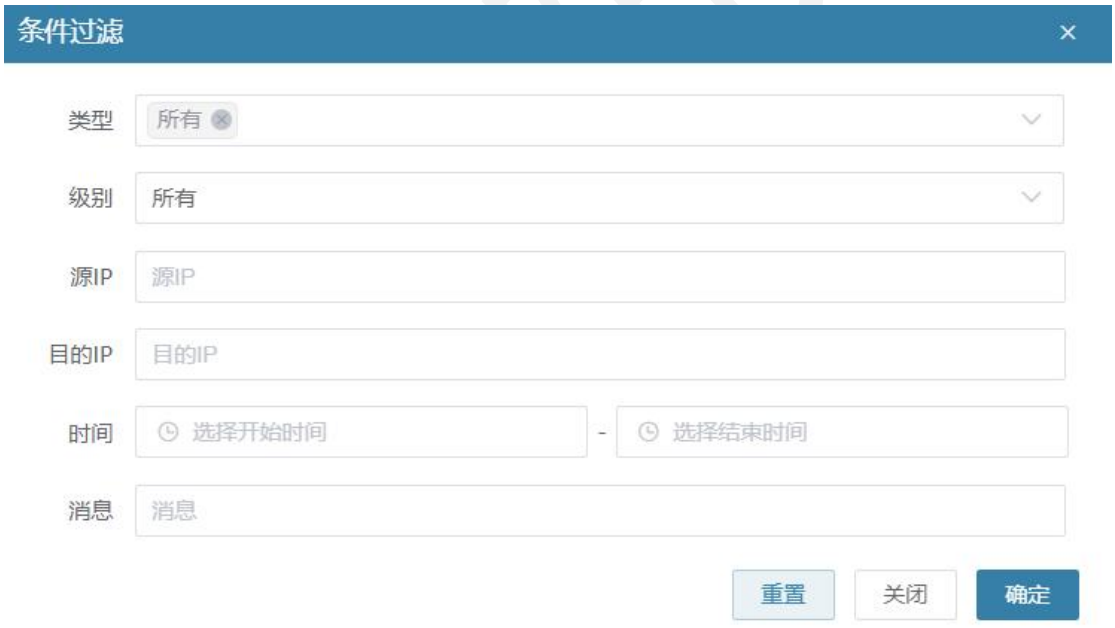


威胁情报

查看威胁情报所记录的日志详情，查看日志级别、所属类型、鼠标移到具体消息条目，可查看具体日志内容。



点击条件过滤，可对威胁情报日志进行筛选，根据需求查询所需日志。

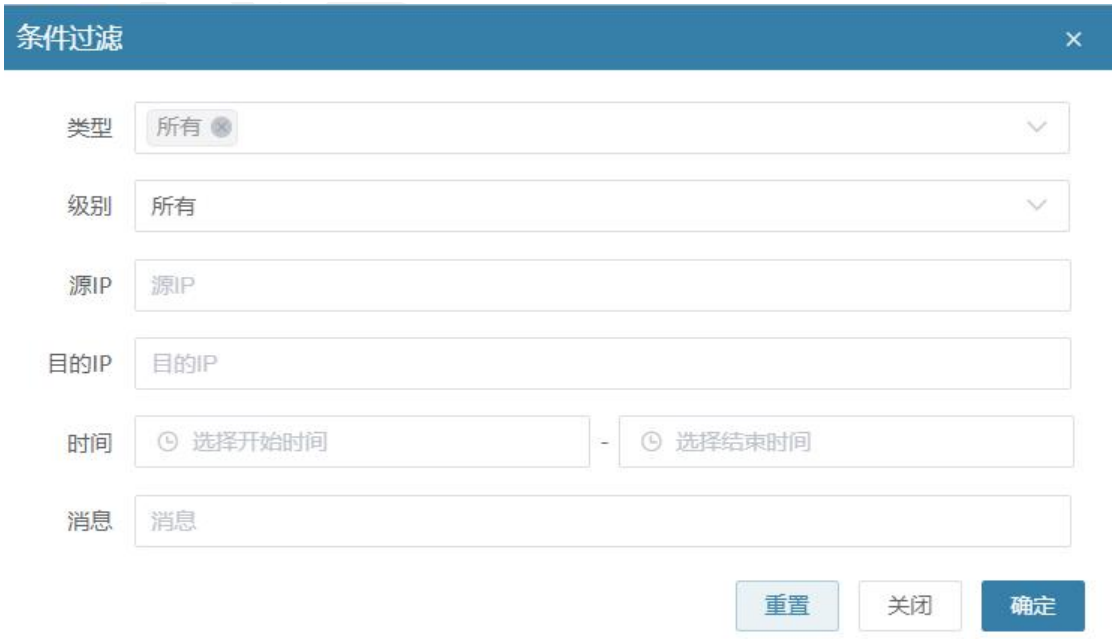


病毒防护

针对内外网入口处进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防御。同时还提供文件扫描功能，可以对特定的文件类型进行扫描。我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 应用协议时进行文件扫描。

在策略--安全防护--病毒防护中配置病毒防护协议、行为。

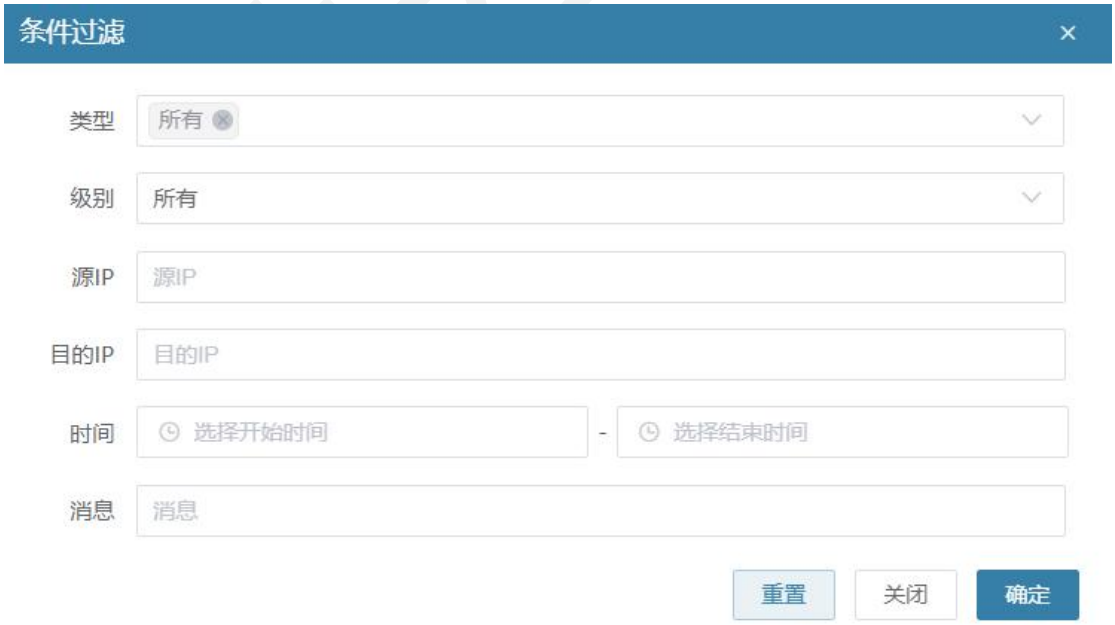
点击条件过滤，可对威胁情报日志进行筛选，根据需求查询所需日志。



IP 黑名单

针对在策略--安全防护--IP 黑名单中的配置，可在此页面查看 IP 黑名单日志。查看 IP 黑名单时间、级别、类型、具体消息。

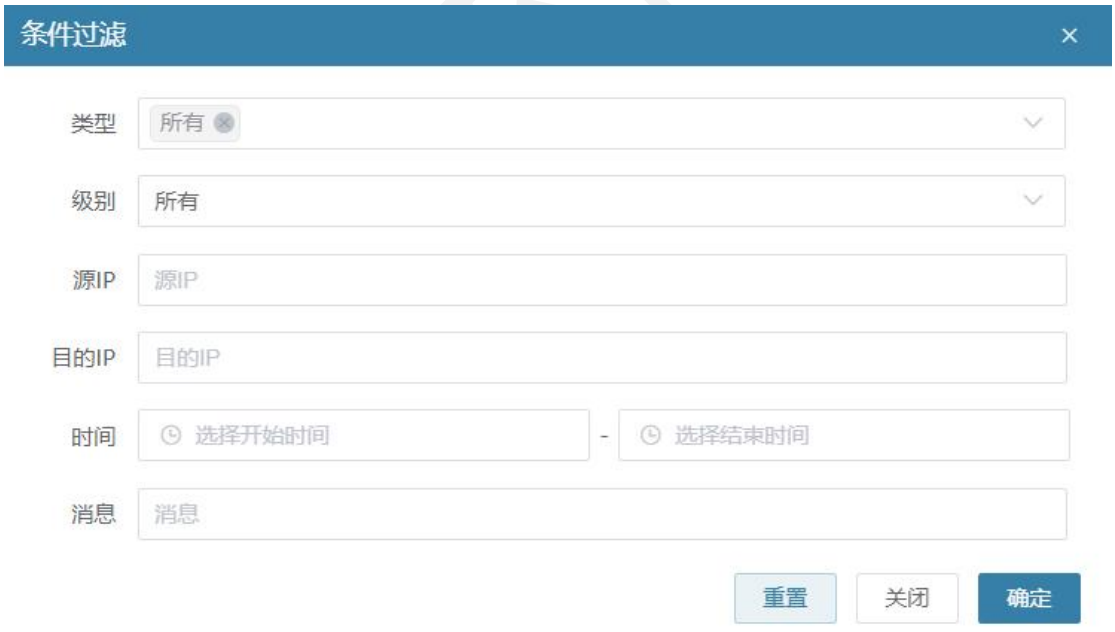
点击条件过滤，可对 IP 黑名单日志进行筛选，根据需求查询所需日志。



域名黑名单

查看在策略--安全防护--域名黑名单中添加域名，所记录的日志信息。查看日志记录的时间、日志级别、类型、具体消息。

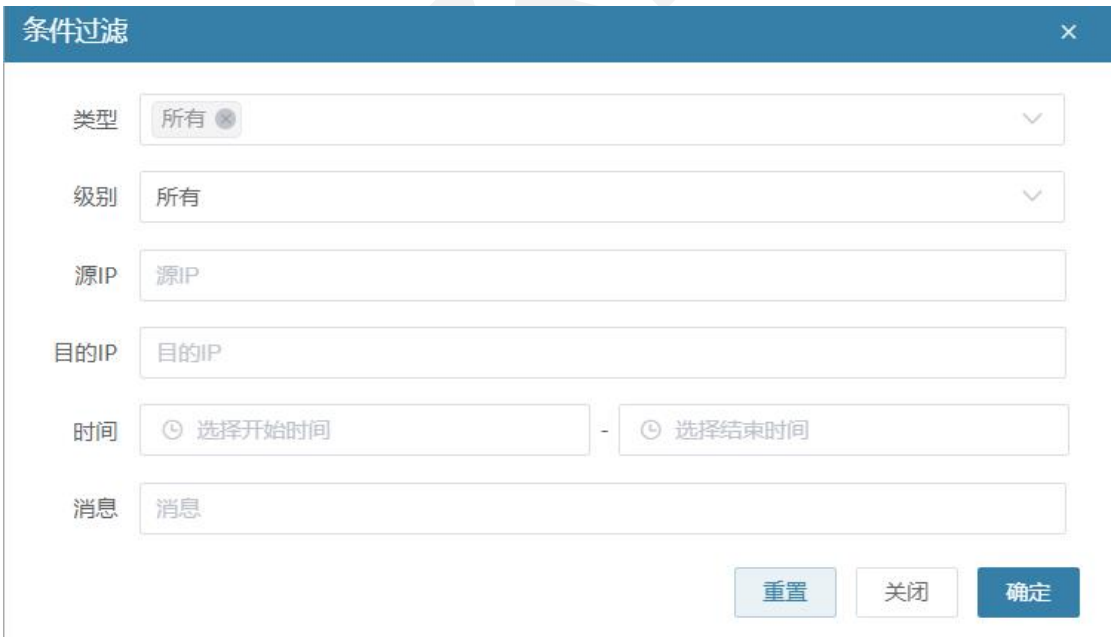
点击条件过滤，可对域名黑名单日志进行筛选，根据需求查询所需日志。



白名单

针对在策略--安全防护--白名单中的配置，可在此页面查看 IP 黑名单日志。查看白名单时间、级别、类型、具体消息。

点击条件过滤，可对白名单日志进行筛选，根据需求查询所需日志。

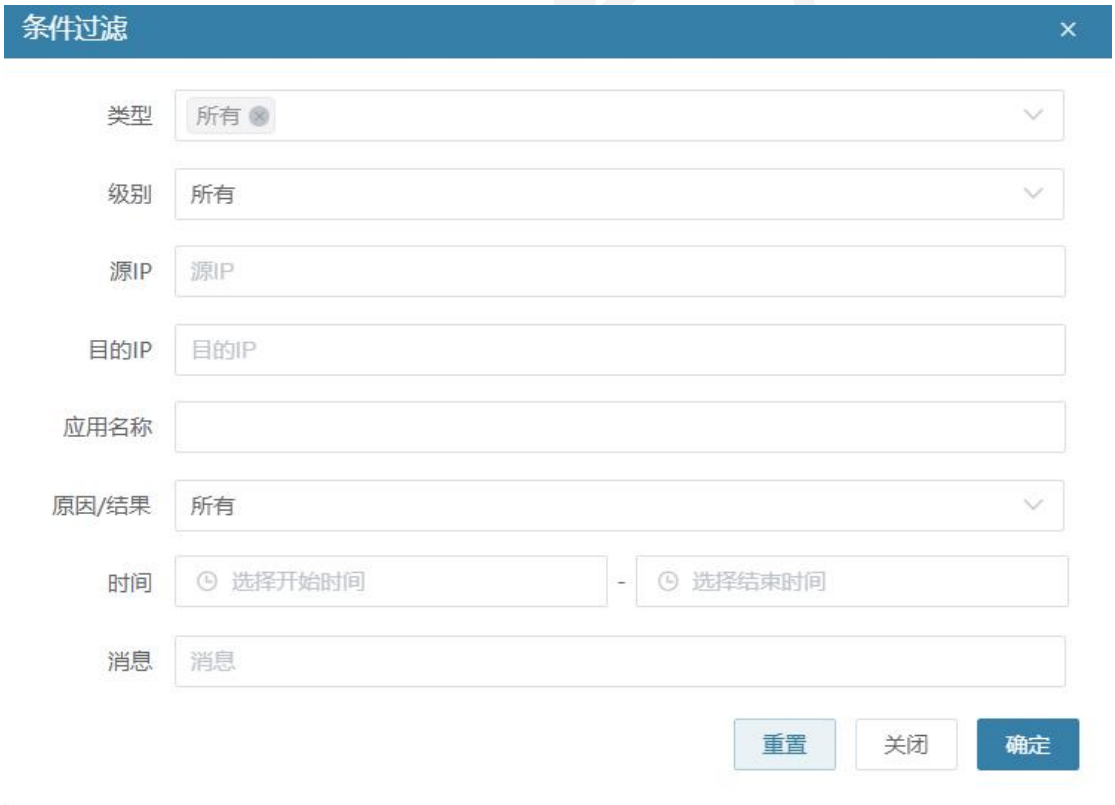


流日志

流日志

为了方便快速查看一条数据流经过设备时的详细处理信息，流日志整合了若干模块的日志信息，在这条数据流拆除的时候，生成一条日志上报。

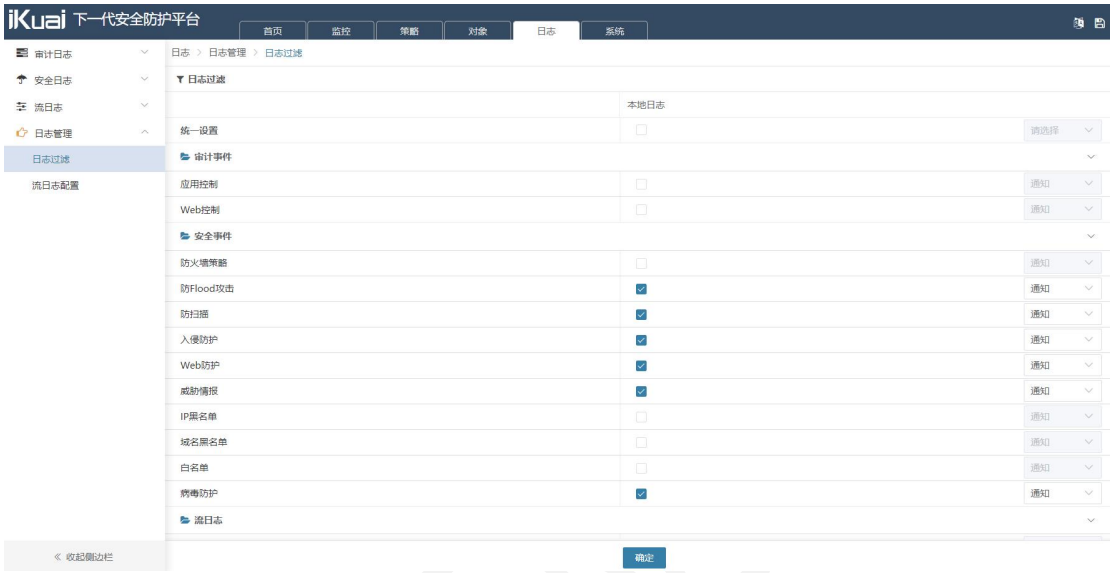
点击条件过滤，可对流日志进行筛选，根据需求查询所需日志。



日志管理

日志过滤

日志过滤：可按需求开启需要进行通知、告警等的日志级别菜单，做一个全局的设置。



参数说明：

审计事件：对应用控制、Web 控制选择开启，选择具体的告警级别。

安全事件：根据需求开启安全日志中的日志功能，选择具体的告警级别。

流日志：对流日志是否开启本地日志，选择具体的告警级别。

流日志配置

为了方便快速查看一条数据流经过设备时的详细处理信息，流日志整合了若干模块的日志信息，在此页面开启流日志配置。

系统

配置

DNS

DNS 配置：可以配置 DNS 服务器来解析设备发出的域名解析请求。

首选 DNS 服务器: 首选 dns 服务器地址。

备选 DNS 服务器: 备选 dns 服务器地址。

域名: 配置了上面的服务器地址后，可以输入一个域名进行测试，dns 服务器是否可用。在这之前应该检查是否有路由到 dns 服务器。

备份/恢复

备份恢复：可以为设备导入已有的配置，方便用户配置操作。同样可以将当前的配置导出供以后使用。

系统配置导入: 选择配置文件导入到设备中。

系统配置导出: 将设备中的配置文件导出。

设备重启

重启系统：在该页面选择重启系统选项可对系统进行重启。

版本管理

特征库版本

对特征库版本进行升级，特征库包含入侵防护特征库、应用分类特征库、URL 分类特征库，根据需求选择特征库类型，支持手动上传特征库文件手动升级，自动升级可使用默认升级服务器或指定升级服务器进行定期升级，也可支持立刻升级。升级完成后可在升级状态处查看是否升级成功。

许可管理

设备附加模块受许可(license)管理控制，如果没有导入许可，这些模块将无法配置及生效。

目前受许可管理的模块包含：**基本功能、入侵防护特征库升级、应用特征库升级、URL 分类特征库升级、威胁情报。**