天清异常流量检测系统 ADM-Detector

Web 管理用户手册

北京启明星辰信息安全技术有限公司

Beijing Venustech Cybervision Co., Ltd

二零一二年五月

版 权 声 明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京启明星辰信息安全技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京启明星辰信息安全技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦　邮编：100193

电话：010-82779088

传真：010-82779000

您可以访问启明星辰网站：www.venustech.com.cn 获得最新技术和产品信息。

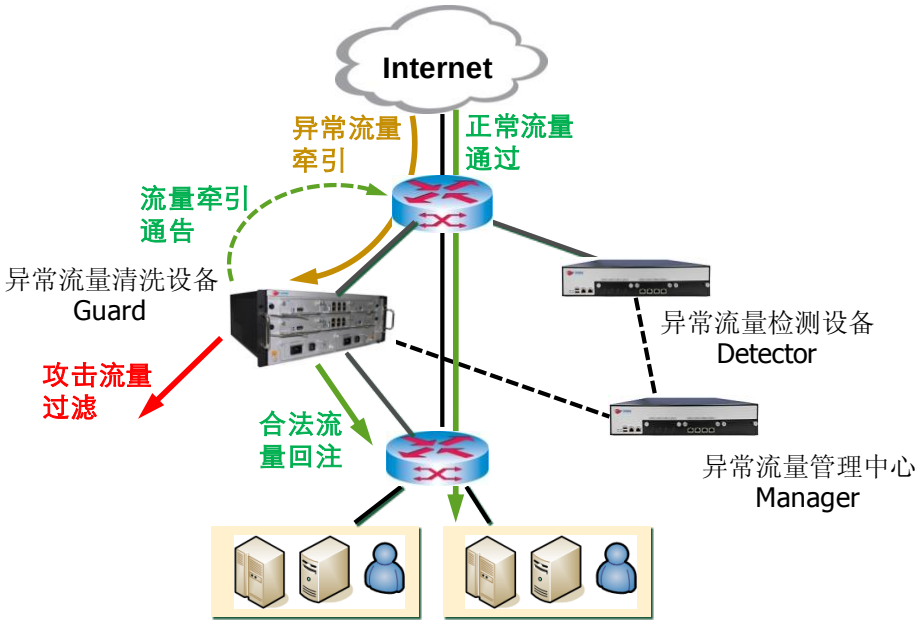
目 录

1 系统概述

1.1 概述

启明星辰的天清异常流量管理与抗拒绝服务系统(天清 ADM)由异常流量检测系统 ADM-Detector、异常流量清洗系统 ADM-Guard 和异常流量管理中心 ADM-Manager 三个模块组成：

- **异常流量检测系统（ADM-Detector，以下简称 Detector）**：通过对不同网络节点的流量进行实时关联分析，发现异常流量和 DDoS 攻击，并及时通知 Guard 对这些流量进行清洗。Detector 也可以单独使用，为用户提供全网流量可视化、DDoS 攻击告警、路由分析等功能。
- **异常流量清洗系统（ADM-Guard，以下简称 Guard）**：根据 Detector 提供的信息，完成后续对异常流量的牵引、DDoS 流量清洗、P2P 带宽控制、流量回注等。Guard 也可以单独部署，本身具备对异常流量的检测功能。
- **异常流量管理中心（ADM-Manager，以下简称 Manager）**：Guard 和 Detector 均具备自管理的能力，但在规模部署的环境中，可以通过 Manager 对多台 Guard 和 Detector 设备进行统一管理，包括检测和清洗策略下发、状态监控、系统升级、日志集中等。



其中的 Detector，除了发现异常流量外，还可用于全网的流量分析，有助于网络管理者进行网络规划、优化、监控、了解网络流量的发展趋势，依据时间、空间、特征维度进行各种分析,使用各种图形、数据等手段直观反映网络状况，为网络管理者提供必要的决策依据，为网络的正常、稳定、可靠运行提供保障。

1.2 Detector 功能介绍

Detector 产品包含如下功能组件：

1. 首页：通过图表以图形化的方式展示当前企业或组织网络的整体状况。用户可以从不同的角度了解各种实时信息。
2. 异常告警：实时展示系统检测到的流量异常和性能异常，并提供异常历史查询。
3. 监控中心：图形化展示网络关键路由，服务器节点性能状态和重要接口流量状况.
4. 流量分析：对路由设备，路由接口，服务器，主机，自治域协议，应用的流量进行分析，并展示流量成分。
5. 路由分析：路由分析是运营商用户比较关注的功能，通过分析路由消息和路由表信息，得到关于路由稳定性和合理性的结论。
6. 数据中心：数据中心提供系统流量分析数据和告警数据基于多种时间粒度、多种时间周期的存储和数据清理。
7. 日志管理：查看系统告警日志，流量日志，系统日志。
8. 报表管理：以统计报表或报告的方式对网络流量进行分析、展示。
9. 配置：可以对设备进行管理，合理定制运行参数，通过多种配置组合，确保系统满足实际需求。
10. 权限设置：采用基于角色的权限管理机制，来支持对用户访问系统进行权限控制。

1.3 名词解释

异常流量

有限的带宽资源承载着非预期的流量，定义为异常流量。

流量型攻击

分布式拒绝服务攻击(DDoS)是目前黑客经常采用而难以防范的攻击手段。

僵尸网络

Botnet 是指采用一种或多种传播手段，将大量主机感染 bot 程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。

DFI

一种基于流量行为的应用识别技术。

DPI

即 DPI(Deep Packet Inspection)深度包检测技术是一种基于应用层的流量检测和控制技术，当 IP 数据包、TCP 或 UDP 数据流通过基于 DPI 技术的带宽管理系统时，该系统通过深入读取 IP 包载荷的内容来对 OSI 七层协议中的应用层信息进行重组，从而得到整个应用程序的内容，然后按照系统定义的管理策略对流量进行整形操作。

Flow

7 个关键字段标示无方向的连接【IPsrc , IPdst , srcPort , dstPort , protocol , TOS , Ifindex】。

日志

设备自身产生的记录、告警等信息

设备

系统中用来产生日志的设备，具备 IP，例如安全设备、网络设备、主机系统等

基线

指在不同流量特征的基础上创建的流量检测基准模型

内网

指用户关注的网络区域内部，由配置的路由器下行接口和检测范围决定

外网

指用户关注的网络区域以外的部分。由配置的路由器上行接口决定

异常检测插件

每个插件包括一个或多个使用同一类基线模型的检测算法。只有插件处在启用的状态下才能启用插件中的算法

检测算法

一种算法会使用一种流量检测基准模型，一种告警类型会有一个或多个算法

检测模式

指检测算法依据的流量类型

IP 规则组

IP 规则组主要应用于告警检测中，对不同的 IP 规则组采取不同的检测参数，属于 IP 规则组中的 IP 将自动被认为是被保护 IP。IP 规则组分为两类：手工规则组和动态规则组

自治域对照表

自治域指的是使用同一种路由协议、相互连接的路由设备组成的网络区域，自治域列表

应用端口对照表

应用/端口是由系统预设或用户自定义的若干个协议端口/端口段的组合，一般情况下，一类应用或者应用协议（如 http、ftp 等）的常用端口可以归并为一个应用/端口

IP 资产对照表

当前资产设备的 IP 地址（IP 地址段）和其描述信息的对应表

流量过滤器

流量过滤器可以针对 IP 范围、路由器接口、自治域或应用协议等条件配置内外网监控条件，统计详细的流量信息（包括总流量及 TOP N 流量）。一般情况下，对需要重点监控的区域配置流量过滤器并对其进行监控

流量牵引策略

异常流量缓解方案

流量分析

对监控对象的流量进行分析，并展示流量成分

路由分析

从多个角度分析路由的稳定性

1.4 管理 Detector

命令行管理

Detector 可以通过超级终端连接设备的串口进行基本的设置，包括：配置设备的网络属性（IP 路由等）、启动停止、恢复出厂设置等。

WEB 管理

Detector 采用 B/S 架构设计，方便用户管理。

WEB 访问推荐使用 IE7.0 及以上版本、Mozilla Firefox10 及以上版本浏览器，最佳显示分辨率为 1024×768。

在浏览器地址栏输入： http://*SERVER_IP*:8888/ta 即可以访问系统。

如果系统支持 SSL，则在浏览器地址栏输入： https:// *SERVER_IP* :8443/ta 访问系统。

系统界面组成:

1. 导航栏：系统导航栏，模块功能列表。
2. 配置按钮：点击可以配置管理面板。
3. 工具栏：全屏、告警提示框开关、换肤、帮助、当前用户信息、退出系统。
4. 管理面板：管理面板区域，点击导航栏时，不同模块的内容展示区域。
5. 模块最小化图标：以前查看过的模块的最小化图标，点击可以重新打开，列表中最多可以显示 10 个，点击右侧的关闭图标，可以关掉当前窗口。
6. 服务器时间及当前用户信息。
7. License 信息：显示当前系统拥有的 License 信息。

系统默认配置

系统默认的设备管理 IP 地址为：10.0.0.1

系统的默认登录用户名用口令为：root/venus.root，请登录系统后及时修改。

此外，系统还内置了以下三个角色与用户，登录后请首先修改口令：

系统管理员：具备系统配置，日志审计操作的权限，对应的内置用户名与口令为：sysadmin/venus.sysadmin。

用户管理员：具备用户管理和权限管理操作的权限，对应的内置用户名与口令为：useradmin/venus.useradmin。

审计管理员：具备对系统操作进行审计的权限，对应的内置用户名与口令为：auditor/venus.auditor。

注：系统目前推荐的客户端浏览器版本为：IE7/IE8。

2 首页

2.1 导航栏

导航栏显示系统各功能模块的图标，点击可以进入该功能模块并显示该功能模块的管理面板。

系统预定义了一些功能模块，但用户可以自定义管理面板，并将其放在导航栏上，具体配置方法请参考下面的【管理面板】部分。

2.2 管理面板

管理面板是当点击导航栏上的不同模块时，该模块的内容展示区域。管理面板可以将多个不同的组件组合起来，在同一个页面进行展示。系统内置了一些预定义的管理面板，用户还可以自定义管理面板。

2.2.1 默认面板

初始化的系统预定义了一个默认的管理面板，在导航栏中的名称为【首页】。首页的内容包括：

1. 最近 30 分钟告警状态

以预警事件图的方式显示最近 30 分钟的告警状态。

预警雷达圆形区域中的点表示告警的 IP 地址，采用 IP 地址子网地址和主机地址来定位具体位置，实际按照 IP 地址的最后两位来定位。圆周角度和半径值分别表示定位的两个坐标，圆周的角度作为横坐标，半径作为纵坐标，将圆周角度等分为 255 份，将 IP 地址的倒数第二位的值作为横坐标，圆形区域的 Y 轴坐标（半径）分为 9 等份，每一等份的点表示 30 个 IP 地址，因此从内到外的 9 个点分别表示的数值为 1-30，31-60，....，240-255。例如 10.50.10.1，10 对应圆周 X 轴，1 对应圆形半径 Y 轴，这样同一子网内的地址就会显示在同一个半径的区域内。

以点的颜色表示在 30 分钟内相关设备的最高的告警等级。

鼠标移动到点上，会以 tooltips 的方式显示该点相关的设备的最近 10 条告警信息。

2. 最近 60 分钟 Top 地址流量
3. 30 分钟内最近 10 条告警

以表格的方式显示最近 30 分钟最近 10 条告警。

4. 最近 30 分钟 TOP 协议流量
5. 最近 24 小时流量告警类型分布

以柱状图显示最近 24 小时告警类型分布。

2.3 工具按钮

工具按钮栏位于首页的右上角，包括的操作有：

- 全屏开关：切换系统是否全屏显示（全屏显示不会使 IE 全屏，IE 全屏请按 F11）
- 告警提示框开关：当用户在规则的告警动作中设置了弹出对话框时，如果有告警，首页会弹出提示框，此处可以选择是否不再弹出对话框
- 换肤：系统换肤功能(换肤后需要重新登录)
- 帮助：在线帮助
- 帐户：可以修改当前用户的个人信息
- 退出登录：退出当前系统，进入重新登录页面

2.4 模块最小化

模块最小化区域位于系统的左下角，用户以前查看过的模块，系统并不会关掉，只会以图标的方式显示在此处，点击图标可以重新打开。

点击右侧的关闭图标，可以关掉当前窗口。

注：列表中最多可以显示 10 个最小化图标。

3 异常

实时展示系统检测到的流量异常和性能异常,并提供异常历史查询。

流量告警主要以图表和列表信息的方式进行展现。

- 图表主要包括线性区域图和柱状分类图
- 图表的统计时间为当日的零点至当前时刻(最晚为当日的 23:59:59.999)
- 流量告警的线性区域图的将统计所有针对流量的告警, 并按高(红色),中(黄色),低(绿色)进行区分
- 柱状分类图类别为流量主要类型.并按高(红色),中(黄色),低(绿色)进行区分
- 页面下方展示的列表查询时间为当日的零点至当前时刻(最晚为当日的 23:59:59.999)
- 单条告警可以进行透视操作,并可以查询单条告警的详细信息,页面的图表列表统一实时刷新

3.1 流量告警类型

3.1.1 DDOS 攻击

告警子类型包括:

- SYN Flood 攻击
- ACK Flood 攻击
- ICMP Flood 攻击
- HTTP Get Flood 攻击
- LAND Flood 攻击
- IGMP Flood 攻击
- TCP Flag NULL
- TCP Flag 误用
- Protocol NULL
- UDP Flood 攻击

3.1.2 蠕虫事件

告警子类型包括:

- Code Red
- 硬盘杀手
- Drive killer
- SQL Slammer

- 冲击波 Shock wave
- 冲击波杀手
- ND Flood 攻击
- 震荡波 Zhentang wave
- 邮件蠕虫 Mail worm
- WinNuke 攻击

3.1.3 流量超长

告警子类型包括:

- Bps 超常
- Pps 超常
- 会话数超常
- Session number

3.1.4 协议比例异常

告警子类型包括:

- Tcp 比例异常
- UDP 异常
- ICMP 异常
- IGMP 异常

3.1.5 流量分布异常

告警子类型包括:

- 源地址分散度异常
- 目的地址分散度异常
- 端口分散度异常

3.1.6 网络误用

告警子类型包括:

- 私有 IP 异常
- Dark IP 异常

3.1.7 僵尸网络异常

3.1.8 DNS 攻击

告警子类型包括:

- DNS Query Flood
- DNS Response Flood
- DNS 畸形报文攻击
- DNS 随机域名攻击
- DNS 投毒检测

3.1.9 自定义异常

可以自定义告警子类型

3.2 性能告警类型

3.2.1 可用性异常

告警子类型包括:

- SNMP 数据中断
- Flow 中断
- Ping 不可达

3.2.2 性能异常

告警子类型包括:

- CPU 阈值
- 内存阈值
- 带宽使用率阈值
- 磁盘使用率阈值

3.2.3 告警查询

告警查询的作用即查询所有的告警信息,罗列几乎所有的常用查询条件,主要分为基本查询条件,流量查询条件和性能查询条件三个大类:

基本查询条件包括:

- 时间条件:(30 分钟/ 1 小时/ 1 天/ 7 天/ 30 天/ 90 天/ 自定义)其中自定义为可以自行选择查询时间.
- 告警 ID: 可以输入多个告警 ID
- 告警来源:可以输入多个告警 IP
- 告警级别:高 中 低 三个级别进行组合
- 正在持续:复选框勾选即为持续,不勾选为查询全部

流量查询条件包括:(选中类别,即可弹出查询条件)

- 流量告警类型：所有流量告警的主要告警类型.(选中复选框,可以弹出对应的告警子类型)
- 告警方向：攻击 被攻击 进行选择组合
- 路由设备：添加的路由设备进行组合(选中复选框,可以弹出对应的路由接口)

性能查询条件包括：(选中类别,即可弹出查询条件)

- 性能告警类型：所有性能告警的主要告警类型.(选中复选框,可以弹出对应的告警子类型)
- 点击查询即可进入查询页面,查询页面由图表和列表组成,图表为线性区域图,列表单条告警可以查看详细.

3.3 告警透视

告警透视是告警与预定义基线参数阀值进行比较的分析功能.

3.3.1 流量告警透视

1、点击流量告警监控列表的右侧【透视】按钮，会将透视页面在上面的 tab 也中进行打开。

2、在告警透视页面中，(基线参数中的高中低阈值)

流量透视图中，由基础线，动态流量线组成，基础线由基线参数配置中获得（高中低级阀值），基础线表示前 30 分钟到当前时间的一段时间的流量展示。

点击流量分析图右上角的【bps】，会将流量分析图切换 bps 分析并将下面分析数据进行切换；

点击流量分析图右上角的【pps】，会将流量分析图切换 pps 分析并将下面分析数据进行切换

点击流量分析图右上角的【sps】，会将流量分析图切换 sps 分析并将下面分析数据进行切换；

3、分析数据：

告警信息：告警类型，告警原因，严重程度（高级为红色，中级为橘黄色，低级为绿色），方向，开始时间，持续时间，状态，告警来源；

统计数据：总字节数，总包数，总回话数，流量峰值（bps/pps/sps）；

相应处理：动作，创建时间，牵引时间；

数据不存在是显示为空。

3.3.2 性能告警透视

1、点击性能告警监控列表的右侧【透视】按钮，会将透视页面在上面的 tab 也中进行打开。

2、性能透视图中将存在已经配置好的 CPU 高中低阈值作为基础线（配置参见性能异常

告警配置）进行展示，cpu 利用率将会作为动态线浮动在基础线上。

3、分析数据：

告警信息：告警类型，告警原因，严重程度（高级为红色，中级为橘黄色，低级为绿色），方向，开始时间，持续时间，状态，告警来源；

4 监控

图形化展示网络关键路由,服务器节点性能状态和重要接口流量状况,默认将展示所有的路由器设备。

在拓扑视图中，点击路由设备，将展示设备地址，CPU 利用率，路由总流量的信息并每隔 30 秒刷新一次.

4.1 新增路由设备

点击左上角的【新增路由设备】按钮，弹出新增路由设备页面, 路由设备属性包括：

- 是否启用（勾选为启用）
- 设备地址
- 设备名称
- 厂家
- flow 版本
- snmp 版本
- snmp 端口
- SNMP Community
- 描述

4.2 关注设备接口

关注接口功能是使用图形化方式展示设备某接口的流量状况.

点击页面左上角的【关注接口】,会弹出新增关注接口页面,如果点选的设备是启用状态,则可以选择路由器的接口.

关注接口属性包括:

- 接口名称（设备对应的接口）
- 关联子网名称
- X,Y 轴坐标

在关注接口中，点选的路由设备是停用状态，提示无可用接口并不允许用户添加改关注接口.

4.3 删除设备或关注接口

选中设备或关注接口,点击左上角的【删除】按钮，将弹出是否删除的对话框，点击删除对话框的【确定】按钮，会将选中的设备进行删除且无法恢复。

4.4 设备详细信息查看

在拓扑视图中，双击设备图标，将在页面上面弹出 tab 页，将设备的详细信息进行展示。

4.5 布局调整

可以手动调整拓视图中设备和关注接口的位置,使其布局更加美观。

在拓扑视图中，拖动设备摆放在不同的位置后，点击左上角的【保存】的按钮，将对本次布局进行保存，保存成功后将弹出对话框提示保存成功。

5 流量分析

流量分析是有助于网络管理者进行网络规划、优化、监控、了解网络流量的发展趋势，通过对网络中多角度，多纬度，依据时间、空间、特征为基础，通过各种分析机制、依据各种图形、数据等手段直观反映网络中状况，直观的反应网络中运行状况为网络管理者提供必要的数据信息，为网络的正常、稳定、可靠运行提供保障。流量分析是基于时间纬度围绕三个方面的内容：流量的来源与去向、流量的组成成分、流量的变化趋势进行分析

分析对象分别是路由设备、路由设备组、路由器接口组、服务器流量群组、主机、自治域

5.1 路由设备

点击 【路由设备】 分组进入所有路由设备流量分析页面，点击展开路由设备分组，列出所有路由设备名称，点击路由器名称进入该路由设备流量分析页面，默认展示该路由设备在最近 30 分钟内的总流量趋势。

主要功能包括：

5.1.1 总流量分析

显示流经所有路由器设备或单个路由器设备的总流量按时间变化的流量趋势。此流量图分为上下两个区域图，上面的区域图代表流入路由器设备的流量，下面的区域图代表流出路由器设备的流量，对于每一个路由器设备的入流量和出流量上下对应。关于流入路由器设备的流量和流出路由器设备的流量的计算是根据路由器的上行流量和下行流量得来。如果当前路由流量定义选择第一种方案：则上行流量的计算为：上行口 OUTPUT 流量和，下行流量的计算为：上行口 INPUT 流量和。如果当前路由流量定义选择第二种方案：则上行流量的计算为：上行口 OUTPUT 流量和，下行流量的计算为：下行口 OUTPUT 流量和。

- 路由设备的总流量趋势图

根据查询条件，该流量图展示了所有路由器设备或单个路由器设备在所选的时间范围内的所选流量定义方案的总流量趋势。通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。默认为距当前时间最近的 30 分钟的流量。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

- 路由设备的总流量数据列表

根据查询条件，分别列出了当前流量趋势图上的每个路由器设备在所选时间段内的流

量当前值，平均值，最大值。每个数值均以 bps、pps 和 sps 三种单位显示。每种单位分别显示出流量的值，入流量的值，总流量的值以及总流量占所有总流量的百分比。

5.1.2 路由器分析

列出流经每台路由器设备的总流量按时间变化的流量趋势。关于每台路由器设备的总流量参照所有路由器总流量的分析方法。

- 路由设备的总流量趋势图

根据查询条件，该流量图展示了每个路由器设备在所选的时间范围内的所选流量定义方案的总流量趋势。该流量图分为上下两部分区域图，上部分区域图展示流入每一台路由器设备的流量趋势图，下部分区域图展示从每一台路由器设备流出的流量趋势图。通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。默认为距当前时间最近的 30 分钟的流量。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

- 路由设备的总流量数据列表

根据自定义的查询条件，分别列出了当前流量趋势图上的每个路由器设备在所选时间段内的流量当前值，平均值，最大值。每个数值均以 bps、pps 和 sps 三种单位显示。每种单位分别显示出流量的值，入流量的值，总流量的值以及总流量占所有总流量的百分比。

5.1.3 路由接口分析

展示当前路由器设备下的每一个接口随时间变化的总流量趋势图。

- 路由接口趋势图

该流量图分为上下两部分，上部分区域图展示从当前路由器的每个接口流入的流量趋势图，下部分趋势图展示从当前路由器的每个接口流出的流量趋势图。默认为距当前时间最近的 30 分钟的流量。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

- 路由接口流量数据列表

根据查询条件，分别列出了当前流量趋势图上的当前路由器设备在所选时间段内的接口流量的当前值，平均值，最大值。每个数值均以 bps、pps 和 sps 三种单位显示。每种单位分别显示出流量的值，入流量的值，总流量的值以及总流量占所有总流量的百分比。

5.1.4 Top 地址分析

展示通过所有路由器设备或单个路由器设备的源/目的 Ip 随时间变化的流量趋势 Top5，

包括源 Ip 地址和目的 Ip 地址。

- 路由设备的 Top5 地址趋势图

根据查询条件，该图展示了路由设备在所选时间范围内的所选流量定义方案 TOP5 源/目的地址的流量趋势。分为两个图，一张为源 Ip 地址的流量趋势图，另一张为目的 Ip 地址的流量趋势图。针对每张流量图都分为上下区域图，通过点击右上方的源 Ip 地址链接（默认），Top5 地址为流经所有器或单个路由器的流量最大的前 5 个源 Ip 地址，则上面的流量区域图展示的是流入 Top5 地址的流量随时间变化的趋势图，下面的流量趋势图展示的是流出 Top5 地址的流量随时间变化的趋势图。如果用户点击目的 Ip 地址链接，Top5 地址为流经所有路由器或单个路由器的流量最大的前 5 个目的源 Ip 地址，则上面的流量区域图展示的是流入 Top5 地址的流量随时间变化的趋势图，下面的流量趋势图展示的是流出 Top5 地址的流量随时间变化的趋势图。通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

- 路由设备的 Top5 地址流量数据列表

根据自定义查询条件，分别列出了路由设备在所选时间范围内的所选流量定义方案的 Top5 源/目的地址的流量大小，包括当前值、平均值、最大值，每个数值均以 bps、pps 和 pps 三种单位显示。当用户点击右上方的源 Ip 地址链接（默认）时，显示的列表为 Top5 源地址列表，当用户点击右上方的目的 Ip 地址链接时，显示的列表为 Top 目的地址列表。

5.1.5 Top 应用分析

展示通过所有路由器的应用随时间变化的流量趋势 Top5。关于应用的趋势图分为上下区域图，上面的区域图表示流入路由器的应用的流量随时间变化的趋势图，下面的区域图表示的是流出路由器的应用的流量随时间变化的趋势图。通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

- 路由设备的 Top5 应用趋势图

根据自定义查询条件，该图展示了路由设备在所选时间范围内的所选流量定义方案 Top 应用的流量趋势。通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

- 路由设备的 Top5 应用流量数据列表

根据自定义查询条件，分别列出了路由设备在所选时间范围内的所选流量定义方案的 Top5 应用的流量大小，包括当前值、平均值、最大值，每个数值均以 bps、pps 和 pps 三种单位显示。

5.1.6 Top 协议分析

展示通过所有路由器的协议随时间变化的流量趋势 Top5。关于应用的趋势图分为上下区域图，上面的区域图表示流入路由器的协议的流量随时间变化的趋势图，下面的区域图表示的是流出路由器的应用的流量随时间变化的趋势图。

- 路由设备的 Top5 协议趋势图

根据自定义查询条件，该图展示了路由设备在所选时间范围内的所选流量定义方案 Top 协议的流量趋势。通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

- 路由设备的 Top5 协议流量数据列表

根据自定义查询条件，分别列出了路由设备在所选时间范围内的所选流量定义方案的 Top5 的流量大小，包括当前值、平均值、最大值，每个数值均以 bps、pps 和 pps 三种单位显示。

5.1.7 Top 自治域分析

根据自定义查询条件，该图展示了路由设备在所选时间范围内的所选流量定义方案 TOP5 源/目的自治域的流量趋势。分为两个图，一张为源自治域的流量趋势图，另一个为目的自治域的流量趋势图。针对每个流量图都分为上下区域图，通过点击右上方的源自治域链接（默认），Top5 自治域为流经所有器或单个路由器的流量最大的前 5 个源自治域，则上面的流量区域图展示的是流入 Top5 自治域的流量随时间变化的趋势图，下面的流量趋势图展示的是流出 Top5 自治域的流量随时间变化的趋势图。如果用户点击目的自治域链接，Top5 自治域为流经所有路由器或单个路由器的流量最大的前 5 个目的自治域，则上面的流量区域图展示的是流入 Top5 自治域的流量随时间变化的趋势图，下面的流量趋势图展示的是流出 Top5 自治域的流量随时间变化的趋势图。通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

- 路由设备的 Top5 地址流量数据列表

根据自定义查询条件，分别列出了路由设备在所选时间范围内的所选流量定义方案的 Top5 源/目的自治域的流量大小，包括当前值、平均值、最大值，每个数值均以 bps、pps 和 pps 三种单位显示。当用户点击右上方的源自治域链接（默认）时，显示的列表为 Top5 源自治域的流量数据列表，当用户点击右上方的目的自治域链接时，显示的列表为 Top 目的

自治域的流量数据列表。

5.2 路由设备接口

展开“路由设备”，再展开某个路由设备的名称，单击某个接口名称，即可在页面右侧查看当前设备下的当前接口的流量信息。

5.2.1 总流量分析

展示当前设备下的当前接口的总流量按时间变化的流量趋势，路由设备接口的总流量分析查看方法，与路由设备的基本相同。

5.2.2 Top 地址分析

展示当前设备下的当前接口的 Top5 地址按时间变化的流量趋势，路由设备接口的 Top 地址分析查看方法与路由设备的基本相同。

5.2.3 Top 应用分析

展示当前设备下的当前接口的 Top5 应用按时间变化的流量趋势，路由设备接口的 Top 应用分析查看方法与路由设备的基本相同。

5.2.4 Top 协议分析

展示当前设备下的当前接口的 Top5 协议按时间变化的流量趋势，路由设备接口的 Top 协议分析查看方法与路由设备的基本相同。

5.2.5 Top 自治域分析

展示当前设备下的当前接口的 Top5 自治域按时间变化的流量趋势，路由设备接口的 Top 自治域分析查看方法与路由设备的基本相同。

5.3 服务器

点击 【服务器】进入所有服务器流量分析页面，默认展示该所有服务器在最近 30 分钟内的总流量趋势。点击展开服务器分组，列出所有服务器名称，点击服务器名称进入该服务器流量分析页面，默认展示该所有服务器在最近 30 分钟内的总流量趋势。

主要功能包括以下功能：

5.3.1 总流量

如果点击【服务器】进入所有服务器流量分析页面，点击【总流量】tab 页，则显示所有服务器的在最近 30 分钟的流量随时间变化的趋势图，关于总流量的分析方法可以参照路由器总流量的分析方法。流量数据列表展示的是最近 30 分钟内的所有服务器总流量的当前值，平均值，最大值。如果展开【服务器】显示所有服务器的名称，点击某一个服务器进入当前服务器流量分析页面，点击【总流量】tab 页，则显示当前服务器的在最近 30 分钟的流量随时间变化的趋势图，关于总流量的分析方法可以参照路由器总流量的分析方法。流量数据列表展示的是最近 30 分钟内的当前服务器总流量的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入服务器的流量，下部分区域图为流出服务器的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.3.2 服务器

点击【服务器】进入所有服务器流量分析页面，点击【服务器】tab 页，显示在最近 30 分钟内每个服务器随时间变化的流量趋势图。流量数据列表展示的是最近 30 分钟内的当前服务器总流量的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入每个服务器的流量，下部分区域图为流出每个服务器的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看每个服务器的流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.3.3 Top 地址

如果点击【服务器】进入所有服务器流量分析页面，点击【Top 地址】tab 页，则显示所有服务器的在最近 30 分钟的源 Top10 地址流量随时间变化的趋势图，关于 Top 地址的分析方法可以参照路由器 Top 地址的分析方法。流量数据列表展示的是最近 30 分钟内的所有服务器源 Top10 地址的当前值，平均值，最大值。如果展开【服务器】显示所有服务器的名称，点击某一个服务器进入当前服务器流量分析页面，点击【Top 地址】tab 页，则显示当前服务器的在最近 30 分钟的源 Top10 地址流量随时间变化的趋势图，关于 Top 地址的分析方法可以参照路由器 Top 地址的分析方法。流量数据列表展示的是最近 30 分钟内的当前服

务器源 Top10 地址的当前值，平均值，最大值。

默认的流量图为流入服务器的 Top10 源地址流量图。

如果用户点击流量趋势图上方的【目的地址】超链接，则流量图和流量数据列表展示的目的 Top10 地址的流量。流量图为流出服务器的 Top10 目的地址流量图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top10 地址流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.3.4 Top 应用

如果点击【服务器】进入所有服务器流量分析页面，点击【Top 应用】tab 页，则显示所有服务器的在最近 30 分钟的 Top5 应用流量随时间变化的趋势图，关于 Top 应用的分析方法可以参照路由器 Top 应用的分析方法。流量数据列表展示的是最近 30 分钟内的所有服务器 Top5 应用的当前值，平均值，最大值。如果展开【服务器】显示所有服务器的名称，点击某一个服务器进入当前服务器流量分析页面，点击【Top 应用】tab 页，则显示当前服务器的在最近 30 分钟的 Top5 应用流量随时间变化的趋势图，关于 Top 应用的分析方法可以参照路由器 Top 应用的分析方法。流量数据列表展示的是最近 30 分钟内的当前服务器 Top5 应用的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入每个服务器的 Top5 应用的流量，下部分区域图为流出每个服务器的 Top5 应用的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top5 应用流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.3.5 Top 协议

如果点击【服务器】进入所有服务器流量分析页面，点击【Top 协议】tab 页，则显示所有服务器的在最近 30 分钟的 Top5 协议流量随时间变化的趋势图，关于 Top 协议的分析方法可以参照路由器 Top 协议的分析方法。流量数据列表展示的是最近 30 分钟内的所有服务器 Top 协议的当前值，平均值，最大值。如果展开【服务器】显示所有服务器的名称，点击某一个服务器进入当前服务器流量分析页面，点击【Top 协议】tab 页，则显示当前服务器的在最近 30 分钟的 Top5 协议流量随时间变化的趋势图，关于 Top 协议的分析方法可以参照路由器 Top 协议的分析方法。流量数据列表展示的是最近 30 分钟内的当前服务器 Top5 协议的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入每个服务器的 Top5 协议的流量，下部分区域图为流出每个服务器的 Top5 协议的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top5 协议流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.4 路由器组

点击 【路由器组】进入所有路由器组流量分析页面，默认展示该所有路由器组在最近 30 分钟内的总流量趋势。点击展开路由器组分组，列出所有路由器组名称，点击路由器组名称进入该路由器组流量分析页面，默认展示当前路由器组在最近 30 分钟内的总流量趋势。

主要功能包括以下功能：

5.4.1 总流量

如果点击【路由器组】进入所有路由器组流量分析页面，点击【总流量】tab 页，则显示所有路由器组的在最近 30 分钟的流量随时间变化的趋势图，关于总流量的分析方法可以参照路由器总流量的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器组总流量的当前值，平均值，最大值。如果点击【路由器组】展开显示所有路由器组的名称，点击某一个路由器组进入当前路由器组流量分析页面，点击【总流量】tab 页，则显示当前路由器组的在最近 30 分钟的流量随时间变化的趋势图，关于总流量的分析方法可以参照路由器总流量的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器组总流量的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入路由器组中所有路由器的流量，下部分区域图为流出路由器组中的所有路由器的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.4.2 路由器组

点击【路由器组】进入所有路由器组流量分析页面，点击【路由器组】tab 页，显示在最近 30 分钟内每个路由器组随时间变化的流量趋势图。流量数据列表展示的是最近 30 分钟内的当前服务器总流量的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入每个路由器组中的所有路由器的流量，下

部分区域图为流出每个路由器组中的所有路由器的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看每个路由器组的流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.4.3 Top 地址

如果点击【路由器组】进入所有路由器组流量分析页面，点击【Top 地址】tab 页，则显示所有路由器组的在最近 30 分钟的源 Top5 地址流量随时间变化的趋势图，关于 Top 地址的分析方法可以参照路由器 Top 地址的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器组源 Top5 地址的当前值，平均值，最大值。如果展开【路由器组】显示所有路由器组的名称，点击某一个路由器组进入当前路由器组流量分析页面，点击【Top 地址】tab 页，则显示当前路由器组的在最近 30 分钟的源 Top5 地址流量随时间变化的趋势图，关于 Top 地址的分析方法可以参照路由器 Top 地址的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器组源 Top5 地址的当前值，平均值，最大值。

默认的流量图分为两部分，上部分区域图为流入路由器组中所有路由器的 Top5 源地址流量图，下部分区域图为流出路由器组总所有路由器的 Top5 源地址流量图。

如果用户点击流量趋势图上方的【目的地址】超链接，则流量图和流量数据列表展示的目的 Top5 地址的流量。流量图分为两部分，上部分区域图为流入路由器组中所有路由器的 Top5 目的地址流量图，下部分区域图为流出路由器组中所有路由器的 Top5 目的地址流量图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top5 地址流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.4.4 Top 应用

如果点击【路由器组】进入所有路由器组流量分析页面，点击【Top 应用】tab 页，则显示所有路由器组的在最近 30 分钟的 Top5 应用流量随时间变化的趋势图，关于 Top 应用的分析方法可以参照路由器 Top 应用的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器组 Top5 应用的当前值，平均值，最大值。如果展开【路由器组】显示所有路由器组的名称，点击某一个路由器组进入当前路由器组流量分析页面，点击【Top 应用】tab 页，则显示当前路由器组的在最近 30 分钟的 Top5 应用流量随时间变化的趋势图，关于 Top 应用的分析方法可以参照路由器 Top 应用的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器组 Top5 应用的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入路由器组中所有路由器的 Top5 应用的流

量，下部分区域图为流出路由器组中所有路由器的 Top5 应用的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top5 应用流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.4.5 Top 协议

如果点击【路由器组】进入所有路由器组流量分析页面，点击【Top 协议】tab 页，则显示所有路由器组的在最近 30 分钟的 Top5 协议流量随时间变化的趋势图，关于 Top 协议的分析方法可以参照路由器 Top 协议的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器组 Top 协议的当前值，平均值，最大值。如果展开【服务器】显示所有服务器的名称，点击某一个服务器进入当前服务器流量分析页面，点击【Top 协议】tab 页，则显示当前服务器的在最近 30 分钟的 Top5 协议流量随时间变化的趋势图，关于 Top 协议的分析方法可以参照路由器 Top 协议的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器组 Top5 协议的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入每个服务器的 Top5 协议的流量，下部分区域图为流出每个服务器的 Top5 协议的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top5 协议流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.4.6 Top 自治域

如果点击【路由器组】进入所有路由器组流量分析页面，点击【Top 自治域】tab 页，则显示所有路由器组的在最近 30 分钟的源 Top5 自治域流量随时间变化的趋势图，关于 Top 自治域的分析方法可以参照路由器 Top 自治域的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器组源 Top5 自治域的当前值，平均值，最大值。如果展开【路由器组】显示所有路由器组的名称，点击某一个路由器组进入当前路由器组流量分析页面，点击【Top 自治域】tab 页，则显示当前路由器组的在最近 30 分钟的源 Top5 自治域流量随时间变化的趋势图，关于 Top 自治域的分析方法可以参照路由器 Top 自治域的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器组源 Top5 自治域的当前值，平均值，最大值。

默认的流量图分为两部分，上部分区域图为流入路由器组中所有路由器的 Top5 源自治域流量图，下部分区域图为流出路由器组总所有路由器的 Top5 源自治域流量图。

如果用户点击流量趋势图上方的【目的自治域】超链接，则流量图和流量数据列表展示的目的 Top5 自治域的流量。流量图分为两部分，上部分区域图为流入路由器组中所有路由

器的 Top5 目的自治域流量图，下部分区域图为流出路由器组中所有路由器的 Top5 目的自治域流量图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top5 自治域流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.5 路由器接口组

5.5.1 总流量

如果点击【路由器接口组】进入所有路由器接口组流量分析页面，点击【总流量】tab 页，则显示所有路由器接口组的在最近 30 分钟的流量随时间变化的趋势图，关于总流量的分析方法可以参照路由器总流量的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器接口组总流量的当前值，平均值，最大值。如果展开【路由器接口组】显示所有路由器接口组的名称，点击某一个路由器接口组进入当前路由器接口组流量分析页面，点击【总流量】tab 页，则显示当前路由器接口组的在最近 30 分钟的流量随时间变化的趋势图，关于总流量的分析方法可以参照路由器总流量的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器接口组总流量的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入路由器接口组中所有接口的流量，下部分区域图为流出路由器接口组中所有接口的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.5.2 接口组

点击【路由器接口组】进入所有路由器接口组流量分析页面，点击【路由器接口组】tab 页，显示在最近 30 分钟内每个路由器接口组随时间变化的流量趋势图。流量数据列表展示的是最近 30 分钟内的当前路由器接口组总流量的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入每个路由器接口组中的所有接口的流量，下部分区域图为流出每个路由器接口组中的所有接口的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看每个路由器接口组的流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及

自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.5.3 Top 地址

如果点击【路由器接口组】进入所有路由器接口组流量分析页面，点击【Top 地址】tab 页，则显示所有路由器接口组的在最近 30 分钟的源 Top10 地址流量随时间变化的趋势图，关于 Top 地址的分析方法可以参照路由器 Top 地址的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器接口组源 Top10 地址的当前值，平均值，最大值。如果展开【路由器接口组】显示所有路由器接口组的名称，点击某一个路由器接口组进入当前路由器接口组流量分析页面，点击【Top 地址】tab 页，则显示当前路由器接口组的在最近 30 分钟的源 Top10 地址流量随时间变化的趋势图，关于 Top 地址的分析方法可以参照路由器 Top 地址的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器接口组源 Top10 地址的当前值，平均值，最大值。

默认的流量图为流入路由器接口组中所有接口的 Top5 源地址流量图。

如果用户点击流量趋势图上方的【目的地址】超链接，则流量图和流量数据列表展示的目的 Top10 地址的流量。流量图为流出路由器接口组中所有接口的 Top10 目的地址流量图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top10 地址流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.5.4 Top 应用

如果点击【路由器接口组】进入所有路由器接口组流量分析页面，点击【Top 应用】tab 页，则显示所有路由器接口组的在最近 30 分钟的 Top5 应用流量随时间变化的趋势图，关于 Top 应用的分析方法可以参照路由器 Top 应用的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器接口组 Top5 应用的当前值，平均值，最大值。如果展开【路由器接口组】显示所有路由器接口组的名称，点击某一个路由器接口组进入当前路由器接口组流量分析页面，点击【Top 应用】tab 页，则显示当前路由器接口组的在最近 30 分钟的 Top5 应用流量随时间变化的趋势图，关于 Top 应用的分析方法可以参照路由器 Top 应用的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器接口组 Top5 应用的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入路由器接口组中所有接口的 Top5 应用的流量，下部分区域图为流出路由器组中所有路由器接口组的所有接口的 Top5 应用的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top5 应用流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及

自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.5.5 Top 协议

如果点击【路由器接口组】进入所有路由器接口组流量分析页面，点击【Top 协议】tab 页，则显示所有路由器接口组的在最近 30 分钟的 Top5 协议流量随时间变化的趋势图，关于 Top 协议的分析方法可以参照路由器 Top 协议的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器接口组 Top5 协议的当前值，平均值，最大值。如果展开【路由器接口组】显示所有路由器接口组的名称，点击某一个路由器接口组进入当前路由器接口组流量分析页面，点击【Top 协议】tab 页，则显示当前路由器接口组的在最近 30 分钟的 Top5 应用流量随时间变化的趋势图，关于 Top 协议的分析方法可以参照路由器 Top 协议的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器接口组 Top5 协议的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入路由器接口组中所有接口的 Top5 协议的流量，下部分区域图为流出路由器组中所有路由器接口组的所有接口的 Top5 协议的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top5 协议流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.5.6 Top 自治域

如果点击【路由器接口组】进入所有路由器接口组流量分析页面，点击【Top 自治域】tab 页，则显示所有路由器接口组的在最近 30 分钟的源 Top10 自治域流量随时间变化的趋势图，关于 Top 地址的分析方法可以参照路由器 Top 自治域的分析方法。流量数据列表展示的是最近 30 分钟内的所有路由器接口组源 Top10 自治域的当前值，平均值，最大值。如果展开【路由器接口组】显示所有路由器接口组的名称，点击某一个路由器接口组进入当前路由器接口组流量分析页面，点击【Top 自治域】tab 页，则显示当前路由器接口组的在最近 30 分钟的源 Top10 自治域流量随时间变化的趋势图，关于 Top 自治域的分析方法可以参照路由器 Top 自治域的分析方法。流量数据列表展示的是最近 30 分钟内的当前路由器接口组源 Top10 自治域的当前值，平均值，最大值。

默认的流量图为流入路由器接口组中所有接口的 Top5 源自治域流量图。

如果用户点击流量趋势图上方的【目的自治域】超链接，则流量图和流量数据列表展示的目的 Top10 自治域的流量。流量图为流出路由器接口组中所有接口的 Top10 目的自治域流量图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top10 自治域流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.6 流量场景

点击 【流量场景】进入所有流量场景流量分析页面，默认展示该所有流量场景在最近 30 分钟内的总流量趋势。点击展开流量场景分组，列出所有流量场景名称，点击流量场景名称进入该流量场景流量分析页面，默认展示该所有流量场景在最近 30 分钟内的总流量趋势。

主要功能包括以下功能：

5.6.1 流量场景

展示每个流量场景随时间变化的流量趋势。默认展示 30 分钟内流入流量场景的流量趋势和流出流量场景的流量趋势图。流量数据列表展示的是最近 30 分钟内的每个流量场景的流量的当前值，平均值，最大值。

该流量图分为上下两部分，上下对称，上部分区域图为流入流量场景的流量趋势图，下部分区域图为流出流量场景的流量趋势图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看流量场景流量趋势图。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.6.2 总流量

展开【流量场景】显示所有流量场景的名称，点击某一个流量场景进入当前流量场景流量分析页面，点击【总流量】tab 页，则显示当前流量场景的在最近 30 分钟的流量随时间变化的趋势图。流量数据列表展示的是最近 30 分钟内的当前流量场景总流量的当前值，平均值，最大值。

流量图分为上下两部分，上部分区域图为流入流量场景的流量，下部分区域图为流出流量场景的流量。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看总流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.6.3 Top 地址

展开【流量场景】显示所有流量场景的名称，点击某一个流量场景进入当前流量场景流量分析页面，点击【Top 地址】tab 页，则显示当前流量场景的在最近 30 分钟的源 Top10 地址流量随时间变化的趋势图。流量数据列表展示的是最近 30 分钟内的当前流量场景源 Top10 地址的当前值，平均值，最大值。

默认的流量图为流入流量场景的 Top10 源地址流量图。

如果用户点击流量趋势图上方的【目的地址】超链接，则流量图和流量数据列表展示的目的 Top10 地址的流量。流量图为流出流量场景的 Top10 目的地址流量图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top10 地址流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.6.4 Top 接口

展开【流量场景】显示所有流量场景的名称，点击某一个流量场景进入当前流量场景流量分析页面，点击【Top 接口】tab 页，则显示当前流量场景的在最近 30 分钟内从路由器流入的 Top10 接口流量随时间变化的趋势图。流量数据列表展示的是最近 30 分钟内的当前流量场景源 Top10Input 接口的当前值，平均值，最大值。

如果用户点击流量趋势图上方的【output】超链接，则流量图和流量数据列表展示流量场景的从路由器流出的 Top 接口流量。流量图为流量场景从路由器流出的 Top10Output 流量图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看 Top10 接口流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.7 主机

5.7.1 总流量

参照服务器总流量分析

5.7.2 Top 地址

参照服务器 Top 地址流量分析

5.7.3 Top 接口

输入主机 Ip 地址，则该流量图默认展示为从路由器流入主机的 Top10 接口的流量图。流量数据列表展示的是最近 30 分钟内从路由器流入主机的 Top10 接口流量的当前值，平均值，最大值。

当用户点击【output】则展示该主机从路由器流出的 Top10 接口的流量图。流量数据列表展示的是最近 30 分钟内该主机从路由器流出的 Top10 接口流量的当前值，平均值，最大值。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

5.7.4 Top 协议

参照服务器 Top 协议分析

5.8 自治域

点击 【自治域】进入所有自治域对流量分析页面，默认展示自定义监控模块中监控的自治域对在最近 30 分钟内的总流量趋势。点击流量数据列表中的自治域对，展示从每个路由器设备流过的当前自治域对的流量趋势。

主要功能包括以下功能：

5.8.1 自治域

展示监控的所有自治域对中每个自治域对在最近 30 分钟内从路由器流入和流出的流量趋势图。流量数据列表展示的是最近 30 分钟内的每个自治域对的当前值，平均值，最大值。

该流量图分为上下两部分，上下对称，上部分区域图为从源自治域流向目的自治域的流量趋势图，下部分区域图为从目的自治域流向源自治域的流量趋势图。

通过趋势图右上方的流量单位单选按钮，可以不同的流量统计单位切换查看自治域流量趋势。

目前本系统只支持 30 分钟/1 小时/1 天/7 天/30 天/90 天等固定粒度的查询时间段以及自定义的查询时间段。如果想要历史的流量趋势或者更细力度的流量趋势，则需要用户手动选择要查询的时间段进行流量的查询。

6 路由

路由分析是运营商用户比较关注的功能，通过分析路由消息和路由表信息，得到关于路由稳定性和合理性的结论。具体的功能包括：

- 路由前缀数目分析：统计路由表中不同长度的网络前缀的数量
- 路由稳定性分析：对路由更新的情况进行分析，包括路由更新数目和各类异常路由更新数目，反应出网络路由的稳定性情况
- 路由数目分析：统计路由条目数量的变化
- BGP 包分析：统计不同 BGP Peer 发生的 BGP 数据包的数量
- 路由震荡分析：统计不同自治域正在抖动和已被抑制的路由情况（仅分析 EBGP）。

6.1 路由前缀分析

点击 【路由前缀数目分析】 分组进入前缀数目分析页面，本页面分为实时分析和历史查询两部分，分析当前路由表中各种前缀长度的数量分布。展示路由前缀数目的分布图和分布矩阵。

6.1.1 实时分析

点击 【路由前缀数目分析】 分组进入前缀数目分析页面，当前默认页面是实时分析页面。系统通过路由前缀数目的分布图和分布矩阵来对当前实时路由前缀数目进行展示分析。系统默认每隔 30 秒钟自动刷新一次。

通过路由前缀数目的分布图和分布矩阵下的路由前缀数目是一致的。

- 设置路由前缀数目分析条件进行分析展示

  前缀类型分为三类:

  - IPv4 单播前缀
  - IPv4 组播前缀
  - IPv4 MPLS_VPN 前缀

  前缀状态：

  - 被选择——当前正在使用的前缀。
  - 已被抑制——由于抖动等因素导致被抑制的前缀。
  - 正在抖动——正在抖动的前缀。
  - 最优——备用的最优先级的前缀。

点击路由前缀数目的分布图上方的【前缀类型】或【前缀状态】进行设置，设置完成后分析页面会立即刷新对当前所设置的路由前缀数条件进行分析展示。系统默认每隔 30 秒钟自动刷新一次。

- 启停分析

进入实时分析页面时系统默认是自动刷新状态。

点击路由前缀数目的分布图上方的【停止】或【继续】键进行路由前缀数目分析的启停操作。系统默认每隔 30 秒钟自动刷新一次。

6.2 路由稳定性分析

点击 【路由稳定性分析】 分组进入稳定性分析页面，本页面分为实时分析和历史查询两部分对路由更新的情况进行分析，通过对路由更新的情况进行分析，包括路由更新数目和各类异常路由更新数目，反应出网络路由的稳定性情况。

6.2.1 实时分析

点击 【路由稳定性分析】 分组进入稳定性分析页面，当前默认页面是实时分析页面。系统通过路由稳定性分析的曲线图和统计列表来对当前实时路由稳定性进行展示分析。系统默认每隔 30 秒钟自动刷新一次。

系统默认 30 分钟时间范围下查看该时间范围内的路由稳定性分析曲线图和路由类型的数据统计列表。

- 路由稳定性分析曲线图

在路由稳定性的曲线图中，展示了所选时间范围内路由稳定性的情况。横坐标表示时间，纵坐标表示各类型路由更新的数

- 路由稳定性统计列表

在统计列表中，展示了各类型路由在默认时间范围内的当前值、最大值、平均值和数量总和。

- 启停分析

进入实时分析页面时系统默认是自动刷新状态。

点击路由稳定性分析曲线图上方的【停止】或【继续】键进行路由稳定性分析的启停操作。系统默认每隔 30 秒钟自动刷新一次

6.2.2 历史分析

在路由稳定性分析页面点击【历史分析】页签进入历史分析页面

自定义时间段。点击曲线图上方【自定义】键，在时间文本框内的任意位置单击鼠标左键，弹出日历表，选择日期和时间（起始时间和结束时间必须设置）

设置完成后点击【查询】键，历史分析页面会立即刷新显示当前时间段下的路由稳定性历史分析数据。

6.3 路由数目分析

点击 【路由数目分析】 分组进入路由数目分析页面，本页面分为实时分析和历史查询两部分对路由数目进行分析，可以分析来自各邻居的路由数目，即按照前缀类型、前缀状态进行分类统计，同时还标明了邻居的名称以及 AS 号

6.3.1 实时分析

点击 【路由数目分析】 分组进入数目分析页面，当前默认页面是实时分析页面。系统通过路由数目分析的曲线图和统计列表来对当前实时路由数目进行展示分析。系统默认每隔 30 秒钟自动刷新一次。

系统默认 30 分钟时间范围下查看该时间范围内的路由数目分析曲线图和路由类型的数据统计列表。

- 设置路由前缀数目分析条件进行分析展示

  前缀类型分为三类:

  - IPv4 单播前缀
  - IPv4 组播前缀
  - IPv4 MPLS_VPN 前缀

  前缀状态：

  - 被选择——当前正在使用的前缀。
  - 已被抑制——由于抖动等因素导致被抑制的前缀。
  - 正在抖动——正在抖动的前缀。
  - 最优——备用的最优先级的前缀。

点击路由前缀数目的分布图上方的【前缀类型】或【前缀状态】进行设置，设置完成后分析页面会立即刷新对当前所设置的路由前缀数条件进行分析展示。系统默认每隔 30 秒钟自动刷新一次。

- 启停分析

进入实时分析页面时系统默认是自动刷新状态。

点击路由数目的分布图上方的【停止】或【继续】键进行路由数目分析的启停操作。系统默认每隔 30 秒钟自动刷新一次。

6.3.2 历史分析

在路由数目分析页面点击【历史分析】页签进入历史分析页面.

- 配置时间段

路由数目分析时间段的设置方式有以下两种：

1、选择时间段。单击曲线图上方的文字链接，可以设置最近 30 分钟、最近 1 小时、最

近 1 天、最近 7 天、最近 30 天或最近 90 天的时间段。

2、自定义时间段。点击曲线图上方【自定义】键，在时间文本框内的任意位置单击鼠标左键，弹出日历表，选择日期和时间（起始时间和结束时间必须设置）

在点击曲线图上方【自定义】键后再时间文本框内的任意位置单击鼠标左键，弹出日历表，选择日期和时间（起始时间和结束时间必须设置）。或单击曲线图上方的文字链接，可以设置最近 30 分钟、最近 1 小时、最近 1 天、最近 7 天、最近 30 天或最近 90 天的时间段。

设置完成后点击【查询】键，历史分析页面会立即刷新显示当前时间段下的路由数目历史分析数据。

- 设置路由前缀条件

  前缀类型分为三类:

  - IPv4 单播前缀
  - IPv4 组播前缀
  - IPv4 MPLS_VPN 前缀

  前缀状态：

  - 被选择——当前正在使用的前缀。
  - 已被抑制——由于抖动等因素导致被抑制的前缀。
  - 正在抖动——正在抖动的前缀。
  - 最优——备用的最优先级的前缀。

点击路由数目的曲线图上方的【前缀类型】或【前缀状态】进行设置。

在不配置时间段的前提下系统默认为当前实时时间段，设置完成后点击【查询】键，历史分析页面会立即刷新显示当前时间段下的路由数目历史分析数据。

6.4 BGP 包分析

6.4.1 实时分析

点击 【BGP 包分析】 分组进入 BGP 包分析页面，当前默认页面是实时分析页面。系统通过 BGP 包分析的曲线图和统计列表来对当前实时 BGP 包进行展示分析。系统默认每隔 30 秒钟自动刷新一次。

系统默认 30 分钟时间范围下查看该时间范围内的路由数目分析曲线图和路由类型的数据统计列表。

- 设置包数类型

包数类型分为正常更新包和无效更新包，其中无效更新包是要被路由器丢弃的异常包

点击 BGP 包分析曲线图上方的【包数类型】进行设置。

设置完成后分析页面会立即刷新对当前所设置的当 BGP 包数类型进行分析展示。

- 启停分析

进入实时分析页面时系统默认是自动刷新状态。

点击 BGP 包分析图上方的【停止】或【继续】键进行 BGP 包分析的启停操作。系统默认每隔 30 秒钟自动刷新一次。

6.4.2 历史分析

在 BGP 包分析页面点击【历史分析】页签进入历史分析页面

➢ 设置包数类型

包数类型分为正常更新包和无效更新包，其中无效更新包是要被路由器丢弃的异常包

点击 BGP 包分析曲线图上方的【包数类型】进行设置。

在不配置时间段的前提下系统默认为当前实时时间段，设置完成后点击【查询】键，历史分析页面会立即刷新显示当前时间段下的 BGP 包历史分析数据。

➢ 配置时间段

在点击曲线图上方【自定义】键后再时间文本框内的任意位置单击鼠标左键，弹出日历表，选择日期和时间（起始时间和结束时间必须设置）。

设置完成后点击【查询】键，历史分析页面会立即刷新显示当前时间段下的 BGP 包历史分析数据。

6.5 路由震荡分析

点击 【路由震荡分析】 分组进入路由震荡分析页面，本页面分为实时分析和历史查询两部分对路由震荡进行分析，路由震荡分析功能只对 EBGP 邻居有效。

通过路由震荡分析，统计了路由表中当前正在震荡和因抖动厉害而被抑制的前缀数目，可分别按正在抖动或已被抑制两种类型来展示。

6.5.1 实时分析

点击 【路由震荡分析】 分组进入路由震荡分析页面，当前默认页面是实时分析页面。系统通过路由震荡分析的曲线图和统计列表来对当前实时 BGP 包进行展示分析。系统默认每隔 30 秒钟自动刷新一次。

系统默认 30 分钟时间范围下查看该时间范围内的路由数目分析曲线图和路由类型的数据统计列表。

➢ 设置路由震荡类型

路由震荡类型：

- 正在抖动
- 已被抑制

点击路由震荡分析曲线图上方的【类型】进行设置。

设置完成后分析页面会立即刷新对当前所设置的当路由震荡类型进行分析展示。

➢ 启停分析

进入实时分析页面时系统默认是自动刷新状态。

点击路由震荡分析图上方的【停止】或【继续】键进行路由震荡分析的启停操作。系统默认每隔 30 秒钟自动刷新一次。

6.5.2 历史分析

在路由震荡分析页面点击【历史分析】页签进入历史分析页面

➢ 配置时间段

在点击曲线图上方【自定义】键后再时间文本框内的任意位置单击鼠标左键，弹出日历表，选择日期和时间（起始时间和结束时间必须设置）。

设置完成后点击【查询】键，历史分析页面会立即刷新显示当前时间段下的路由震荡历史分析数据。

➢ 设置路由震荡类型

路由震荡类型：

- 正在抖动
- 已被抑制

点击路由震荡分析曲线图上方的【类型】进行设置。

在不配置时间段的前提下系统默认为当前实时时间段，设置完成后点击【查询】键，历史分析页面会立即刷新显示当前时间段下的路由震荡历史分析数据。

7 数据

数据管理包括数据存储策略、远程备份、清除告警功能，主页显示管理设备硬盘使用情况,数据库使用的基本信息以及 netflow 流量分析图。通过一级菜单“数据”按钮进入数据管理界面。

7.1 存储策略

数据管理模块的存储策略用来自定义数据表的存储期限。

7.1.1 新增策略

单击存储策略列表上方的【新增】按钮，进入新增策略页面，各项参数含义如下：

- 表明信息——选择告警、流量、过滤器、路由表。
- 保留时间——填写库表信息保留时间。
- 时间粒度——选择库表信息保留时间的时间单位。

注意事项：

- 表名信息：存数策略添加成功后在存储策略列表显示，同时添加页面表明信息下拉框中不再显示已填加成功表名。
- 保留时间：只支持数字格式。
- 时间粒度：可以根据需要制定策略执行的时间单位：分钟、小时、天、周、月、季、年。

7.1.2 编辑策略

单击存储策略列表最后一列的【编辑】按钮，对存储策略进行编辑。

注意事项：

- 表名信息：此项已经选定不允许进行重新编辑。

7.1.3 删除策略

单击存储策略列表最后一列的【删除】按钮，进行存数策略删除。同时存储策略列表进行刷新。

7.1.4 磁盘使用率阀值

单击存储策略列表上方的【磁盘使用率阀值】按钮，设定磁盘自动清理功能。

各项参数含义如下：

- 磁盘阀值——磁盘占用超过此阀值时进行自动清理。
- 状　　态——选择磁盘阀值清理功能是否启用，此项为单选项。

注意事项：

- 磁盘阀值：输入 0-100 之间整数。

7.2 远程备份

启用备份功能，即可按照设定时间将当前日志审计的告警监控信息和流量分析数据自动备份到远程备份服务器中。

7.2.1 新增备份信息

单击远程备份列表上方的【新增】按钮，进入新增备份页面，各项参数含义如下：

- 服务器地址：填写远程备份服务器 IP 地址。
- 用　户　名：填写远程备份服务器登录用户名。
- 登录密码：填写远程备份服务器登录密码。
- 备份路径：填写远程备份服务器文件备份路径。
- 状　　态：选择此远程备份是否启用。

注意事项：

- 服务器地址：远程服务器地址要符合 IP 格式要求。
- 必选性要求：远程备份添加中所有选项均不能为空。

7.2.2 编辑备份信息

单击远程备份列表中【编辑】按钮，对备份信息的属性进行编辑，编辑的界面中各项参数含义与添加界面中一致。

7.2.3 删除备份信息

单击远程备份列表中【删除】按钮，进行远程备份删除。同远程备份列表进行刷新。

7.2.4 备份时间

单击远程备份列表上方【备份时间】按钮，设定远程备份时间，各项参数含义如下：

- 备份时间——选择每天进行备份时间，选择范围为 0 至 23 之间。
- 状　　态——远程备份功能是否启用。

7.3 清除警告

单击页面的“清除警告”按钮，即弹出是否清除所有警告信息的提示框，单击“确定”，即清除所有警告信息，单击“取消”，不清除信息。

 此操作可能引起告警监控及相关查询不正常，因此不建议使用。

。

8 报表

报告是将多个报表合并生成一个报表，同时可以输入报告描述，显示在报告的最前面。

报表分内置报表与自定义报表，自定义报表又分事件统计报表、事件趋势报表、事件明细报表。

报表目前支持的格式为 PDF/HTML/PNG/DOCX/RTF/XLSX/XLS。

8.1 报表组

报表以树形结构的方式管理，报表组下可以有子报表组。

1、新增报表组

选中报表组结点，点击报表树上方的工具条中的【添加】按钮，会弹出添加组的对话框，报表组的属性包括：名称（必填）、描述。

添加操作完成后，报表树会及时更新，报表树上会显示新添加的报表组节点。

2、编辑报表组

编辑报表组的操作类似于添加操作，用户首先需要先选中欲编辑的报表组，再点击报表树上方的工具条中的【编辑】按钮。

完成报表组的修改后，报表树会及时更新，报表树的节点会显示为新修改后的内容。

3、删除报表组

在进行删除报表组操作前，用户需要先选中一个报表组。点击报表树上方的工具条中的【删除】按钮，弹出是否删除的确认对话框，点击【确定】按钮完成组的删除操作，点击【取消】按钮取消删除。

如果该报表组下有子节点存在，则必须先删除子结点后才能删除该报表组。

删除报表组后，报表树结构及时刷新，不再显示已经删除的报表组节点。

4、导出报表组

导出报表组是将系统中的所有报表及报表组全部导出，主要是为了备份或恢复报表或报表组，以及系统移植。

点击报表组上方的工具条中的【导出】按钮，系统会以 zip 文件的格式将所有报表及报表组导出。

5、导入报表组

导入是将以前导出的报表组与报表，全部导入到系统中。如果已有报表与导入报表的编号相同，已有报表会被覆盖。

8.2 系统内置报表

系统内置了一些预定义的审计报表，供用户直接使用以查看一些通用条件下的报表数

据，这是内置的报表，不能修改和删除，只能查看、导出、调度运行。

具体报表的查看、导出、调度等操作，请参考下面【报表操作】。

8.3 报表操作

8.3.1 查看

点击报表列表中的【查看】按钮，在弹出的对话框中输入报表的统计时间范围，时间范围分为相对时间和绝对时间两种，相对时间的单位包括天、周、月；绝对时间可以通过点击日历按钮来选择确切的开始时间和结束时间。

点击【预览】按钮，就可以以预览方式查看报表了。

8.3.2 导出

点击报表列表中的【查看】按钮，在弹出的对话框中输入报表的统计时间范围，时间范围分为相对时间和绝对时间两种，相对时间的单位包括天、周、月；绝对时间可以通过点击日历按钮来选择确切的开始时间和结束时间。

点击【导出】按钮，选择导出的格式，就可以导出生成的报表了。

报表目前支持的导出格式为 PDF/HTML/PNG/DOCX/RTF/XLSX/XLS。

8.3.3 调度

调度是指自动定时生成报表。

点击报表列表中的【调度】按钮，可以输入调度参数，包括：

- 调度类型：设置报表的运行周期
- 时间范围：报表的统计时间，相对时间或绝对时间
- 报表格式：目前支持 PDF/HTML/WORD/EXCEL/PNG
- 首次运行时间：报表的首次运行时间
- 邮件通知：生成报表时，同时发送通知给指定的接收人，如果同时选中了发送附件，可以将生成的报表通过邮件发送给指定的接收人

新建调度完成后，即可以对调度进行操作，包括查看、下载、删除、编辑等。

1、查看调度

在调度列表中，点击【查看】按钮，可以查看和下载该调度已经生成的报表文件，点击【关闭】按钮返回上一页。

2、删除调度

选中需要删除的调度任务，点击【删除】按钮，可以直接删除，也可以选择【备份并下载已经生成的报表文件后删除】,将报表先进行备份处理，再进行删除操作；选择【直接删除】就可以完成删除。系统支持批量删除。

3、刷新调度

点击调度列表上方的【刷新】按钮，调度列表及时更新，显示刷新后的报表调度状态。

8.3.4 复制

在报表列表页面选定一条需要复制的报表，点击工具栏中的【复制】按钮，选中需要复制到的报表组，即可完成对该报表的复制操作，复制报表遇同名时，自动在文件名后添加后缀以便区分，系统支持批量复制操作。

复制完成后，报表列表及报表树及时刷新。完成复制后，可以进行适当修改而成为符合要求的报表。

8.3.5 移动

在报表列表页面选择需要移动的报表，点击工具条栏的【移动】按钮，选择需要移动到的报表组，即可完成对该报表的移动操作，移动报表遇同名时，自动在文件名后添加后缀以便区分，系统支持批量移动操作。

移动完成后，报表列表及报表树及时刷新。

9 配置

9.1 系统配置

9.1.1 系统管理

系统部分主要是做一些系统的基础配置，这些配置通常会在系统的其他地方引用，比如：系统基本信息、网络配置、诊断分析工具、配置导入导出、登录许可控制、许可证管理、系统升级等。

9.1.1.1 系统基本信息

显示系统的基本信息其中，系统 ID 是系统自身唯一的标识符，不得编辑，CPU、物理内存信息是硬件本身的信息不可编辑。主机名、系统时间和 NTP 服务器可以通过保存按钮来更新系统基本信息。

修改系统时间时需注意：单击系统时间单行文本框可以选择相应的系统时间

NTP 服务用于同步系统的服务器时间.

9.1.1.2 用户认证配置

配置当用户在 1 分钟内，连续几次登录失败后，将用户帐户锁定一段时间。

当前默认值为：用户在 1 分钟内，连接登录 3 次失败，则将帐号锁定 5 分钟只有 5 分钟后才能再次登录。

属性	描述
认证时间锁定	当账户被锁定后，在该时间段内该帐户无法登录系统
认证次数锁定	用户登录系统，输入密码次数达到允许的失败次数后，账户将被锁定

9.1.1.3 管理中心

管理 IP 和接口配置

9.1.1.3.1 新增

点击【新增】按钮，会弹出添加管理中心配置的对话框，管理中心配置的属性包括：

- 中心管理 IP：必填，设置中心管理 IP。
- 监听端口：必填，设置中心管理 IP。

添加操作完成后，中心管理配置会及时更新，列表页会显示新添加的中心管理配置

9.1.1.3.2 编辑

编辑管理中心配置的操作类似于添加操作，用户首先需要先选中欲编辑的中心管理配置，会弹出编辑管理中心配置的对话框。

完成管理中心配置的修改后，管理中心配置会及时更新，管理中心配置会显示为新修改后的内容。

9.1.1.3.3 删除

在进行删除管理中心配置操作前，用户需要先选中一个管理中心配置。点击管理中心配置上方的工具条中的【删除】按钮，弹出是否删除的确认对话框，点击【确定】按钮完成组的删除操作，点击【取消】按钮取消删除。

删除管理中心配置后，管理中心配置及时刷新，不再显示已经删除的管理中心配置。

9.1.1.4 备份与还原

9.1.1.4.1 导入

点击【导入】按钮，会弹出导入配置文件的对话框，找到自己的要导入的配置导入确定。文件必须以(.ta)结尾

9.1.1.4.2 备份

点击【备份】按钮，会弹出备份的对话框，点击确定则备份当前时间的系统配置，同时将配置信息更新到列表中

9.1.1.4.3 快速还原

点击操作栏中的快速还原按钮弹出是否还原的确认对话框，点击【确定】按钮完成组的还原操作，点击【取消】按钮取消还原

9.1.1.4.4 删除

在进行删除备份还原配置操作前，用户需要先选中一个备份还原配置。点击备份还原配置上方的工具条中的【删除】按钮，弹出是否删除的确认对话框，点击【确定】按钮完成组

的删除操作，点击【取消】按钮取消删除。

删除管理中心配置后，管理中心配置及时刷新，不再显示已经删除的管理中心配置

9.1.1.5 转发配置

配置外部设备接收 NetFlow 数据提供配置

9.1.1.5.1 新增

点击【新增】按钮，会弹出添加转发配置的对话框，转发配置的属性包括：

- 转发 IP：必填，设置转发 NetFlow 服务器的 IP。
- 转发端口：必填，设置转发 NetFlow 服务器的端口。
- 路由设备：必填，设置转发 NetFlow 的路由设备。
- 是否生效

添加操作完成后，转发配置会及时更新，列表页会显示新添加的转发配置

9.1.1.5.2 编辑

转发配置配置的操作类似于添加操作，用户首先需要先选中欲编辑的转发配置，会弹出编辑转发配置的对话框。

完成转发配置的修改后，转发配置会及时更新，转发配置会显示为新修改后的内容。

9.1.1.5.3 删除

在进行删除转发配置操作前，用户需要先选中一个转发配置。点击转发配置上方的工具条中的【删除】按钮，弹出是否删除的确认对话框，点击【确定】按钮完成组的删除操作，点击【取消】按钮取消删除。

删除转发配置后，转发配置及时刷新，不再显示已经删除的转发配置

9.1.1.6 系统升级

此功能只有在我们的硬件产品或 Linux 操作系统上才会提供。您需要首先将我们提供给你的升级包上传到系统的指定目录，然后点击【升级】按钮，完成升级。升级完成，系统将自动重启。

9.1.1.7 系统自身性能

包括在线用户、系统日志、服务器监控、数据库监控、监控阈值配置，系统服务监控等。

- 在线用户

显示当前登录系统的在线用户，包括登录 IP、用户名称、最后登录时间等。

➢ 系统日志

显示系统自身日志，只能查询，不能修改、删除。

显示的信息包括：用户名、IP、操作时间、操作内容、操作结果等。

➢ 服务器监控

显示系统所在的主机的监控信息。包括：主机名、操作系统、IP 等，以及以图形的方式显示 CPU 使用率、内存利用率、磁盘使用情况等。

➢ 数据库监控

显示系统所使用的数据库监控信息。包括内存占用率、数据库所在碰盘空间使用率、活动线程与打开连接数。

➢ 监控阈值配置

监控阈值是指某个监控指标所能达到的最大值或最小值，当监控指标的某项监控值大于等于该值时系统将会生成一条监控类型的告警事件，你可以通过规则配置触发告警动作。

目前可以针对 CPU 使用率、内存使用率、磁盘空间使用率设置告警阈值。

➢ 系统服务监控

在这里可以监控系统的主要服务进程的工作状态

9.1.1.8 用户认证配置

配置当用户在 1 分钟内，连续几次登录失败后，将用户帐户锁定一段时间。

当前默认值为：用户在 1 分钟内，连接登录 3 次失败，则将帐号锁定 5 分钟，只有 5 分钟后才能再次登录。

属性	描述
认证时间锁定	当账户被锁定后，在该时间段内该帐户无法登录系统
认证次数锁定	用户登录系统，输入密码次数达到允许的失败次数后，账户将被锁定

9.1.2 网络配置

9.1.2.1 网卡配置

在此配置本系统的网络参数（运行表示该网口的网络连接正常，停止表示该网口的网络连接断开），每个网口均可设置一个 IP 地址。初始状态下显示出厂参数，需手工设置网卡的 IP 地址及子网掩码。若要解除某个网络参数的 IP 绑定，点击【停止】弹出是否停止的确认对话框，点击【确定】按钮完成组的停止操作，点击【取消】按钮取消停止。若要启动某个网络参数的 IP 绑定，点击【启动】弹出是否启动的确认对话框，点击【确定】按钮完成组的启动操作，点击【取消】按钮取消删除

9.1.2.2 路由配置

9.1.2.2.1 新增路由配置

点击【新增】按钮，会弹出添加路由配置的对话框，路由配置的属性包括：

目的网络：必填，设置本系统路由信息的目的网路 IP。

网关：必填，设置本系统路由信息的网关。

接口：必填，设置本系统路由信息的接口。

添加操作完成后，路由配置会及时更新，列表页会显示新添加的路由配置。

注意：系统默认的路由配置不会删除。

9.1.2.2.2 删除路由配置

点击路由配置的【删除】按钮，弹出是否删除的确认对话框，点击【确定】按钮完成组的删除操作，点击【取消】按钮取消删除。

删除路由配置后，路由配置及时刷新，不再显示已经删除的路由配置。

9.1.3 诊断分析

9.1.3.1 Ping 分析

ping 工具用于检测主机存活或网络通断情况

9.1.3.2 抓包分析

抓包，即依据自行设置的条件启动抓包任务，获取符合抓包条件的网络数据包。抓包过程中，无法添加其他抓包任务

点击【抓包】按钮，会弹出抓包配置的对话框，抓包配置的属性包括：

端口——填写一个端口号，表示本次任务是对该端口进行抓包，范围是 1~65535。填写 0 表示所有端口。

协议——可以填写 TCP、UDP、ICMP 或任意。

最大抓包数量——需要抓包数量的最大值，范围是 1~10000。

网口——选择从哪个网口抓包。

时长——指的是抓包的时长。

9.1.3.3 SNMP 分析

SNMP 分析是对 SNMP 服务器设备通断的分析。

SNMP 分析的属性包括：

设备地址：必填，设置 SNMP 设备 IP。

端口：必填，设置 SNMP 设备端口。

SNMP Communtiy：必填，设置 SNMP Communtiy。

SNMP 版本：必填，设置 SNMP 版本。

9.1.3.4 FLOW 分析

Flow 分析是对提供设备当前接收到的 Flow 情况。最近 5s/10s/30s 内的设备接收的 flow 数据详情，如果采集 flow 超过 100 条，则立即完成诊断。

Flow 配置的属性包括：

Flow 条数：分为 100、500、1000。

时长：分为 5s、10s、30s。

9.1.4 数据代理接口

9.1.4.1 Snmp 配置

在此配置 SMTP 服务器信息和发件人的帐号等信息

9.1.4.1.1 新增

点击【新增】按钮，会进入添加 SNMP 配置的页面，SNMP 配置的属性包括：

启用 SNMP 配置：非必填

SNMP 配置名称：必填，设置 SNMP 配置名称。

管理主机 IP：非必填，设置 SNMP 管理主机 IP 可以有多个。

IP 列表：非必填，用于存储 SNMP 管理主机 IP 列表。

只读权限社区名：必填，设置只读权限社区名称。

读写权限社区名：必填，设置读写权限社区名称。

Trap 权限社区名：必填，设置 Trap 权限社区名。

是否启用 V3：非必填

安全级别：高、中、低

用户名：非必填，设置 V3 用户名称。

认证模式：非必填，设置认证模式分为 MD5、SHA

认证密码：非必填，设置认证密码。

加密模式：非必填，设置密码模式分为 DES、AES。

加密密码：非必填，设置加密密码。

添加操作完成后，SNMP 配置会及时更新，列表页会显示新添加的 SNMP 配置。

9.1.4.1.2 编辑

编辑 SNMP 配置的操作类似于添加操作，用户首先需要先选中欲编辑的 SNMP 配置，会弹出编辑 SNMP 配置的对话框。

完成 SNMP 配置的修改后，SNMP 配置会及时更新，SNMP 配置会显示为新修改后的内容。

9.1.4.1.3 删除

在进行删除 SNMP 配置操作前，用户需要先选中一个 SNMP 配置。点击 SNMP 配置上方的工具条中的【删除】按钮，弹出是否删除的确认对话框，点击【确定】按钮完成组的删除操作，点击【取消】按钮取消删除。

删除 SNMP 配置后，SNMP 配置及时刷新，不再显示已经删除的 SNMP 配置。

9.1.4.2 Syslog 配置

9.1.4.2.1 新增

点击【新增】按钮，会弹出添加 SYSLOG 配置的对话框，SYSLOG 配置的属性包括：

服务器 IP：必填，设置 SYSLOG 采集服务器 IP

日志类型：非必填，设置日志类型分为：警告日志、流量日志、系统日志。

启用：非必填

添加操作完成后，SYSLOG 配置会及时更新，列表页会显示新添加的 SYSLOG 配置。

9.1.4.2.2 编辑

SYSLOG 配置的操作类似于添加操作，用户首先需要先选中欲编辑的 SYSLOG 配置，会弹出编辑 SYSLOG 配置的对话框。

完成 SYSLOG 配置的修改后，SYSLOG 配置会及时更新，SYSLOG 配置会显示为新修改后的内容。

9.1.4.2.3 删除

在进行删除 SYSLOG 配置操作前，用户需要先选中一个 SYSLOG 配置。点击 SYSLOG 配置上方的工具条中的【删除】按钮，弹出是否删除的确认对话框，点击【确定】按钮完成组的删除操作，点击【取消】按钮取消删除。

删除 SYSLOG 配置后，SYSLOG 配置及时刷新，不再显示已经删除的 SYSLOG 配置。

9.1.5 产品授权管理

显示产品的授权信息，以及系统的设备序列号，您需要将系统的设备序列号提供给我们，

然后再导入我们提供给您的产品授权许可文件

9.1.6 策略管理

9.1.6.1 异常检测

9.1.6.1.1 性能告警

9.1.6.1.1.1 性能异常告警配置

性能异常告警配置主要设置 CUP 阈值,内存阈值,带宽使用率阈值的高中低阈值百分比,并且可以制定潜伏周期,观察周期的时间(单位:分钟).

9.1.6.1.1.2 数据中断告警配置

数据中断告警配置主要配置路由设备流中断, 路由设备 SNMP 数据中断, 服务器 SNMP 数据中断的是否启用和时间周期(三个选项:5 分钟 10 分钟 15 分钟)

9.1.6.1.1.3 Ping 不可达告警配置

Ping 不可达告警配置实现了增加,删除,修改,查看(列表,单条)操作.可以新增 Ping 不可达告警,有三种类型可以选择(路由设备,服务器,IP 地址),可以进行单条和批量的删除操作,可以进行更新,并且单条可以查看详细.

9.1.6.1.2 自定义告警

自定义告警页面由列表组成, 实现了增加,删除,修改,查看(列表,单条)操作.新增可以设置(启用,名称,主体类型,包长,字节数/flow,包数/flow,协议,源端口,目的端口,协议端口 Tcp Flag 等字段),可以进行单条,批量删除,并且可以根据配置的单条信息,动态初始化更新页面,实现更新操作.可以查看单条信息的详细信息

9.1.6.1.3 检测引擎

检测引擎的作用作用即时配置一些引擎常用参数,主要类别分为基本信息设置 容量设置 阈值设置三个类别.

基本信息设置包括: 持续多少次后异常告警 Flow 接收端口号 是否记录时间窗基线值过滤器 TOP IP 记录个数等选项.

阈值设置包括: 5 分钟 IP 流量记录阈值 实时 IP 流量记录阈值等设置.

容量设置包括: 是否启用渐进分析 内网 IP 流表容量上限(默认上限 10000) 外网 IP 流表容量上限(默认上限 10000) 内网 AS 流表容量上限(默认上限 5000) 外网 AS 流表容量上限(默认上限 5000) 内网应用流表容量上限(默认上限 5000) 外网应用流表容量上限(默

认上限 5000)等设置

9.1.6.1.4 告警通知

为了实现系统检测到异常流量信息时及时通知用户，需要通过此功能定义多种告警通知类型，每种类型包括多个事件类型、需要通知的用户、事件源所在的 IP 或 IP 范围以及这些异常事件的严重级别。定义完成后，如果系统检测到的异常事件属于任何一类通知类型，系统会向此通知类型包含的用户发送邮件和短信等信息，从而方便用户及时掌握网络流量状态。如果不定义这些通知类型，异常流量信息出现时不会通知用户。

通知方式可以多选，比如可以在选择邮件通知的通知选择短信通知。被通知的用户也可以选择多个。

邮件通知需要配置系统的邮件功能，请进入系统管理，点击邮件配置。

短信通知需要配置系统的短信发送功能，请进入系统管理，点击短信配置。

9.1.6.2 检测范围

9.1.6.2.1 检测范围

检测指定的 IP 段的流量情况。如果不配置，系统默认检测通过路由器的所有 IP 的流量信息。当配置了一个或多个检测范围后，系统会优先检测这些 IP 范围，从而提高检测的效率和准确性

9.1.6.2.2 DarkIp

定义一个 IP 或 IP 段，当系统检测到的流量信息属于此 IP 或 IP 段时，系统会认为这些流量为异常流量，然后通知用户网络流量出现异常

9.1.6.2.3 私有 IP

定义一个 IP 或 IP 段，这些 IP 是不会被 Internet 分配的，它们在 Internet 上也不会被路由，如果系统检测到外网到内网的流量来自这些 IP 里的一个或多个，那么这些流量会被系统认为是异常流量

9.1.6.3 自定义监控

为流量分析里的自治域分析、协议分析、应用分析配置需要监控的自治域、协议或应用

9.1.6.3.1 应用个端口监控

配置需要监控的应用。配置完成后流量分析里的应用分析页面出现被监控的应用的流量

信息。此页面只显示被监控的应用，不显示其他的应用，如果想查看所有的应用信息，请进入运行配置里的对照表管理，选择 IP 应用端口对照表查看。当停止监控一个应用后，列表里就不会显示此应用，而且应用分析页面也不会出现此应用的流量信息

9.1.6.3.2 协议监控

配置需要监控的协议。配置完成后流量分析里的协议分析会展示所有被监控的协议的流量信息。列表页面只显示被监控的协议，停止监控某个协议后，列表里不会显示此协议

9.1.7 运行配置

9.1.8 设备管理

主要针对路由设备、路由设备接口、服务器和服务器接口进行配置，包括它们的添加、修改、删除、状态控制以及 SNMP 采集状态的控制等包括：路由器设置、服务器设置、路由器流量定义

9.1.8.1 路由器管理

新增:

路由器可以手动创建，点击【新增】按钮，既可以添加路由器设备。新增路由器设备时可以输入必填属性和非必填属性。

必填属性:设备地址，设备名称，厂家，flow 版本，snmp 版本，snmp 端口,采样率,snmp 团体字符串

非必填属性:描述

编辑:

在路由器列表中选中欲编辑的路由器设备，点击【编辑】按钮，既可以编辑选中的路由器设备。路由器的所有属性均可编辑。

删除:

在路由器列表中选中欲编辑的路由器设备，点击【删除】按钮，既可以删除选中的路由器设备。可支持批量删除。删除路由器或删除当前路由器下的接口信息。

点击【启用 snmp】按钮，则对 snmp 监控的路由器设备扫描接口信息。

修改路由设备接口信息:

在设备列表中，展开路由设备接口列表并单击某个接口的名称，弹出修改路由接口信息的对话框。即可修改路由设备接口信息。

修改路由设备接口方向:

在设备列表的”接口”一栏下，单击”接口”弹出修改路由设备接口方向的对话框，即可修改路由设备接口方向。

9.1.8.2 2.19.3.1.2 服务器管理

新增:

服务器可以手动创建，点击【新增】按钮，既可以添加服务器设备。新增服务器设备时可以输入必填属性和非必填属性。

必填属性:服务器地址,服务器名称,服务器系统类型,snmp 版本,snmp 端口,带宽 ,snmp 团体字符串

非必填属性:描述

其中服务器操作系统类型，目前只支持对 Windows 的 snmp 监控，如果选择其他系统类型则 snmp 端口，snmp 团体字符串，带宽的值都采用默认值不能修改。

编辑:

在服务器列表中选中欲编辑的服务器设备，点击【编辑】按钮，既可以编辑选中的服务器设备。服务器的所有属性均可编辑。

删除:

在服务器列表中选中欲编辑的服务器设备，点击【删除】按钮，既可以删除选中的服务器设备。可支持批量删除。 删除服务器将删除当前服务器下的所有接口信息。

修改服务器接口信息:

在服务器列表中，展开服务器接口列表并单击某个接口名称，弹出修改服务器接口信息的对话框。

关于服务器的接口在添加服务器的时候默认扫描接口。

9.1.8.3 2.19.3.1.3 路由流量定义

这里有两种方案，在项目初始化时就默认采用方案一，用户可以启用两种方案中的其中一个。这里选中的方案将影响流量分析模块的流量计算。

9.1.9 设备组管理

主要针对路由器组，路由器接口组进行配置，包括它们的添加、修改、删除等。

9.1.9.1 2.19.3.2.1 路由设备组管理

新增:

路由设备组可以手动创建，点击【新增】按钮，既可以添加路由设备组。新增路由设备组时可以输入必填属性和非必填属性。

必填属性:设备组名称

非必填属性:路由设备，描述

这里的路由设备是在设备管理中添加的路由设备。

编辑:

在路由设备组列表中选中欲编辑的路由设备组，点击【编辑】按钮，既可以编辑选中的路由设备组。路由设备组的所有属性均可编辑。

删除:

在路由设备组列表中选中欲编辑的路由设备组，点击【删除】按钮，既可以删除选中的路由设备组。

9.1.9.2 2.19.3.2.2 路由接口组

新增:

路由接口组可以手动创建，点击【新增】按钮，既可以添加路由接口组。新增路由接口组时可以输入必填属性和非必填属性。

必填属性:接口组名称

非必填属性:设备信息，描述

这里的设备信息是在设备管理中添加的路由设备。其中的一行代表一个路由设备，其中的上行树代表这个路由设备的所有上行口；下行树代表这个路由设备的所有下行口。

编辑:

在路由接口组列表中选中欲编辑的路由接口组，点击【编辑】按钮，既可以编辑选中的路由接口组。路由接口组的所有属性均可编辑。

删除:

在路由接口组列表中选中欲编辑的路由接口组，点击【删除】按钮，既可以删除选中的路由接口组。

9.1.10 对照表管理

保存和系统相关的一些基本信息，如 IP 资产信息、IP 应用端口信息、自治域信息。其中一些信息是系统预置的，不可删除，另一部分是自定义的，允许删除

9.1.10.1 IP 资产对照表

配置被监控的硬件设备的名称和 IP 地址或 IP 段的对应关系，配置完成后会在其他用到此设备的页面显示设备的名称，而不是显示此设备的 IP 地址或 IP 段，如果点击设备的名称会显示设备的详细信息。

9.1.10.2 IP 应用端口对照表

保存应用名称和对应的协议和端口号的对应关系。一个应用包含特定的一个或几个协议和端口号，配置此信息后在自定义监控等用到应用端口信息的地方会显示应用名称，而不是显示此应用的协议信息和端口信息。

应用端口信息分两类，一类是系统预置的应用端口信息，另一类属于自定义类型。预置

的应用端口信息不允许删除和编辑。一个应用可能包含多个协议和端口，通过选择不同的协议，填入不同的端口号可添加多个协议和端口，另外每个应用都有一个监控状态，如果是监控状态，那么流量分析功能会展示此应用的流量信息，修改此状态请通过策略管理-自定义监控-应用端口监控完成

9.1.10.3 自治域对照表

配置自治域编号和自治域详细信息的对应关系，配置完成后在流量分析功能里的自治域分析或者自定义监控里的自治域监控等页面里，用到自治域信息的地方会显示自治域的具体名称，而不是显示自治域编号，并且点击自治域名称会弹出自治域的具体描述等详细信息。

自治域信息也包含两种类型，一种是系统预置自治域，不能删除或编辑；另外一种是自定义自治域，就是通过页面添加的，允许删除或编辑。

9.1.11 高级配置

9.1.11.1 镜像流分析配置

镜像流分析配置跟路由器的镜像配合使用，使程序收到的流量是 netflow 格式的，这种用法主要是用在路由器自身不能发送 Netflow 格式的流量，如果路由器自己可以发 Netflow，就不用镜像流分析配置。

镜像流分析配置的属性包括：

启用：非必填

本地设备：必填，设置本地网络 IP

端口：必填，设置本地网络端口。

并发条数：必填，设置并发条数。

采样率：必填，设置采样率。

IP 段：非必填。设置 IP 段。

Input：必填，设置输入端口。

Ouput：必填，设置输出端口。

路由设备：必填，设置路由设备。

10 权限

系统采用基于角色的权限控制机制，即系统只对角色分配权限，用户只能通过拥有一个或者多个角色来获取权限，而不能直接对用户分配权限。

每个用户在创建的时候可以被赋予相应的角色权限。

用户可以有一个或者多个角色，也可以没有任何角色，没有任何角色则表示没有任何权限，用户可以登录系统，但不能访问任何内容。

如果用户所具有的角色被管理员删除，那么该用户就不再具有相应的权限，需要管理员对该用户重新分配角色。

目前系统按模块分配权限，有的模块还可以分配子模块的权限，部分模块的权限可以控制到树结点。

目前支持的操作有读、写、导出。用户只有具有导出权限，才可以下载，导出。

注：对于树形结点的权限来说，如果用户有了树形结点的根结点或组结点的权限，则拥有该根结点或组结点下的所有子结点的权限，包括新增加的子结点的权限。

10.1 内置角色与用户

本系统基于三权分立设计。默认的内置了三个角色，请登录后立即修改口令：

1. 系统管理员：具备系统配置，日志审计操作的权限，对应的内置用户名与口令为：sysadmin/venus.sysadmin
2. 用户管理员：具备用户管理和权限管理操作的权限，对应的内置用户名与口令为：useradmin/venus.useradmin
3. 审计管理员：具备对系统操作进行审计的权限，对应的内置用户名与口令为：auditor/venus.auditor

系统权限管理的操作必须由用户管理员及其授权的管理员进行。

10.2 用户管理

10.2.1 新增用户

点击用户列表上方的工具条中的【添加】按钮，会进入新增用户的页面，新增用户的属性包括：

登陆用户名：新用户的登陆名称，必填，(用户名由 6-64 个字母、数字或'_'组成,且不能以'_'开头和结尾)

1. 真实姓名：新用户的真实名称，必填
2. 登录密码：新用户的密码，必填

3. 确认密码：再次确认新用户的密码，必填
4. 联系电话：用户的电话号码
5. 手机：用户的移动电话号码
6. 电子邮箱：用户电子邮箱地址
7. 描述信息：此用户的说明
8. 角色信息：在添加用户的时候，同时将用户与现有的角色关联

添加操作完成后，用户列表会及时更新，列表中显示新添加的用户。

10.2.2 编辑用户

点击用户列表最后一列中的工具条中的【编辑】按钮，可以对用户的属性进行编辑。

10.2.3 删除用户

点击用户列表上方的工具条中的【删除】按钮，可以删除选中的用户，支持批量删除。

删除用户会同时将用户与角色的关联关系删除。

删除后，用户列表同时刷新。

10.2.4 锁定和解锁用户

用户在一分钟内，连续登录失败的次数达到一定数目，会被锁定一段时间。用户可以在锁定时间过后，再次尝试登录系统，也可以通知用户管理员解锁。

点击用户列表最后一列中的工具条中的【解锁】按钮，可以将锁定的用户解锁。

10.3 角色管理

10.3.1 新增角色

点击角色列表上方的工具条中的【新增】按钮，会进入新增角色的页面，新增角色的属性包括：

1. 角色名称：新角色的名称，必填
2. 角色描述：新角色的描述
3. 用户：此处可以点击【新增用户】将系统中的已有用户跟新建角色关联，或者点击【删除用户】删除角色跟用户的关联关系
4. 权限信息：配置角色的权限信息。

目前系统按模块分配权限，有的模块还可以分配子模块的权限，部分模块的权限可以控制到树结点。

目前支持的操作有读、写、导出。用户只有具有导出权限，才可以下载，导出。

注：对于树形结点的权限来说，如果用户有了树形结点的根结点或组结点的权限，则

拥有该根结点或组结点下的所有子结点的权限，包括新增加的子结点的权限。

添加操作完成后，角色列表会及时更新，列表中显示新添加的角色。

10.3.2 编辑角色

点击角色列表最后一列中的工具条中的【编辑】按钮，可以对角色的属性进行编辑，编辑的属性跟新增权限时相同。

10.3.3 删除角色

点击角色列表上方的工具条中的【删除】按钮，可以删除选中的角色，支持批量删除。

删除后，角色列表同时刷新。

删除角色会同时将用户与角色的关联关系删除。

11 附录

11.1 常用命令

本产品可以使用这些命令：

命令以及参数	描述
tsoc -h	显示帮助信息
tsoc --start *servicename*	启动服务(未给出参数 servicename 时，启动 tsoc 服务)
tsoc --stop *servicename*	停止服务(未给出参数 servicename 时，停止 tsoc 服务)
tsoc --restart *servicename*	重启服务(未给出参数 servicename 时，重启 tsoc 服务)
tsoc --status *servicename*	显示服务状态(未给出参数 servicename 时，显示 tsoc 服务状态)
tsoc -U	升级系统
tsoc -R	恢复系统，保留 license 使用记录和用户数据
tsoc -Rtf	恢复出厂设置，删除用户数据
tsoc -E	导出系统日志文件(导出到/home/admin/data/tsoc.log.zip)
tsoc -P	修改 admin 用户密码
tsoc -d	配置 DNS 服务器
tsoc -N *hostname*	修改主机名
tsoc --rmEvent *true/false*	启动/停止当磁盘使用容量达到 80%时，自动删除最早的归档数据的功能
tsoc --repair_DB	修复数据库表
tsoc --restore_DB	恢复数据库
tsoc --snmpShow	显示 snmp 的指定属性值
tsoc --snmpModify	修改指定的 snmp 属性值
网络配置	
tsoc -i	显示接口信息，参数可选
-e	配置网卡参数
-p	配置 IP 地址
-m	配置子网掩码
备注：这些参数是中，-e 是必须的，用来指定第几个接口，另外三个可以和-e 进行组合。	

如：tsoc -e eth0 -p *ip* -m *mask*	
tsoc --modifyGate	配置默认网关
tsoc --route	显示路由表信息
tsoc --addroute	添加路由
tsoc --delroute	删除路由
系统操作	关机
tsoc --poweroff	重启
tsoc --reboot	

11.2 需要开放端口列表

需要开放的端口：

端口号	协议	描述
8888	TCP	向外提供 Web 访问
8443	TCP	配置 https 访问时需要开放 8443 端口
514	TCP/UDP	用于接收 syslog 日志
8514	TCP/UDP	接收转发的日志
8034	UDP	级联通讯
22	TCP	提供 SSH 服务供远程访问
161	UDP	用于收发 SNMP 信息
162	UDP	用于接收 SNMP Trap
199	TCP	SNMP V3 远程监控端口,用于本机能被网管设备监控，可酌情开放
2100	TCP	FTP 服务,供上传升级包使用