百卓网络 Smart 产品

用户手册 V2.0

北京百卓网络技术有限公司

商标、版权声明

“百卓网络”、“百卓”、“byzoro”、“PatrolFlow”、“PatrolVision”、“PatrolLink”“PatrolGuard”以上均为北京百卓网络技术有限公司注册商标。本产品的所有部分，包括配件和软件，其版权都归北京百卓网络技术有限公司所有，未经北京百卓网络技术有限公司书面许可，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。可随时查阅我们的公司网站 www.byzoro.com。北京百卓网络技术有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但北京百卓网络技术有限公司不对本手册中的遗漏、不准确或错误导致的损失和损害承担责任。

目录

第一章：手册简介

首先感谢您购买使用 Smart 系列产品。本系列产品可基于 Web 界面来进行管理和配置，使用方便简捷。在安装使用产品之前，请先仔细阅读本手册，以便更好的使用 Smart 产品。本手册的主要目的是帮助读者快速完成网络设置，通过设备实现内网计算机与互联网的高速连接，如果您想对内网计算机做更多的监控，请详细阅读随机光盘的用户手册。

读者对象

本手册的读者对象为安装 Smart 的工程技术人员，以及配置和管理 Smart 的系统管理员。本手册需要读者熟悉路由器、广域网、内网的相关知识。

手册约定

1、手册中有关图标的约定如下：

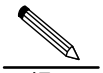
图标	说明
	这个图标主要是警告用户，如果采用不正确的方式操作设备，可能会对人体或设备造成伤害，或造成业务中断、数据丢失等。
	这个图标表示提醒用户注意事项。
	这个图标主要给出一些与正文相关的信息，同时给用户一些指引，帮助用户更好的理解正文的内容。

2、手册中在 Smart 管理界面中相关约定如下：

符号	说明
【 】	带有方括号【】表示界面中的按钮名，如单击【确认】按钮
< >	带有< >表示菜单名或者窗口名。
\	多级菜单采用\隔开。如windows的“\Program Files\Tencent\qq”菜单

获取技术支援

北京百卓网络技术有限公司在中国的技术支持为两级架构，技术支持团队包括百卓网络厂家工程师和百卓网络签约的代理商、授权集成商的认证工程师，共同为用户提供两级的技术支持服务。客户可以登录北京百卓网络技术有限公司网站 www.byzoro.com获取服务支持热线电话和邮箱。此外，客户还可通过北京百卓网络技术有限公司网站及时了解最新产品动态，以及下载需要的技术文档。



鉴于本系列产品安装配置方法类似，在本手册所提到的设备，如无特别说明，系指 Smart S80。由于各型号产品的硬件和软件规格略微存在一定的差异，所有涉及产品规格的问题需要请与北京百卓网络技术有限公司联系确认。

第二章：产品介绍

产品概述

Smart 系列产品是百卓网络专门为小型企业量身定制的上网行为管理设备。设备在功能设计上充分考虑小型企业对网络设备在高性价比方面的要求，将多种应用功能集成于一身，其中包括网络应用封堵、流量控制、链路负载均衡、网页分类阻断、上网内容审计、防火墙、VPN 等。Smart 产品集多种功能于一身，可有效减少网络建设成本、规范员工上网行为、提升网络带宽价值，避规企业接入互联网可能导致的潜在安全和法律风险、增强网络的稳定性和安全性。另外，设备还提供人性化的 WEB 配置界面并配以简易的网络开通设置参数，帮助网络管理员快速完成企业网络的开通任务，减少网络管理员的配置和维护时间。

关键特性

精准的应用识别

通过采用百卓网络独有的智能模式识别技术并结合业界领先的增强型 DPI(深度报文检测)技术，设备可精确识别各种网络应用及协议(包括各种采用跳跃端口、动态端口或经加密和代理后的网络应用及协议)，最大限度保证网络应用控制及信息内容审计结果的准确性。

强大的上网行为管理

设备内置实时更新的最全面的应用识别和 URL 分类库，具备基于关键字过滤各种网络信息内容(包括网络发帖、Email 及即时聊天等)的能力，并可以基于用户、组、时间、网络接口等多种条件的灵活组合制定灵活的控制策略，帮助网络管理者对网络用户实施最精确、灵活的上网行为管理决策，提高企业员工的工作效率。

专业的信息内容审计

设备提供专业的信息内容审计能力，管理者可定义内容审计策略(包括内容审计的深度)，设备根据所定义的审计策略详细记录用户的所有上网行为日志及网络访问信息内容，并提供简单易用的审计日志查询手段，帮助企业管理者全面掌握并快速定位与网络行为及信息内容相关的问题。

灵活的带宽管理策略

提供最大带宽、保证带宽、弹性带宽等多种带宽管理手段，并提供基于用户、应用、时间、网络接口等多种条件组合实施的带宽管理策略，使得网络管理者可以灵活控制网络用户的带宽使用规则，从而优化网络带宽利用，提升网络带宽的价值。

完善的链路管理手段

设备提供负载均衡、策略路由、智能路由选路等丰富的双 WAN 链路接入特性，可根据多种条件实现两条出口线路间的流量负载均衡，智能路由选路功能可以使设备在不同的出口线路上智能分配去往不同运营商的流量。策略路由功能则可指定不同的用户或应用走不同的线路，保证关键应用和用户的通讯质量。

强大的统计分析能力

设备提供以表格、饼图、柱状图、折线图等多种形式展现的网络信息统计分析报表、活跃度和访问频度排名信息及各种周期(周、月、季度等)的统计分析报告，分析对象全面覆盖流量、用户、用户组、应用、应用类别等。各种统计分析数据为网络管理者提供全面了解网络运行状况的手段，并为制定网络流量优化、上网行为管理等策略提供了科学的依据。

简易的设备管理

设备提供基于 HTTPS 安全协议的 WEB 管理界面、CLI 命令行配置界面、分级分权的设备管理授权。同时设备提供简易的网络开通配置参数，帮助网络管理员快速完成企业网络的开通配置参数，减轻网络管理员的配置和维护时间，有效削减管理成本，提高管理效率。

产品规格

型号	Smart S40	Smart S80
适用环境	50 用户以下	100 用户以下
防火墙吞吐量	50Mbps	70Mbps
最大并发连接数	60,000	80,000
安全处理器	400MHz	500MHz
内存	256M	512M
FLASH	64M	64M
硬盘	内置 80G 硬盘	内置 80G 硬盘
网络接口	4×10/100Base-T （2×WAN、2×LAN）	4×10/100Base-T （2×WAN、2×LAN）
外形尺寸	300×155×44mm	300×155×44mm
外壳材质	工业级钢壳	工业级钢壳
温度	0~50 ℃/32-122 ℉(工作温度)	-40-70 ℃/-40-158 ℉(贮存温度)
相对湿度	10%-90%无凝结(工作湿度)	5%-95%无凝结(贮存湿度)
电源	12VDC/1.5A	12VDC/1.5A
功耗	＜10W	＜10W
风扇	无风扇静音设计	无风扇静音设计

如需了解更多产品信息请登录 www.byzoro.com

第三章：硬件安装

面板布置

前面板

设备的前面板由以下几部分组成，如下图所示：

- 2 个外网口指示灯（WAN）
- 2 个内网口指示灯（LAN）
- 1 个电源状态指示灯（POWER）
- 1 个系统状态指示灯（SYSTEM）

设备前面板

后面板

设备的后面板由以下几部分组成，如下图所示：

- 2 个 100M 外网接口（WAN）
- 2 个 100M 内网接口（LAN）
- 1 个数据管理接口（USB）
- 1 个命令行配置串口（CONSOLE）
- 电源插孔用于连接随机附带的电源适配器（PWR）

设备后面板

指示灯说明

- 电源指示灯
  - 面板上的 POWER 指示灯
  - 指示灯亮，说明电源输入正常
  - 指示灯不亮电源输入异常，需要检测电源线连接是否正确
- 系统运行指示灯
  - 面板上的 SYSTEM 灯
  - 指示灯不亮或一直长亮说明系统有故障
  - 指示灯在系统初始化时长亮，系统正常工作时指示灯慢闪，每 1.6 秒闪亮一次
- 网络接口指示灯：
  - 有 4 个网络接口指示灯
  - 接口指示灯亮，表示链路连接正常；不亮，则说明链路连接不正常
  - 接口指示灯闪亮，表示端口收到了数据或者在发送数据

安装环境

Smart 产品工作环境要求如下：
输入电压：12V DC（直流）
输入电流：1.5A
温度：0～50℃
湿度：10～90%无凝结

为了保证设备长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的

设备良好接地可有效避免雷击所造成的设备损坏。

空气畅通和室温稳定。本产品符合关于环境保护方面的设计要求。

安装参数

设备安装

如果您希望将设备平放在桌子表面等平面物体上，请您将随机附带的橡胶脚垫粘附于设备底部的脚垫安装位置，以利于设备的散热和防滑。

如果您希望将设备安装在标准的 19 英寸机柜中，则借助设备随机附带的延长挂耳可以满足您的需求（如下图）。

加装挂耳效果图

电源连接

将随机附带的电源适配器与设备进行连接，前面板的 Power 灯（绿色）和 SYSTEM 灯(绿色)会点亮。大约 1—2 分钟后，SYSTEM 灯(绿色)闪亮，说明设备工作正常。

1. 如果 Power 灯不亮或者闪亮，请检测供电电源及电源适配器是否正常。
2. 如果开机 5 分钟后，SYSTEM 灯持续长亮，请关闭电源 5 分钟，然后重新上电。

网络连接

使用标准的 RJ-45 以太网线将 LAN 口与内部内网连接，LAN 口通常用于连接用户内部网络的核心交换机。

使用标准的 RJ-45 以太网线将 WAN 口与 Internet 互联网连接，WAN 口通常用于连接用户网

为了尽量减少影响，建议先按照实际需求对 Smart 进行正确配置后再接入实际网络中。

络的出口路由器、ADSL Modem 或直接运营商所提供的专线等。

安全注意事项

进行各种操作时，请遵守所在地的安全规范及相关设备和产品的安全指示，本手册介绍的注意事项只作为补充。

1. 直接接触或通过潮湿物体间接接触高压、市电，可能带来致命危险。
2. 不规范、不正确的高压操作可能引起火灾和电击等意外事故，并对设备和人体造成严重、致命的伤害。
3. 进行电气操作时，必须遵守所在地的法规和规范。相关工作人员必须具有相应的高压、交流电等作业资格。
4. 对交流电源设备及电源线等进行操作时，严禁佩戴手表、手镯、戒指等易导电物体。
5. 注意对设备防潮防水，一旦发生进水或潮湿现象，应立即切断电源。
6. 进行电气操作时，必须使用专用工具。

电气安全操作

人体产生的静电会损害设备上的静电敏感元器件。在接触设备之前必须配带防静电手腕，并将防静电手腕的另一端良好接地。

避免静电损害

警告

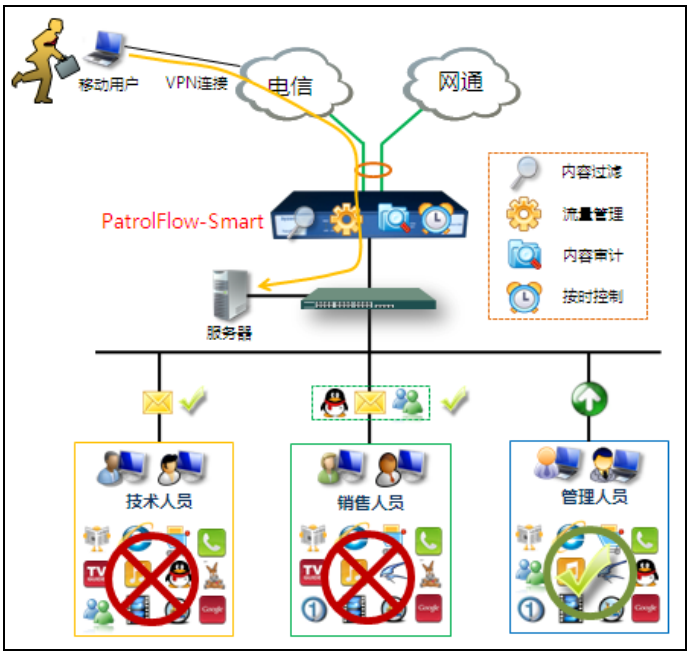
对光纤进行操作时，严禁肉眼靠近或直视光纤出口，避免激光损伤眼睛。

避免激光损害

第四章：接入模式简介

Smart 系列产品支持多种接入模式，可根据用户的实际需求串接在网络中并设置为网关模式或透明桥接模式，还可工作于审计模式以旁路方式接入网络中。

路由模式

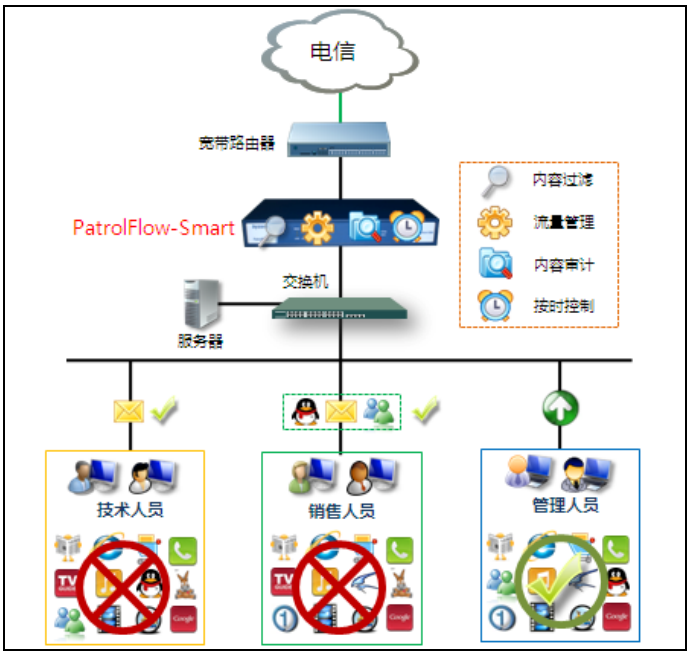


路由模式组网示意图

组网特点：

只需一台设备即可同时实现双线接入、负载均衡、应用控制、带宽控制、VPN、内容过滤、上网行为及内容审计等功能，从而增强企业网络安全性、提高员工工作效率、增加带宽价值、减少建网成本。

桥接模式

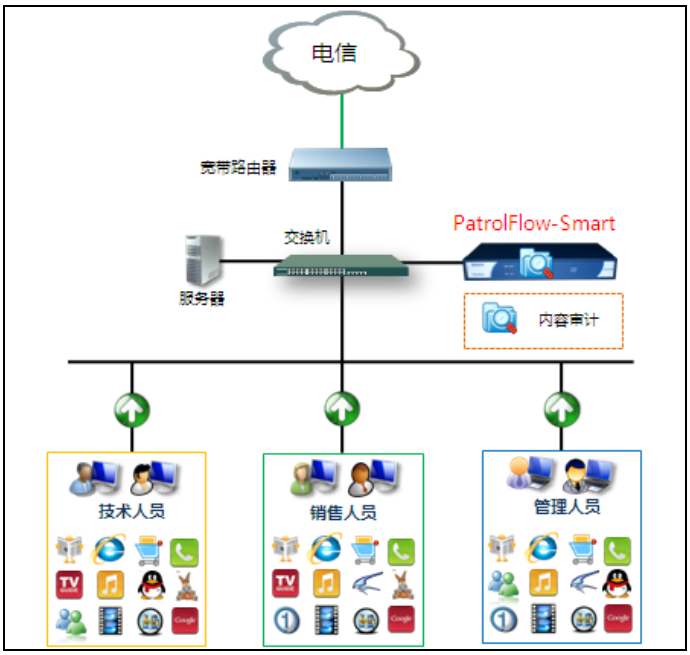


桥接模式组网示意图

组网特点：

将设备串接在原有网络出口设备与网络交换机之间，使得网络管理者可以对内网用户进行应用控制、带宽控制、内容过滤、上网行为及内容审计等控制和管理，并由此增强企业网络安全性、提高员工工作效率、增加带宽价值。

旁路模式



旁路模式组网示意图

组网特点：

设备以旁路模式接入到原有网络中，通常接在企业中与网络出口设备（如宽带路由器、防火墙等）相连的交换机的镜像接口上。该模式下设备的接入完全不影响原有网络的运行，也不需要改变原有网络的拓扑。但本模式下设备仅能实现对内网用户的互联网访问行为及访问内容的审计，无法对用户进行任何的控制和管理。本模式适用于仅需要对网络行为和内容进行审计，而无需进行控制的场合。

第五章：快速安装使用指南

设备出厂默认参数

设备出厂即已具备以下配置信息：

- WAN0 口出厂配置信息：
  - 默认状态为通过 DHCP 从外网自动获取地址
- WAN1 口出厂配置信息：
  - 默认状态为通过 DHCP 从外网自动获取地址
- LAN0 口出厂配置信息：

- 接口 IP 地址：192.168.1.254/255.255.255.0
- 默认开启 DHCP 服务器功能，可通过本接口自动为内网主机分配 192.168.1.100－192.168.1.200 的 IP 地址。

■ LAN1 口出厂配置信息：
- 接口 IP 地址：192.168.2.254/255.255.255.0
- 默认开启 DHCP 服务器功能，可通过本接口自动为内网主机分配 192.168.2.100－192.168.2.200 的 IP 地址。

■ 地址转换功能（NAT）：
- 默认开启 NAT 功能
- 所有从内网到外网的流量均进行 NAT 转换

■ 设备默认管理链接：
- https://192.168.1.254:8443（LAN0 口）
- https://192.168.2.254:8443（LAN1 口）

■ 设备默认登录信息
- 登录账号：admin
- 登录密码：admin

如果您的网络使用情况满足上述设备出厂默认的配置要求，则您只需将 Smart 设备正确连接到网络中即可正常使用。否则您需要参照以下章节内容根据自身实际网络情况对设备进行适当的配置。

建立正确的管理设置

Smart 产品具有默认的设备管理地址（见上述章节内容）和登录信息。这些值可以根据您的实际需要而改变，但为了描述方便在本手册中将按设备出厂默认值描述配置参数。

为了能够登录设备并根据您的网络实际需求配置各项参数，您必需首先正确建立与设备的管理连接，建立连接的参数如下：

请使用标准 RJ-45 网线将您用于管理设备的计算机与设备的 LAN0 口（或 LAN1 口）相连，然后将您计算机的 IP 地址获取方式设置为自动获取 IP 地址。在正确设置好计算机的 IP 地址参数后，您可以通过 Ping 命令检查计算机与 Smart 设备之间是否已经正常连通。下面以 Windows XP 操作系统为例说明如何执行 Ping 命令来检测连通性：在 Windows XP 桌面中依次选择“开始\所有程序\附件\命令提示符”，在下图所示命令行操作界面中输入：ping 192.168.1.254（如果你的计算机连接在设备的 LAN1 口，请执行 ping 192.168.2.254），如果界面显示为：

```
C:\Documents and Settings\Administrator>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=3ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

连接 LAN0 口时 Ping 命令结果

```
C:\Documents and Settings\Administrator>ping 192.168.2.254

Pinging 192.168.2.254 with 32 bytes of data:

Reply from 192.168.2.254: bytes=32 time=1ms TTL=64
Reply from 192.168.2.254: bytes=32 time<1ms TTL=64
Reply from 192.168.2.254: bytes=32 time<1ms TTL=64
Reply from 192.168.2.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

连接 LAN1 口时 Ping 命令结果

那么恭喜您！您的计算机已与 Smart 成功建立连接，您将可以继续完成下述章节中有关设备配置的工作。如果屏幕显示如下：

```
C:\Documents and Settings\Administrator>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

管理连接不正确

这说明您的计算机还未与 Smart 设备成功建立连接，您需要从以下几个方面去检查：

1、确认硬件连接是否正确

1. 确保计算机网卡接口与 Smart 的 LAN 口均是点亮的（有数据传输时是闪亮）。
2. 确保您的计算机正在与设备的 LAN 口（LAN0 或者 LAN1 口）连接而不是与 WAN 口相连，同时请注意不同的 LAN 接口具有不同的管理 IP 地址。

注意

LAN0 口管理 IP 地址为：192.168.1.254

LAN1 口管理 IP 地址为：192.168.2.254

2、确认计算机的 TCP/IP 设置是否正确

可以通过 IPconfig 命令检查，如下图所示即为正确：

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.200
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254
```

连接 LAN0 口时的 IP 配置信息

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.200
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.254
```

连接 LAN1 口时的 IP 配置信息

登录设备

当您按照上述参数完成与设备的管理连接配置后，你就已经为管理和配置设备做好了必要的准备。至此您将可以登录设备的 WEB 管理页面按配置页面的提示信息以及您自身的网络管理需求对设备进行必要的配置。设备登录参数如下：

打开您计算机的 WEB 浏览器（如 IE、火狐、腾讯 TT、傲游等），在浏览器地址栏中输入并访问 https://192.168.1.254:8443（此处假设你的管理计算机连接在设备的 LAN0 口，如果您的管理计算机连接在设备的 LAN1 口，请输入 https://192.168.2.254:8443）。

提示

1. 登录时请务必完整输入 https://192.168.1.254:8443。(请注意是：**https**)
2. 如果在确认管理计算机配置及网络连接一切正常情况下仍无法登录设备，请检查您的浏览器设置是否设置了“代理服务器”选项。如设置了该选项，在设备配置过程中请将其取消。

如果您的管理计算机能够与设备建立正确的登录连接，您将会看到如下图所示的设备登陆界面。通过该登陆界面对话框您可以输入设备的登录用户名和密码（设备出厂默认的登录用户名和密码均为小写的：admin），然后点击【登录】按钮登录设备。

设备登录界面

如果输入的登录用户名和密码正确，如下图浏览器将进入设备配置界面。Smart 配置界面的左侧为主配置菜单选项栏，用户可该菜单栏中选择需要进行配置的菜单选项。而配置界面右侧为设备参数配置及信息显示区域，用户可在此区域内配置、修改和查看设备的各项参数及信息。

设备配置界面

设备登录后的首要显示页面为“系统状态”信息页面，该页面将为您提供有关设备型号、工作模式、软件版本、运行时间、CPU 负载、内存，硬盘使用率等设备基本信息，并进一步提供用户流量、应用流量、连接数等排名信息以及设备接口流量及状态等统计信息。通过综合观察该页面所提供的信息内容，网络管理员可以快速了解设备及网络的当前运行状况，为以后的设备管理和网络管理提供依据。

使用向导配置设备

为了简化设备的配置复杂度，并帮助网络管理员快速开通网络，设备提供以下 5 种应用场景的配置向导：以太网宽带(动态 IP+NAT)、以太网宽带(静态 IP+NAT)、虚拟拨号 (PPPoE+NAT)、透明桥接、旁路审计。这 5 个配置向导所适用的网络使用环境如下，您可以根据自己的实际网络使用环境选择适当的配置向导快速配置设备：

以太网宽带(动态 IP+NAT)

如果您申请的出口线路是通过 DHCP 从运营商处动态获取 IP 地址的以太网宽带线路，同时您希望通过 Smart 设备连接网络出口线路，使得内部网络中的主机都能共享上网，请选择该模式。

以太网宽带(静态 IP+NAT)

如果您申请的出口线路是静态 IP 地址的以太网宽带线路，并且您希望通过 Smart 设备连接网络出口线路，使得网络中的主机都能共享上网，请选择该模式。

虚拟拨号 (PPPoE+NAT)

如果您申请的出口线路是 PPPoE 虚拟拨号线路(通常为 ADSL 线路)，并且您希望通过 Smart 设备连接网络出口线路，使得网络中的主机都能共享上网，请选择该模式。

透明桥接

如果您是在现有网络中部署 Smart 设备，并且您希望在不替现有网络设备的情况下，使用 Smart 设备控制网络用户的应用和流量并对网络用户的上网行为和网络访问内容监控和分析，请选择该模式。本模式下 Smart 设备通常串接在出口路由器(或防火墙)和企业内网主交换机之间。

旁路审计

如果您只希望使用 Smart 设备对内部网络中的应用、流量及员工上网行为、网络访问内容等信息进行监控和分析，请选择该模式。审计模式下设备无法对应用和流量进行控制。

以太网宽带(动态 IP+NAT)

要使用配置向导完成“以太网宽带(动态 IP+NAT)”的功能配置，请在配置界面左侧的主菜单栏中选择＜基础配置＞→＜配置向导＞，如下图所示：

配置向导

在上图的应用模式选择页面中选择“以太网宽带(动态 IP+NAT)”，并点击【下一步】按钮，进入该应用模式的接口配置页面（如下图），在该配置页面中我们需要选定用于连接运营商线路的外网接口（WAN0/WAN1）以及连接内部网络的内网接口（LAN0/LAN1）。由于在本应用模式中外网口为通过 DHCP 动态获取地址，因此无需进行参数配置，本例中我们选择 WAN0 口作为连接运营商网络的外网接口。而对于 LAN 口我们需要根据用户网络的 IP 地址规划为其配置 IP 地址和子网掩码，通常情况下 LAN 口所配置的 IP 地址即为内网用户主机的网关地址。本例中 LAN0 口 IP 地址为 10.0.0.1，子网掩码为 255.255.255.0。

接口参数配置

如果您希望通过设备为内网用户动态分配 IP 地址，则您可以通过勾选 LAN 口配置页面中的“使用 DHCP 配置”选项开启内网接口上的 DHCP 服务器功能，并指定可分配给内网用户的 IP 地址范围及 DNS 参数（如下图）。

接口参数配置（使用 DHCP 动态分配 IP 地址）

配置项及其说明（内网口）：

配置参数	说明
IP 地址	设置 LAN 口的 IP 地址
子网掩码	设置 LAN 口的子网掩码
使用 DHCP 配置	启用指定 LAN 口的 DHCP 服务器功能
起始 IP 地址	设置 DHCP 服务器自动分配 IP 地址的起始地址，该地址必需与指定 LAN 口 IP 地址设置在同一网段。

结束 IP 地址	设置 DHCP 服务器自动分配 IP 地址的起始地址，该地址必需与指定 LAN 口 IP 地址设置在同一网段，并且结束 IP 地址必须大于起始 IP 地址。
DNS 服务器 1	设置 DNS 服务器地址，允许留空。
DNS 服务器 2	设置备用 DNS 服务器地址，允许留空。如果两个 DNS 选项均留空则您需要在用户电脑上手动配置 DNS 服务器方可保证其能够正常访问互联网。

提示

1. 在配置向导中你只能同时配置一个外网口和一个内网口的参数。
2. LAN 口上开启 DHCP 服务器功能时，DHCP 客户端分配得到的网关地址即为该 LAN 口上配置的 IP 地址。

完成上述接口参数配置后，点击页面下方的【下一步】按钮进入下图所示的带宽管理配置页面。

带宽管理

在此配置页面中，您可以通过配置“每用户最大带宽”选项为网络中的每台主机指定最大使用带宽，您还可以分别指定整个网络中的 P2P 下载、P2P 流媒体、HTTP 流媒体应用的最大使用带宽。

提示

1. 如果您不想对用户或某些应用的带宽进行限制，您可以将用户或应用的上、下行带宽输入框留空（不输入任何数值）。
2. 为了限制用户或应用的带宽，您必须同时指定用户或应用的上、下行带宽值。
3. 上行或下行带宽值输入为 0 则表示限制该方向上的所有流量。
4. 如果您需要了解各应用类中的详细应用，请点击其后的“查看详细应用”链接。

完成带宽管理配置后，点击页面中的【下一步】按钮进入下图所示的应用控制配置页面。

应用控制

在本配置页面中你可以通过勾选相应的应用类以禁止网络中的所有用户使用该应用类中的

提示

如果您需要了解各应用类中的详细应用，请点击其后的“查看详细应用”链接。

应用。

内容审计配置

配置向导的最后一步是配置内容审计功能，如果您需要记录和查看内部网络中用户的上网行为及互联访问日志（如发帖内容、网页浏览、邮件内容、聊天内容等），那么您需要开启设备的内容审计功能。

一旦您完成上述所有参数的配置，并点击页面中的【完成】按钮，设备将立即自动重启并使用您新配置的参数进行工作。至此，“以太网宽带(动态 IP+NAT)”应用模式的设备端配置工作全部完成。您只需按实际网络环境要求将设备连接到网络中，并正确配置内网中各主机的网络参数即可正常上网。

以太网宽带（静态IP+NAT）

要使用配置向导完成“以太网宽带(静态 IP+NAT)”的功能配置，请在配置界面左侧的主菜单栏中选择＜基础配置＞→＜配置向导＞选项。如下图所示：

配置向导

在上图的应用模式选择页面中选择“以太网宽带(静态 IP+NAT)”，并点击【下一步】按钮，进入该应用模式的接口配置页面（如下图），在该配置页面中我们需要选定用于连接运营商线路的外网接口（WAN0/WAN1）以及连接内部网络的内网接口（LAN0/LAN1）。为了使得网络能够正常使用请您按照运营商所提供真实数据配置外网口的各项参数，本例中我们选择 WAN0 口作为连接运营商网络的外网接口。而对于 LAN 口我们需要根据用户网络的 IP 地址规划为其配置 IP 地址和子网掩码，通常情况下 LAN 口所配置的 IP 地址即为内网用户主机的网关地址。本例中 LAN0 口 IP 地址为 10.0.0.1，子网掩码为 255.255.255.0。

接口参数配置

如果您希望通过设备为内网用户动态分配 IP 地址，则您可以通过勾选 LAN 口配置页面中的

“使用 DHCP 配置”选项开启内网接口上的 DHCP 服务器功能，并指定可分配给内网用户的 IP 地址范围及 DNS 参数（如下图）。

接口参数配置（使用 DHCP 动态分配 IP 地址）

配置项及其说明（外网口）：

配置参数	说明
IP 地址	设置 WAN 口的 IP 地址
子网掩码	设置 WAN 口的子网掩码
缺省网关	设置网关地址，如果不清楚，可向 ISP 咨询。
DNS 服务器	设置 DNS 服务器地址，通常由 ISP 提供，必须配置。
备用 DNS 服务器	设置备用 DNS 服务器地址，通常由 ISP 提供，允许留空。

配置项及其说明（内网口）：

配置参数	说明
IP 地址	设置 LAN 口的 IP 地址
子网掩码	设置 LAN 口的子网掩码
使用 DHCP 配置	启用指定 LAN 口的 DHCP 服务器功能
起始 IP 地址	设置 DHCP 服务器自动分配 IP 地址的起始地址，该地址必需与指定 LAN 口 IP 地址设置在同一网段。
结束 IP 地址	设置 DHCP 服务器自动分配 IP 地址的起始地址，该地址必需与指定 LAN 口 IP 地址设置在同一网段，并且结束 IP 地址必须大于起始 IP 地址。
DNS 服务器 1	设置 DNS 服务器地址，允许留空。

DNS 服务器 2	设置备用 DNS 服务器地址，允许留空。如果两个 DNS 选项均留空则您需要在用户电脑上手动配置 DNS 服务器方可保证其能够正常访问互联网。

提示

1. 在配置向导中你只能同时配置一个外网口和一个内网口的参数。
2. LAN 口上开启 DHCP 服务器功能时，DHCP 客户端分配得到的网关地址即为该 LAN 口上配置的 IP 地址。

完成上述接口参数配置后，点击页面下方的【下一步】按钮进入下图所示的带宽管理配置页面。

带宽管理

在此配置页面中，您可以通过配置“每用户最大带宽”选项为网络中的每台主机指定最大使用带宽，您还可以分别指定整个网络中的 P2P 下载、P2P 流媒体、HTTP 流媒体应用的最大使用带宽。

提示

1. 如果您不想对用户或某些应用的带宽进行限制，您可以将用户或应用的上、下行带宽输入框留空（不输入任何数值）。
2. 为了限制用户或应用的带宽，您必须同时指定用户或应用的上、下行带宽值。
3. 上行或下行带宽值输入为 0 则表示限制该方向上的所有流量。
4. 如果您需要了解各应用类中的详细应用，请点击其后的“查看详细应用”链接。

完成带宽管理配置后，点击页面中的【下一步】按钮进入下图所示的应用控制配置页面。

应用控制

在本配置页面中你可以通过勾选相应的应用类以禁止网络中的所有用户使用该应用类中的

如果您需要了解各应用类中的详细应用，请点击其后的“查看详细应用”链接。

应用。

内容审计配置

配置向导的最后一步是配置内容审计功能，如果您需要记录和查看内部网络中用户的上网行

为及互联访问日志（如发帖内容、网页浏览、邮件内容、聊天内容等），那么您需要开启设备的内容审计功能。

一旦您完成上述所有参数的配置，并点击页面中的【完成】按钮，设备将立即自动重启并使用您新配置的参数进行工作。至此，“以太网宽带(静态 IP+NAT)”应用模式的设备端配置工作全部完成。您只需按实际网络环境要求将设备连接到网络中，并正确配置内网中各主机的网络参数即可正常上网。

虚拟拨号(PPPoE+NAT)

要使用配置向导完成“虚拟拨号(PPPoE+NAT)”的功能配置，请在配置界面左侧的主菜单栏中选择＜基础配置＞→＜配置向导＞选项。如下图所示：

配置向导

在上图的应用模式选择页面中选择“虚拟拨号(PPPoE+NAT)”，并点击【下一步】按钮，进入该应用模式的接口配置页面（如下图），在该配置页面中我们需要选定用于连接运营商线路的外网接口（WAN0/WAN1）以及连接内部网络的内网接口（LAN0/LAN1）。为了使得网络能够正常使用请您正确配置 PPPoE 拨号所需的账号及密码，本例中我们选择 WAN0 口作为 PPPoE 拨号的外网接口。而对于 LAN 口我们需要根据用户网络的 IP 地址规划为其配置 IP 地址和子网掩码，通常情况下 LAN 口所配置的 IP 地址即为内网用户主机的网关地址。本例中 LAN0 口 IP 地址为 10.0.0.1，子网掩码为 255.255.255.0。

接口参数配置

如果您希望通过设备为内网用户动态分配 IP 地址，则您可以通过勾选 LAN 口配置页面中的“使用 DHCP 配置”选项开启内网接口上的 DHCP 服务器功能，并指定可分配给内网用户的 IP 地址范围及 DNS 参数（如下图）。

接口参数配置（使用 DHCP 动态分配 IP 地址）

配置项及其说明（外网口）：

配置参数	说明
PPPoE 账号	PPPoE 拨号的用户名，由 ISP 提供
PPPoE 密码	PPPoE 拨号的密码，由 ISP 提供

配置项及其说明（内网口）：

配置参数	说明
IP 地址	设置 LAN 口的 IP 地址
子网掩码	设置 LAN 口的子网掩码
使用 DHCP 配置	启用指定 LAN 口的 DHCP 服务器功能
起始 IP 地址	设置 DHCP 服务器自动分配 IP 地址的起始地址，该地址必需与指定 LAN 口 IP 地址设置在同一网段。
结束 IP 地址	设置 DHCP 服务器自动分配 IP 地址的起始地址，该地址必需与指定 LAN 口 IP 地址设置在同一网段，并且结束 IP 地址必须大于起始 IP 地址。
DNS 服务器 1	设置 DNS 服务器地址，允许留空。
DNS 服务器 2	设置备用 DNS 服务器地址，允许留空。如果两个 DNS 选项均留空则您需要在用户电脑上手动配置 DNS 服务器方可保证其能够正常访问互联网。

提示

1. 在配置向导中你只能同时配置一个外网口和一个内网口的参数。
2. 如果 PPPoE 拨号不成功（通常现象为 WAN 口无法获得 IP 地址），则请确认所输入的 PPPoE 账号及密码是否正确（注意字母的大小写）。
3. LAN 口上开启 DHCP 服务器功能时，DHCP 客户端分配得到的网关地址即为该 LAN 口上配置的 IP 地址。

完成上述接口参数配置后，点击页面下方的【下一步】按钮进入下图所示的带宽管理配置页面。

带宽管理

在此配置页面中，您可以通过配置“每用户最大带宽”选项为网络中的每台主机指定最大使用带宽，您还可以分别指定整个网络中的 P2P 下载、P2P 流媒体、HTTP 流媒体应用的最大使用带宽。

提示

1. 如果您不想对用户或某些应用的带宽进行限制，您可以将用户或应用的上、下行带宽输入框留空（不输入任何数值）。
2. 为了限制用户或应用的带宽，您必须同时指定用户或应用的上、下行带宽值。
3. 上行或下行带宽值输入为 0 则表示限制该方向上的所有流量。
4. 如果您需要了解各应用类中的详细应用，请点击其后的“查看详细应用”链接。

完成带宽管理配置后，点击页面中的【下一步】按钮进入下图所示的应用控制配置页面。

应用控制

在本配置页面中你可以通过勾选相应的应用类以禁止网络中的所有用户使用该应用类中的应用。

提示

如果您需要了解各应用类中的详细应用，请点击其后的“查看详细应用”链接。

内容审计配置

配置向导的最后一步是配置内容审计功能，如果您需要记录和查看内部网络中用户的上网行为及互联访问日志（如发帖内容、网页浏览、邮件内容、聊天内容等），那么您需要开启设备的内容审计功能。

一旦您完成上述所有参数的配置，并点击页面中的【完成】按钮，设备将立即自动重启并使用您新配置的参数进行工作。至此，“虚拟拨号(PPPoE+NAT)”应用模式的设备端配置工作全部完成。您只需按实际网络环境要求将设备连接到网络中，并正确配置内网中各主机的网络参数即可正常上网。

透明桥接

要使用配置向导完成“透明桥接”的功能配置，请在配置界面左侧的主菜单栏中选择＜基础配置＞→＜配置向导＞，如下图所示：

配置向导

在上图的应用模式选择页面中选择“透明桥接”，并点击【下一步】按钮，进入该应用模式的桥接参数配置页面（如下图）。在该配置页面中我们必须为桥组配置 IP 地址及子网掩码，同时我们还可以为桥组指定默认网关、DNS 服务器，并可根据实际应用需求为桥组添加新的成员接口。

桥接参数配置

配置项及其说明：

配置参数	说明
桥组 IP	设置桥组的 IP 地址
子网掩码	设置桥组的子网掩码

缺省网关	设置网关地址，允许留空。
DNS 服务器	设置 DNS 服务器地址，允许留空。
备用 DNS 服务器	设置备用 DNS 服务器地址，允许留空。如果两个 DNS 选项均留空则您需要在用户电脑上手动配置 DNS 服务器方可保证其能够正常访问互联网。
桥组成员接口	配置桥组成员接口

提示

1. 在桥接模式下，桥组 IP 是您管理设备的重要 IP 地址，请务必正确配置。
2. 设备的桥组成员接口默认包含 WAN0 和 LAN0，且您无法将它们从桥组中移除。

完成上述桥组参数配置后，点击页面下方的【下一步】按钮进入下图所示的带宽管理配置页面。

带宽管理

在此配置页面中，您可以通过配置“每用户最大带宽”选项为网络中的每台主机指定最大使用带宽，您还可以分别指定整个网络中的 P2P 下载、P2P 流媒体、HTTP 流媒体应用的最大使用带宽。

1. 如果您不想对用户或某些应用的带宽进行限制，您可以将用户或应用的上、下行带宽输入框留空（不输入任何数值）。
2. 为了限制用户或应用的带宽，您必须同时指定用户或应用的上、下行带宽值。
3. 上行或下行带宽值输入为 0 则表示限制该方向上的所有流量。
4. 如果您需要了解各应用类中的详细应用，请点击其后的“查看详细应用”链接。

提示

完成带宽管理配置后，点击页面中的【下一步】按钮进入下图所示的应用控制配置页面。

应用控制

在本配置页面中你可以通过勾选相应的应用类以禁止网络中的所有用户使用该应用类中的

提示

如果您需要了解各应用类中的详细应用，请点击其后的“查看详细应用”链接。

应用。

内容审计配置

配置向导的最后一步是配置内容审计功能，如果您需要记录和查看内部网络中用户的上网行为及互联访问日志（如发帖内容、网页浏览、邮件内容、聊天内容等），那么您需要开启设备的内容审计功能。

一旦您完成上述所有参数的配置，并点击页面中的【完成】按钮，设备将立即自动重启并使用您新配置的参数进行工作。至此，“透明桥接”应用模式的设备端配置工作全部完成。您只需按实际网络环境要求将设备连接到网络中，并正确配置内网中各主机的网络参数即可正常上网。

旁路审计

要使用配置向导完成“旁路审计”的功能配置，请在配置界面左侧的主菜单栏中选择＜基础配置＞→＜配置向导＞，如下图所示：

配置向导

在上图的应用模式选择页面中选择“旁路审计”，并点击【下一步】按钮，进入该应用模式的参数配置页面（如下图）。在该配置页面中我们必须为设备配置正确的管理参数：IP 地址及子网掩码，还可指定设备的默认网关地址。另外，还必须为设备指定需要进行内容审计的内网主机 IP 地址段。

旁路审计参数配置

添加被审计内网网段对话框

配置项及其说明：

配置参数	说明
设备管理 IP	设置设备的管理 IP 地址
子网掩码	设置子网掩码
缺省网关	设置网关地址，允许留空。
内网审计网段配置	设置需要进行行为审计的内网用户 IP 网段
子网掩码	设置被审计网段的子网掩码

配置完成后的效果图

提示

1. 在旁路模式下必须通过 WAN0 口接收审计数据，并通过 LAN0 口管理设备。
2. 为了确保内容监控及数据分析结果的准确性，请您正确配置被审计用户的网段地址。

一旦您完成上述配置参数，并点击页面中的【完成】按钮，设备将立即自动重启并使用您新配置的参数进行工作。至此，“旁路审计”应用模式的配置工作全部完成。您只需按实际网络环境要求将设备连接到网络中即可正常工作。

第六章　配置指南

当您成功登录设备，浏览器将显示以下配置界面。设备配置主菜单位于配置界面左侧，右侧为各功能配置及信息显示区域，下面详细介绍各个功能菜单的作用。

设备配置界面

系统状态

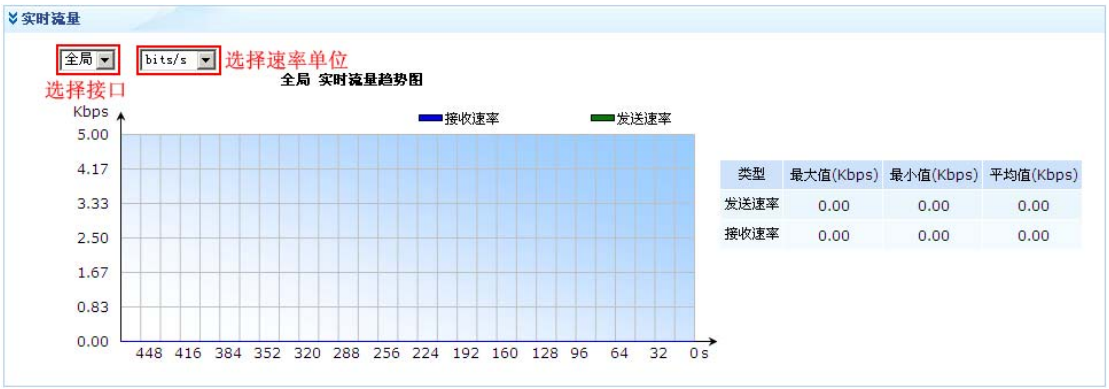
系统状态页面是登录进入系统后的默认页面，该页面以图表方式显示了设备及网络运行状况的综合信息，通过查看系统状态页面，管理员可以快速了解设备及网络的当前的基本运行状况。本页面的说明如下：

系统基本信息

参数及其说明：

参数	说明
设备型号	显示设备的具体型号
工作模式	显示设备当前的工作模式，设备支持路由、桥接、旁路三种工作模式。用户点击【更改模式】可切换设备工作模式。
软件版本	显示设备当前的软件版本号，点击【升级版本】可进行软件版本升级操作。
系统当前时间	显示设备当前系统时间，点击【设置时间】可重新设置系统时间。
系统运行时间	显示系统持续运行的时间。每次设备重启后该时间均重新累计。
序列号	序列号是唯一标识设备的串号。
CPU 负载	以百分比形式显示当前 CPU 的负载率。
内存使用率	以百分比形式显示当前内存的使用率。
硬盘使用率	以百分比形式显示当前硬盘使用率。
在线用户数	显示当前处于活动状态的上网用户数，点击【查看在线用户】可查看当前所有在线用户的详细信息。

- 实时流量：以图形和表格方式分别显示设备的上行流量和下行流量速率。图表的横坐标为时间，单位为秒，纵坐标为流量速率。流量速率单位默认为 bps(比特/秒)，也可以选择 Bps(字节/秒)。由于设备所处的网络环境差别较大为了使流量信息更加清晰可读，在流量较小的情况下，使用 bps，在流量较高的情况下，使用 Kbps，在流量很高的情况下，使用 Mbps，如下图：



实时流量

提示

若选择接口后无法显示实时流量信息，请检查以下两点：

1. 确认该接口是否有数据流量
2. 确认在＜流量分析＞→＜流量分析配置＞菜单中，“实时流量分析开关”是否已开启

■ 流量排名：显示前三名的用户流量、应用流量以及连接数排名，如需查看更详细的排名信息，可点击每个排名信息表格右上角的【查看】按钮进行查看。

流量排名

参数及其说明：

参数	说明
用户名	默认情况下设备采用用户主机 IP+MAC 地址后四位来标识用户，如果有自定义了用户名信息，将显示为自定义的用户名。
应用类型	显示进行流量排名的应用类别名称

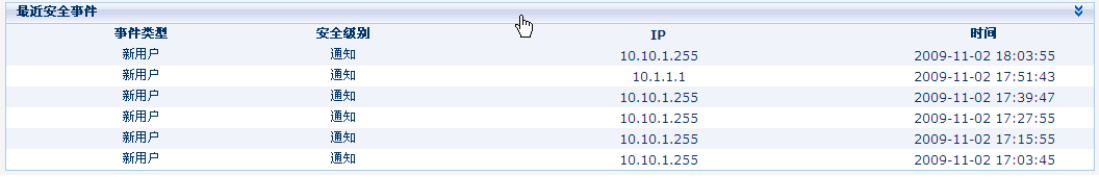
■ 接口信息：可以查看设备各接口的 IP 地址、MAC 地址、链路状态、接收和发送报文的信息。

接口信息

接口信息参数说明：

参数	说明
链路状态	接口的物理链路状态，物理接口链路使能后显示 UP，未使能显示 down
接收字节	接口上接收的数据流量统计，以字节为单位
发送字节	接口上发送的数据流量统计，以字节为单位
接收包	接口上发送的数据包数量统计
发送包	接口上发送的数据包数量统计

■ 最近安全事件：可以查看最近发生的安全事件。



安全事件

■ 系统软件要求：可以查看系统软件要求。

系统软件要求

基础配置

配置向导

具体参考第五章的“快速安装使用指南”相关部分内容。

工作模式配置

Smart 设备提供三种工作模式，各工作模式详细介绍见第四章“接入模式介绍”内容。通过在主菜单上选择＜基础配置＞→＜工作模式设置＞可进入工作模式配置页面，该页面为您提供切换设备工作模式或修改设备当前工作模式下相关参数的功能。以下内容详细介绍各工作模式的相关配置信息。

路由模式

通过在主菜单上选择＜基础配置＞→＜工作模式设置＞菜单并选择页面中的“路由模式”选项可进入路由模式配置页面。路由模式下设备支持动态 IP、静态 IP 以及 PPPoE 三种外网（WAN 口）接入方式。

路由模式－WAN 口接入方式

静态 IP

路由模式－WAN 口静态 IP 接入配置页面

配置项及其说明（WAN 口配置）：

配置参数	说明
IP 地址	设置 WAN 口的 IP 地址
子网掩码	设置 WAN 口的子网掩码
缺省网关	设置网关地址，如果不清楚，可向 ISP 咨询。
DNS 服务器	设置 DNS 服务器地址，通常由 ISP 提供，必须配置。
备用 DNS 服务器	设置备用 DNS 服务器地址，通常由 ISP 提供，允许留空。

配置项及其说明（LAN 口配置）：

配置参数	说明
IP 地址	设置 LAN 口的 IP 地址
子网掩码	设置 LAN 口的子网掩码

动态 IP

动态IP接入方式下设备WAN口将通过DHCP协议从ISP处动态获取IP地址、子网掩码及缺省网关和DNS等信息。并且设备所获取的WAN口相关网络参数将显示在页面中。

路由模式－WAN 口动态 IP 接入配置页面

配置项及其说明（LAN 口配置）：

配置参数	说明
IP 地址	设置 LAN 口的 IP 地址
子网掩码	设置 LAN 口的子网掩码

PPPoE 拨号

PPPoE拨号接入方式下设备WAN口将通过PPPoE拨号方式接入到ISP网络中。

路由模式－WAN 口 PPPoE 接入配置页面

配置项及其说明（WAN 口配置）：

配置参数	说明
PPPoE 账号	PPPoE 拨号的用户名，由 ISP 提供
PPPoE 密码	PPPoE 拨号的密码，由 ISP 提供

配置项及其说明（LAN 口配置）：

配置参数	说明
IP 地址	设置 LAN 口的 IP 地址
子网掩码	设置 LAN 口的子网掩码

桥接模式

通过在主菜单上选择＜基础配置＞→＜工作模式设置＞菜单并选择页面中的“桥接模式”选项可进入桥接模式配置页面。

桥接模式参数配置

配置项及其说明：

配置参数	说明
桥组 IP	设置桥组的 IP 地址
子网掩码	设置桥组的子网掩码
缺省网关	设置网关地址，允许留空。
DNS 服务器	设置 DNS 服务器地址，允许留空。
备用 DNS 服务器	设置备用 DNS 服务器地址，允许留空。如果两个 DNS 选项均留

	空则您需要在用户电脑上手动配置 DNS 服务器方可保证其能够正常访问互联网。
桥组成员接口	配置桥组成员接口

提示

1. 在桥接模式下，桥组 IP 是您管理设备的重要 IP 地址，请务必正确配置。
2. 设备的桥组成员接口必须包含 WAN0 和 LAN0，您无法将它们从桥组中移除。

旁路模式

通过在主菜单上选择＜基础配置＞→＜工作模式设置＞菜单并选择页面中的“旁路模式”选项可进入旁路模式配置页面。

旁路模式配置

添加被审计内网网段对话框

配置项及其说明：

配置参数	说明

设备管理 IP	设置设备的管理 IP 地址
子网掩码	设置子网掩码
缺省网关	设置网关地址，允许留空。
被审计内网网段 IP 地址	设置需要进行行为审计的内网用户 IP 网段
子网掩码	设置被审计网段的子网掩码

网络参数设置

内网口设置

在左侧的主菜单栏中选择＜基础配置＞→＜内网口设置＞，进入下图所示页面，您可以在该页面中配置 LAN 口的各项参数。

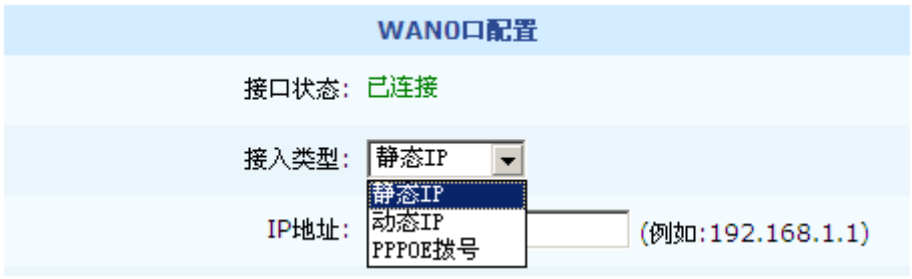
内网口设置

配置项及其说明：

配置参数	说明
IP 地址	设置 LAN 口的 IP 地址
子网掩码	设置 LAN 口的子网掩码
清空配置	用于清除已配置的参数数值

外网口设置

在左侧的主菜单栏中选择＜基础配置＞→＜外网口设置＞进入下图所示页面，您可以在此配置 WAN 口的各项参数。设备支持动态 IP、静态 IP 以及 PPPoE 三种外网（WAN 口）接入方式。



WAN 口接入方式

静态 IP

WAN口设置－静态IP

配置项及其说明：

配置参数	说明
IP 地址	设置 WAN 口的 IP 地址
子网掩码	设置 WAN 口的子网掩码
缺省网关	设置网关地址，如果不清楚，可向 ISP 咨询。
DNS 服务器	设置 DNS 服务器地址，通常由 ISP 提供，必须配置。
备用 DNS 服务器	设置备用 DNS 服务器地址，通常由 ISP 提供，允许留空。
清除配置	用于清除已配置的参数数值

动态IP

动态 IP 接入方式下设备 WAN 口将通过 DHCP 协议从 ISP 处动态获取 IP 地址、子网掩码及缺省网关和 DNS 等信息。并且设备所获取的 WAN 口相关网络参数将显示在页面中。

WAN口配置－动态IP

PPPoE拨号

PPPoE 拨号接入方式下设备 WAN 口将通过 PPPoE 拨号方式接入到 ISP 网络中。

WAN口配置－PPPoE拨号

配置项及其说明：

配置参数	说明
PPPoE 账号	PPPoE 拨号的用户名，由 ISP 提供
PPPoE 密码	PPPoE 拨号的密码，由 ISP 提供
连接/断开	单击按钮，可连接或断线 PPPoE 线路
清除帐号	清空已经配置的 PPPoE 账号和密码

用户组

设备提供创建和编辑用户组的能力，管理员可以根据企业的组织架构在设备中创建与之相适应的用户组（部门），并为用户组（部门）添加成员，由此实现基于用户组（部门）的网络管理和行为审计功能。

在左侧的主菜单栏中选择＜基础配置＞→＜用户组配置＞进入下图所示页面，该页面中的表格显示了设备中已创建的用户组信息。同时，您还可以通过选择配置界面中的相应按钮新建和编辑用户组。

用户组管理页面

新建用户组

当需要添加新的用户组时，您可以点击页面中的【添加】按钮，添加用户组的配置界面如下图所示：

添加用户组配置页面

配置项及其说明：

配置参数	说明
组名	配置用户组（部门）的名称，支持中英文输入

组描述	可选项，用于对用户组的描述
添加组成员	向该组添加成员，可选操作。稍后您还可以通过用户组列表中的【编辑】按钮添加组成员。

组成员管理

通过点击用户组列表“操作”栏中的【成员管理】按钮，您可以将用户组内的用户移动到其它用户组中，如下图

成员管理

用户配置

根据用户形成的方式设备把用户分为两种类型：固定用户和动态用户。固定用户是管理员手动添加的用户。动态用户是由设备通过自动检测用户 PC 所发送数据包的源 IP 地址而自动形成的用户，默认情况下所有动态用户都将被归到 default 组。对于固定用户无论是否上线，它的信息总是会出现在用户列表中，而动态用户一旦下线将会被清除出用户列表。对于网络管理而言固定用户比动态用户具有更加丰富的控制和管理特性。

在左侧的主菜单栏中，选择＜基础配置＞→＜用户配置＞可进入如下所示用户配置页面，该配置页面显示了设备中所有的固定用户及当前在线的动态用户列表。并且为管理员提供丰富的用户查询手段，以方便管理员快速查找特定的用户。同时，您还可以通过界面中提供的各种按钮对用户信息进行创建和编辑操作。

用户配置

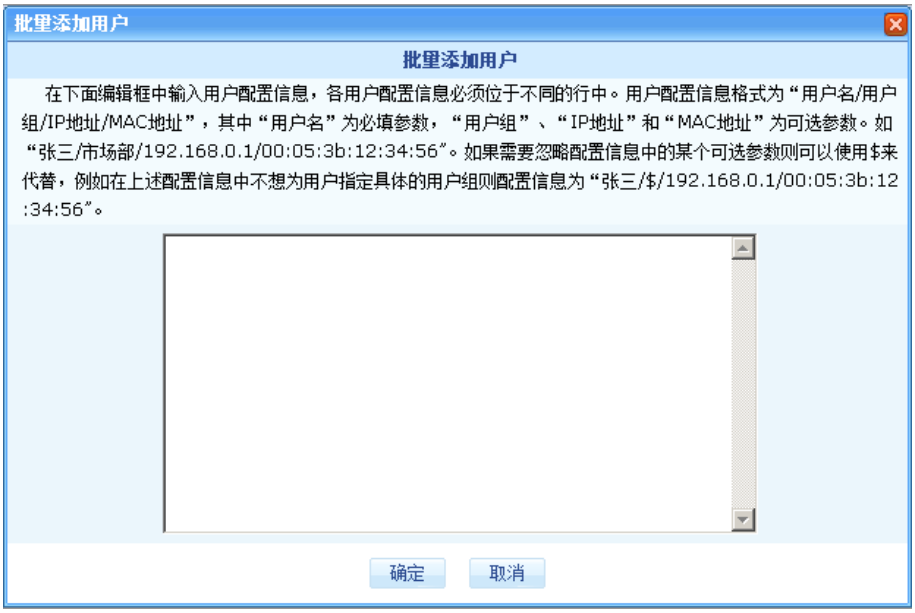
配置项及其说明：

配置参数	说明
逐个添加	逐个添加固定用户
批量添加	一次添加多个固定用户
设为固定用户	将选择的动态用户设置成固定用户
导出	将设备当前的用户列表导出，包括固定和动态用户
删除	删除选择的用户
编辑	编辑用户信息

逐个添加用户

逐个添加用户

点击【批量添加用户】，如下图，请按照约定的格式添加用户



批量添加用户

时间计划

通过定义时间计划模块并在设备的各种控制功能配置步骤中调用时间计划模块，可以实现按时间段对各种网络行为进行控制和管理的目的。如需配置时间计划请在配置界面左侧的主菜单栏中依次选择＜基础配置＞→＜时间计划＞进入时间计划配置界面。通过该页面您可以查看当前已经创建的时间计划模板，并可以继续创建新的时间计划模板或删除、编辑已有模板。

时间计划

默认情况下设备内置了四个时间模板：全部时间和三个上班时间模板，您可以根据实际需要选择内置的时间模板或添加新的时间模板。

在上图中点击【添加】按钮可进入时间计划配置界面，如下图：

时间计划配置

时间计划配置参数

配置参数	说明
名称	设置时间模板的名称
绝对时间	绝对时间指由明确起始和结束时间所组成的时间段范围
周期时间	周期时间指可周期性出现的时间，如每天、工作日、周末等

提示

一个时间计划可以同时包含绝对时间范围和周期时间范围

上网行为管理

Smart 设备具有专业的应用控制、内容审计及网址分类封堵等上网行为管理功能，设备能精确识别和控制各种常用的网络应用及协议，能够过滤各种网络信息内容，从而能够有效提高企业的工作效率，保护企业的安全和机密，营造绿色和谐的上网环境。

内容分析开关

内容分析开关是设备对各种网络应用及其内容进行深度分析和过滤的基础。因此，如需使用与内容分析和过滤相关的功能均需开启本开关。设备中与内容分析及过滤相关的功能包括：内容过滤、审计查询、应用统计、报表中心这五个功能模块。

如需开户内容分析开关请在配置界面左侧的主菜单栏中选择＜上网行为管理＞→＜内容分析开关＞进入下图所示配置页面：

内容分析开关配置

应用控制

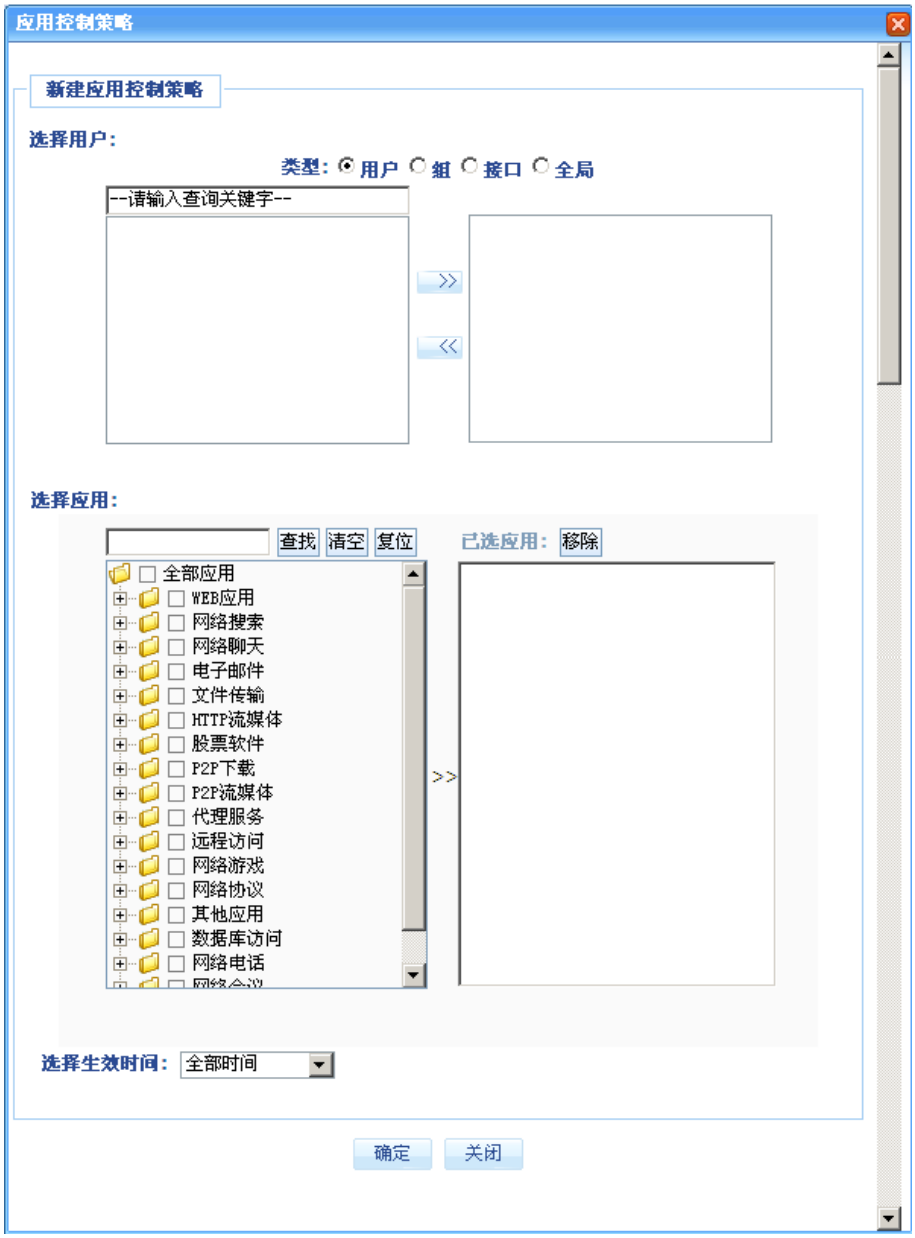
设备提供应用控制功能，帮助管理员根据网络管理的需求灵活控制各种网络应用的使用。例如管理员可以在上班时间禁止员工使用炒股、玩游戏、聊天、看电影等影响工作效率的网络应用，而在下班时间放开对这些网络应用的使用权限，由此实现对企业网络的科学化、人性

化管理。

为了方便控制和管理，设备内置了丰富的网络应用分类，且每一应用类别中又包含若干具体应用，管理员可以针对用户、用户组及时间段对网络应用（或应用类）实行精细化的管理。如需使用应用控制功能，请在配置界面左侧的主菜单栏中依次选择＜上网行为管理＞→＜应用控制＞进入下图所示页面。在该页面中您可以添加、修改和删除应用控制策略。

应用控制配置界面

通过点击以上页面中的【添加】按钮您可以进入以下新建应用控制策略对话框。在该对话框中您可以根据网络管理的需求配置应用控制策略的参数。



新建应用控制策略

四类可控制对象说明：

对象	说明
接口	包括物理接口（WAN 口、LAN 口）和逻辑接口（如子接口、PPPoE 拨号接口）。接口选择框中仅显示链路状态为“连接”状态的接口。
组	在＜用户组配置＞功能菜单中预先定义的用户组。
用户	在＜用户配置＞功能菜单预先定义的用户，您仅能对固定用户配置应用控制策略
全局	指所有流经设备的流量

内容过滤

内容过滤功能可以帮助您对网络中的敏感内容进行过滤，当前软件版本提供网站内容过滤，收发邮件过滤，文件传输过滤以及 MSN 聊天内容过滤功能。以下分别介绍各过滤功能的配置方法。

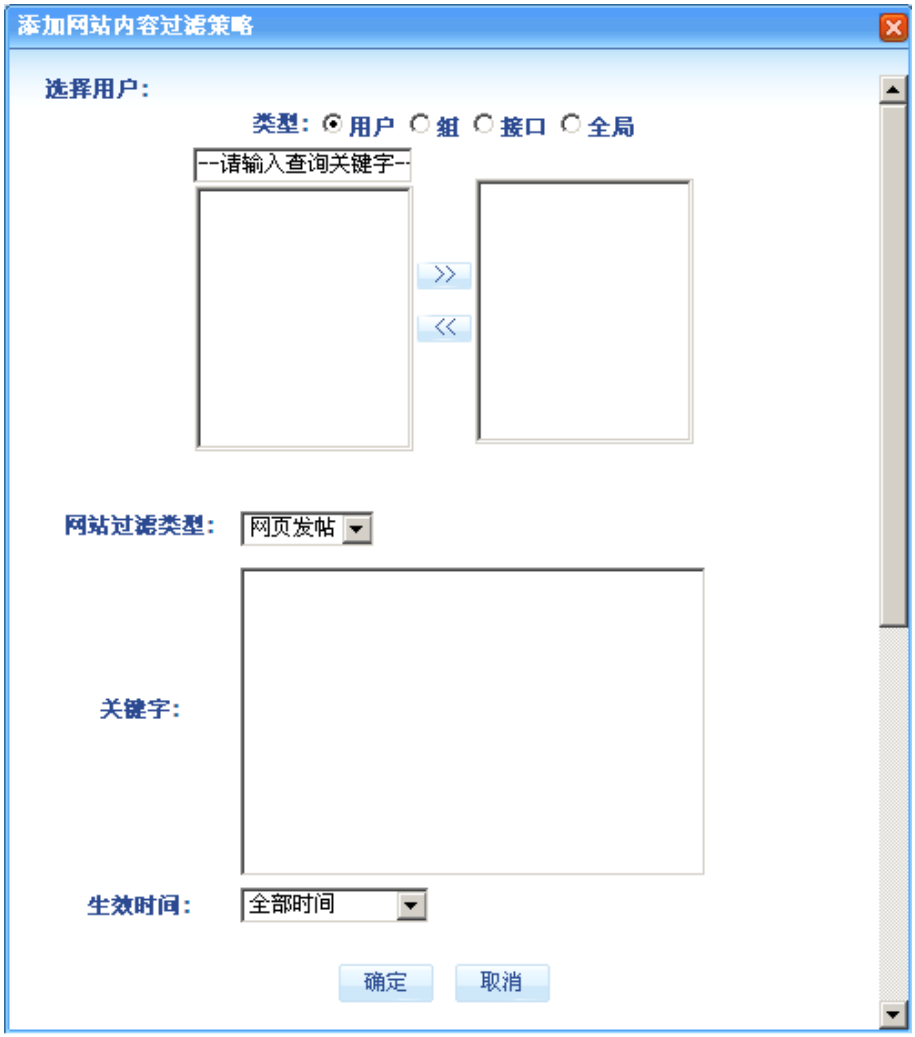
网站内容过滤

网站内容过滤功能可以帮助您阻止用户访问网页标题及网址中具有指定关键字的网站(或网页)，并可过滤具有指定关键字的网页发帖内容和网络搜索结果。

如需使用网站内容过滤功能，请在配置界面左侧的主菜单栏中依次选择在左侧的导航栏中选择＜上网行为管理＞→＜网站内容过滤＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的网站内容过滤策略，并可以继续创建新的策略或删除、编辑已有策略。

网站内容过滤

在以上网站内容过滤配置界面中点击【添加】按钮可进入以下添加网站内容过滤策略配置页面，在该配置页面中您可以根据管理需求选择不同的网站内容过滤类型并配置相关参数。



网站内容过滤配置

网站内容过滤策略可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内容。

网站过滤类型说明：

过滤类型	说明
网页主题	网页主题指浏览器窗口左上角的标题，例如新浪首页左上角的“新浪首页”标题，如图红框位置：  如需通过过滤网页主题名称来限制用户对新浪网的访问，则将网页主题过滤关键字指定“新浪”即可。
网页 URL	在 http://news.sohu.com/fangtan/、http://f1.sports.sohu.com/s2010/7896/s276248566/这两个网页中，红字以外的部分都属于网页 URL，如您想限制用户浏览所有在网页 RUL 中带有“fangtan”关键字的网页，则此处的过滤关键字设置为“fangtan”即可。
网页发帖	过滤包含指定过滤关键字的发帖信息内容。
网页搜索	当搜索引擎中输入的搜索关键字包含指定的过滤关键字时，则设备将阻止搜索引擎对该关键字进行搜索。

提示

设备支持在同一过滤类型中同时指定多个过滤关键字，当所访问内容中包含任意一个过滤关键字，该内容均被过滤。

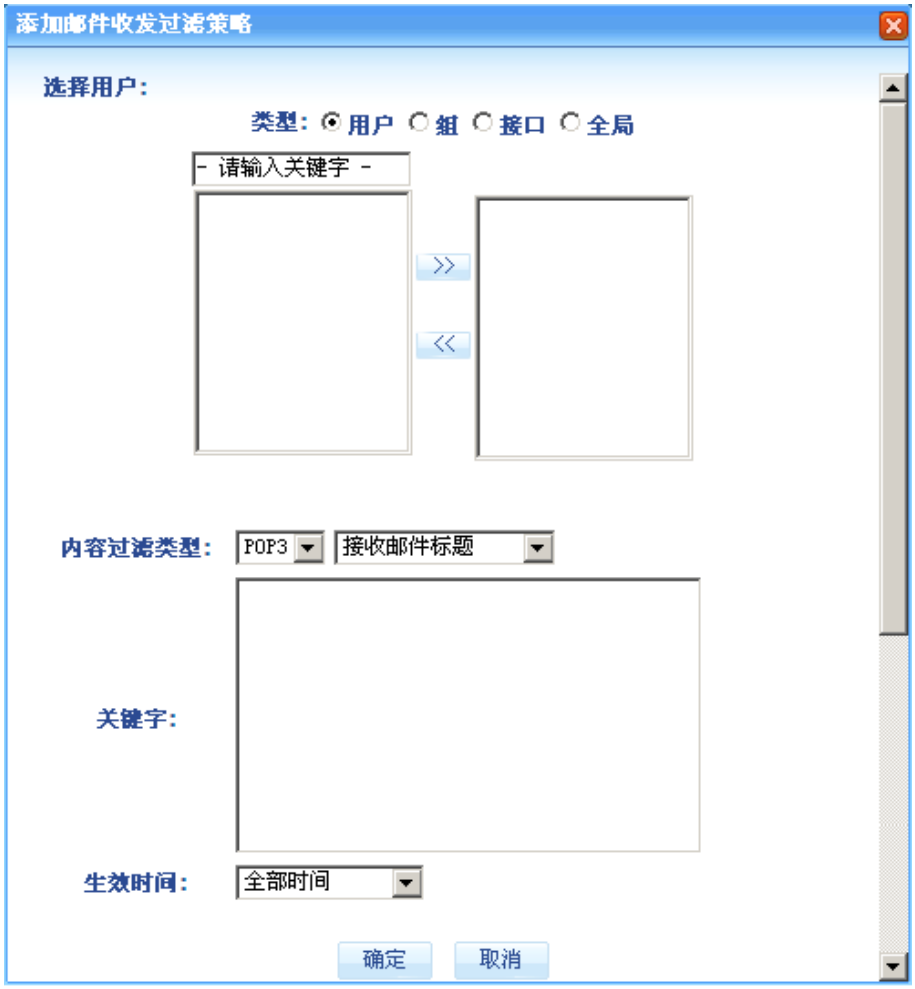
收发邮件过滤

设备支持按多种条件对收发邮件进行过滤的能力，所支持的过滤条件包括收发邮件的标题、附件名称和域名。

如需使用收发邮件过滤功能，请在配置界面左侧的主菜单栏中依次选择在左侧的导航栏中选择＜上网行为管理＞→＜收发邮件过滤＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的收发邮件过滤策略，并可以继续创建新的策略或删除、编辑已有策略。

收发邮件过滤

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加收发邮件过滤策略配置页面，在该配置页面中您可以根据管理需求选择不同的收发邮件过滤类型并配置相关参数。



收发邮件过滤

收发邮件过滤策略可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内容。

收发邮件过滤类型说明：

过滤类型	说明
收、发邮件标题	在收、发邮件过程中过滤邮件标题中包含指定关键字的邮件。
收、发邮件附件名	在收、发邮件过程中过滤邮件附件名中包含指定关键字的邮件。
收、发邮件域名白名单	收、发邮件域名白名单功能允许您使用包含指定域名关键字的邮箱收、发邮件，其它未指定邮箱不能收、发邮件。如：允许用户接收域名为 ABC.com 的邮箱所发的邮件或允许用户从域名为 ABC.com 的邮箱发送的邮件，则在收、发邮件域名白名单关键字中填写“ABC”即可。
收、发邮件域名黑名单	收、发邮件域名黑名单功能禁止您使用包含指定域名关键字的邮箱收、发邮件，其它未指定邮箱可以收、发邮件。如：禁止用户接收域名为 ABC.com 的邮箱所发的邮件或禁止用户从域名为 ABC.com 的邮箱发送邮件，则在收、发邮件域名黑名单关键字中填写“ABC”即可。

提示

设备支持在同一过滤类型中同时指定多个过滤关键字，当所传输内容中包含任意一个过滤关键字，该内容均被过滤。

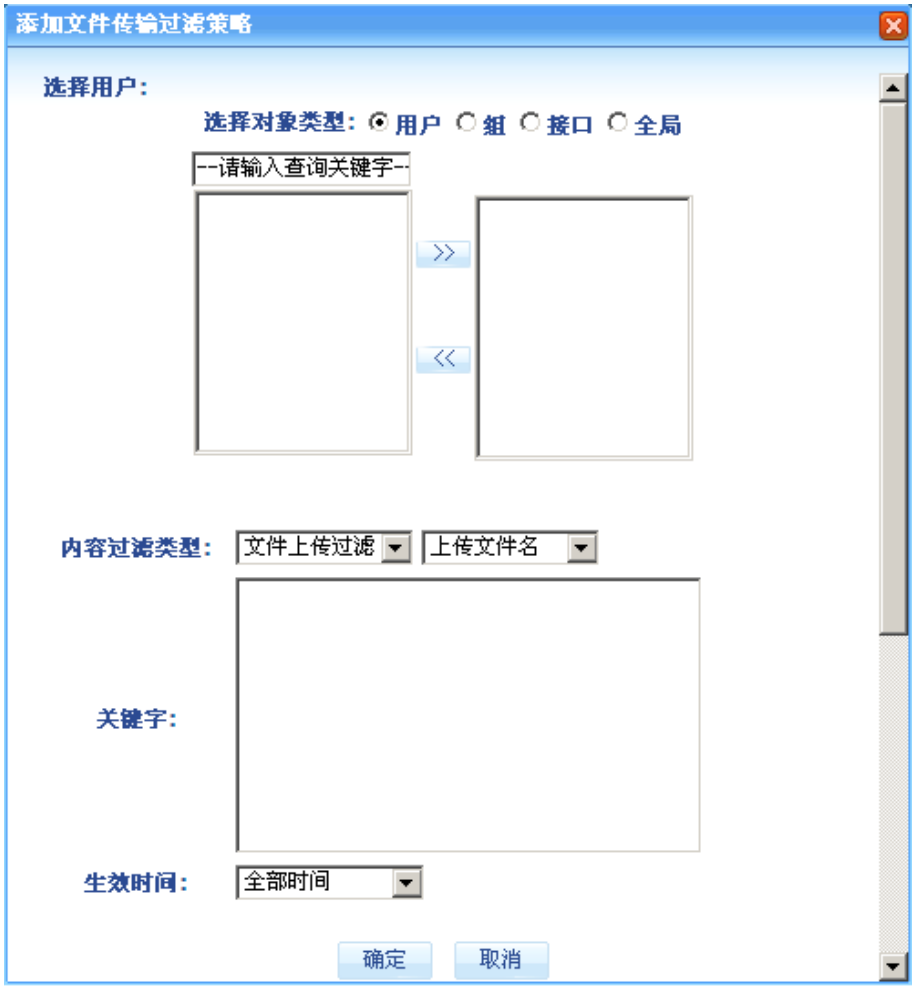
文件传输过滤

设备支持按多种条件对文件的发送和接收进行过滤的能力，所支持的过滤条件包括发送和接收文件的名称、类型和大小。

如需使用文件传输过滤功能，请在配置界面左侧的主菜单栏中依次选择在左侧的导航栏中选择＜上网行为管理＞→＜文件传输过滤＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的文件传输过滤策略，并可以继续创建新的策略或删除、编辑已有策略。

文件传输过滤

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加文件传输过滤策略配置页面，在该配置页面中您可以根据管理需求选择不同的文件传输过滤类型并配置相关参数。



文件传输过滤配置

文件过滤策略可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内容。

文件传输过滤类型说明：

过滤类型	说明
上传、下载文件名	在上传和下载文件时过滤文件中包含指定关键字的文件。
上传、下载文件类型	在上传和下载文件时过滤由关键字作为指定文件后缀名的文件。如您可输入 rar、doc、exe 等文件后缀名关键字从而过滤这些类型的文件。
上传、下载文件大小	在上传和下载文件时过滤文件尺寸大于由关键字所指定大小的文件。文件大小的单位：KB。如禁止用户上传或下载大小超过 1024KB 的文件，在关键字中填写为 1024 即可。

提示

设备支持在同一过滤类型中同时指定多个过滤关键字，当所传输内容中包含任意一个过滤关键字，该内容均被过滤。

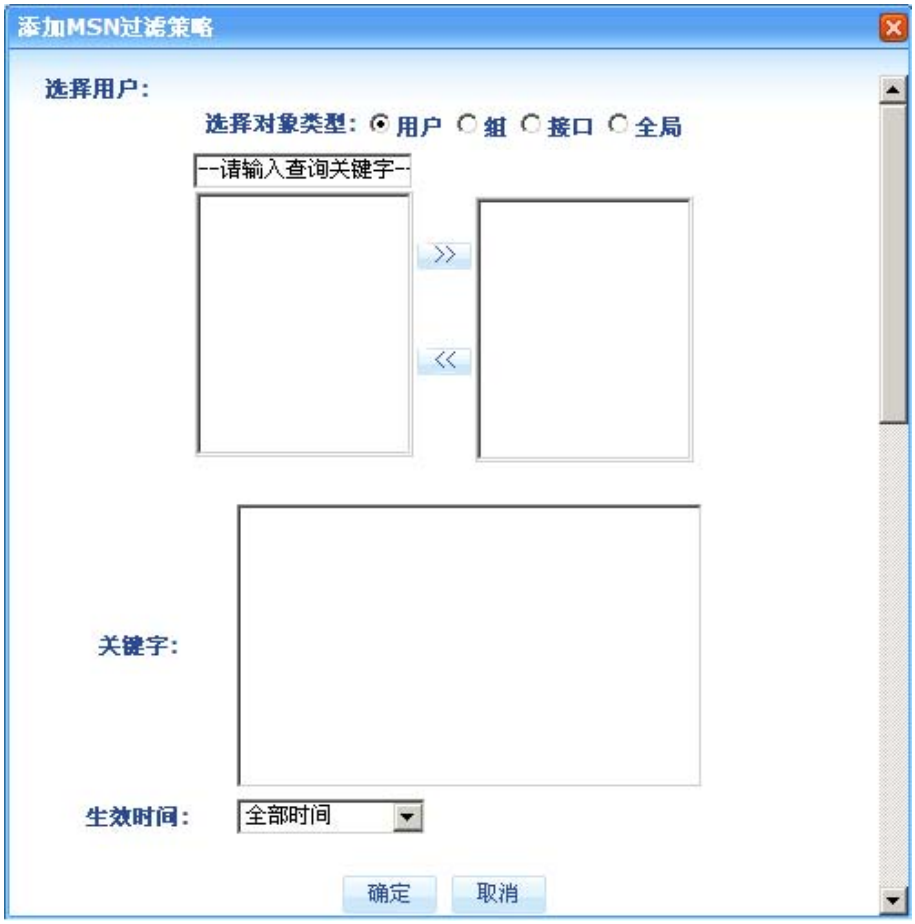
MSN聊天过滤

设备可以根据关键字过滤非加密的 MSN 聊天内容。

如需使用 MSN 聊天过滤功能，请在配置界面左侧的主菜单栏中依次选择在左侧的导航栏中选择＜上网行为管理＞→＜MSN 聊天过滤＞进入下图所示配置页面。通过该页面您可以查看当前已经创建的 MSN 聊天过滤策略，并可以继续创建新的策略或删除、编辑已有策略。

MSN 聊天过滤

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加 MSN 聊天过滤策略配置页面：



添加 MSN 聊天过滤策略

MSN 聊天内容过滤策略可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内

容。

设备支持在同一过滤类型中同时指定多个过滤关键字，当所传输内容中包含任意一个过滤关键字，该内容均被过滤。

网址封堵

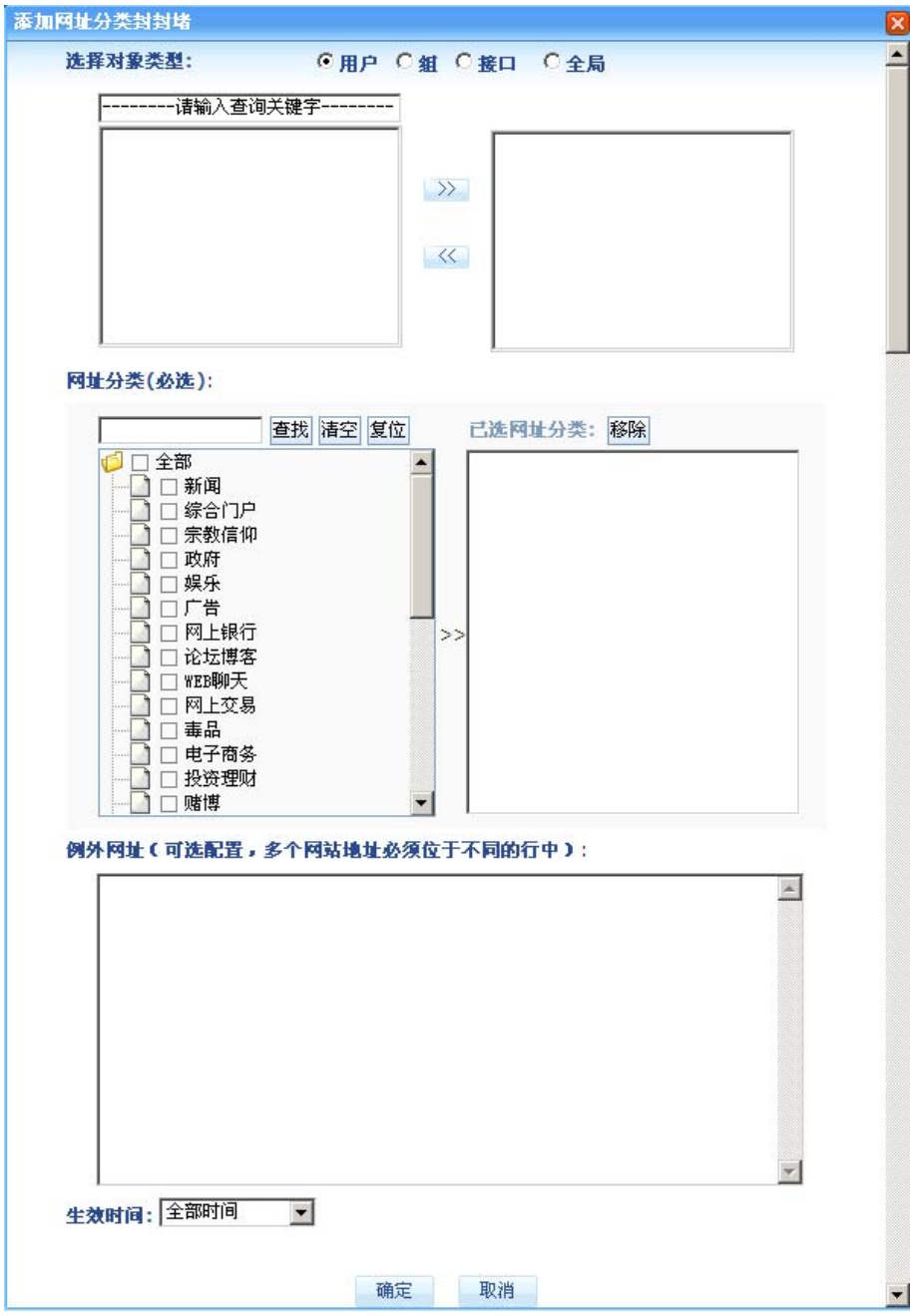
在日常的网络管理工作中，网管员通常需要根据企业管理的要求有针对性的对各类网站进行封堵。为了方便管理员的配置，设备内置全面并精确分类的网址分类库，同时还允许网络管理员根据自身网络管理的特殊需求自定义新的网址分类。另外，设备还提供基于用户、用户组以及时间等条件组合的网址分类封堵策略以及网址白名单、网址黑名单等丰富的网址访问控制功能。由此为网络管理员实施精确化、科学化、人性化网络管理提供了可能。

网址分类封堵

如需使用网址分类封堵功能，请在配置界面左侧的主菜单栏中依次选择在左侧的导航栏中选择＜上网行为管理＞→＜网址封堵＞→＜网址分类封堵＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的网址分类封堵规则，并可以继续创建新的规则或删除、编辑已有规则。

网址分类封堵

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加网址分类封堵配置界面：



网址分类封堵

网址分类封堵策略可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内容。

例外网址的使用说明：

当您封堵了某一网址类别，但同时又希望用户能访问该类别中的某些特殊网址时可使用“例外网址”功能。例如您希望公司员工除新浪新闻外其它新闻类网站均不能访问，则您只需在创建网址分类封堵策略时先在网址分类框中选择“新闻”类网址进行封堵，随后在例外网址编辑框中输入“news.sina.com”即可。

提示

网址分类封堵、网址白名单以及网址黑名单功能的优先处理顺序为：网址黑名单→网址白名单→网址分类封堵，当配置中发生冲突时，按此优先级进行处理。

网址白名单

在网络管理过程中，有时您希望网络用户仅能访问由您指定的少数网站（除此之外的其它网站均无法访问），这时你就可以使用网址白名单功能。

如需使用网址分类封堵功能，请在配置界面左侧的主菜单栏中依次选择在左侧的导航栏中选择＜上网行为管理＞→＜网址封堵＞→＜网址白名单＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的网址白名单列表，并可以继续创建新的网址白名单列表或删除已有列表信息。

网址白名单

在上图所示页面中点击【添加】按钮您可以进入如下所示的网址白名单配置界面：

网址白名单策略配置

网址白名单可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内容。

提示

网址分类封堵、网址白名单以及网址黑名单功能的优先处理顺序为：网址黑名单→网址白名单→网址分类封堵，当配置中发生冲突时，按此优先级进行处理。

网址黑名单

在网络管理过程中，如果您希望禁止网络用户访问某些由您指定的网站（除此之外的其它网站均可访问），这时你就可以使用网址黑名单功能。

如需使用网址分类封堵功能，请在配置界面左侧的主菜单栏中依次选择在左侧的导航栏中选择＜上网行为管理＞→＜网址封堵＞→＜网址黑名单＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的网址黑名单列表，并可以继续创建新的网址黑名单列表或删除已有列表信息。

网址黑名单

在上图所示页面中点击【添加】按钮您可以进入如下所示的网址白名单配置界面：

网址黑名单策略配置

网址黑名单可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内容。

提示

网址分类封堵、网址白名单以及网址黑名单功能的优先处理顺序为：网址白名单→网址黑名单→网址分类封堵，当配置中发生冲突时，按此优先级进行处理。

自定义网址分类

该功能帮助网络管理员根据网络管理的需求自行定义新的网址类别，并可为新的网址类别添加管理所需的网址，由此实现更灵活的网址分类管理策略。

如需使用网址分类封堵功能，请在配置界面左侧的主菜单栏中依次选择在左侧的导航栏中选择＜上网行为管理＞→＜网址封堵＞→＜网址黑名单＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的网址分类及其所对应的网站地址列表，并可以继续创建新的网址分类和网站地址列表或删除已有列表信息。

自定义网址分类

新增网址分类

在上图所示页面中点击【添加网址分类】按钮您可以进入如下所示的新增网址分类对话框：

新增网址分类对话框

配置项及其说明：

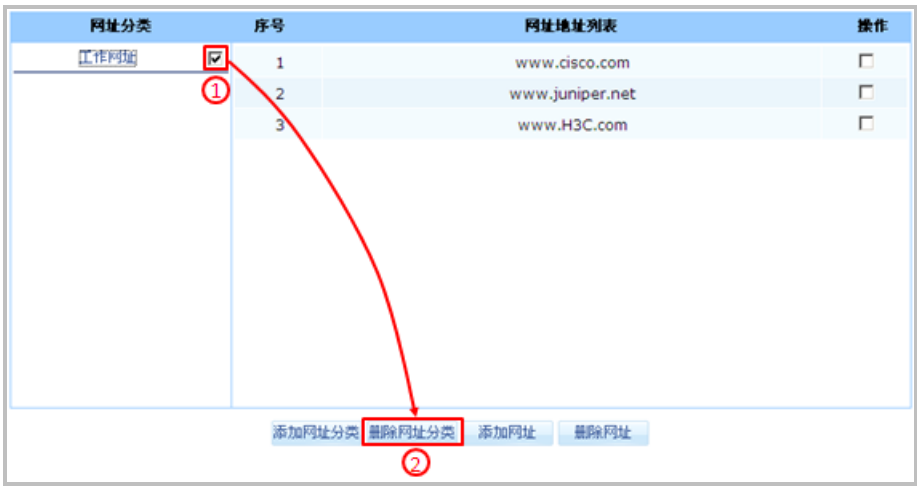
配置参数	说明
网址分类名称	为新网址分类指定名称，可以是汉字、字母、数字及其组合。
网站地址	为新的网址分类添加网址，可添加多个网址，但每个网址必须位于不同的行中

提示

1. 新添加的网址分类名称不能与设备内置的网址分类名称重名
2. 用户自定的网址分类必须重启设备后方可生效

删除网址分类

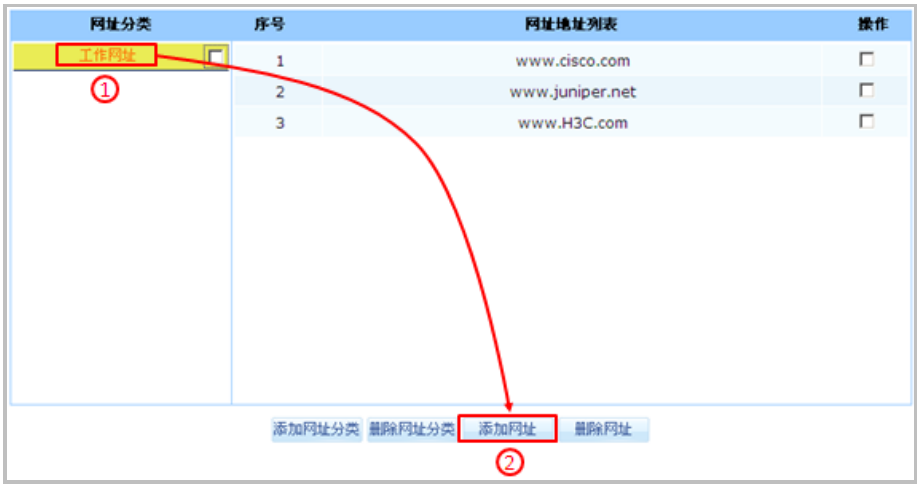
如要删除已创建的网址分类，请先勾选网址分类名称右侧的选择框（当需要删除多个网址分类时，您可以同时勾选多个），然后点击页面下方的【删除网址分类】按钮即可，如下图所示：



删除网址分类

为网址分类添加网址

您可以通过两种方法为网址分类添加网址，一种方法是在创建新网址分类时进行添加（见上述关于新增网址分类的说明）。另一种方法是在创建完网址分类后再添加网址，步骤如下图所示，先用鼠标点选需要添加新网址的网址分类名称，然后再点击页面下方的【添加网址】按钮，在随后出来的添加网址对话框中输入新网址即可。



添加网址

从网址分类中删除网址

如要从网址分类中删除网址，请先用鼠标点选需要从中删除网址的网址分类名称，然后在右侧出来的网址列表中勾选需要删除的网址（可多选），最后再点击页面下方的【删除网址】按钮即可。如下图所示：

删除网址

免审免控配置

对于网络管理而言，在某些特定的情况下需要对特定的用户、特定的网站或者特定的主机不进行任何的控制和审计，Smart 设备为您提供了相关的配置。

免审免控用户

当您希望对网络中某些特殊的用户（如企业领导、公司高层等）不进行审计和控制时，你可

以使用本功能。

如需配置免审免控用户功能，请在配置界面左侧的主菜单栏中依次选择＜上网行为管理＞→＜免审免控配置＞→＜免审免控用户＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的免审免控用户列表，并可以继续创建新的用户列表或删除已有列表信息。

免审免控用户配置

在上图所示页面中点击【添加】按钮您可以进入如下所示的免审免控用户配置对话框：

免审免控用户配置

提示

1. 您只能对固定用户进行免审免控处理
2. 上述免审免控用户配置对话框的用户选择框中仅显示设备中的固定用户

免审免控网站

当您希望对某些特殊的网站（如病毒升级网站、软件补丁升级网站等）不进行审计和控制时，你可以使用本功能。

如需配置免审免控网站功能，请在配置界面左侧的主菜单栏中依次选择＜上网行为管理＞→＜免审免控配置＞→＜免审免控网站＞，进入下图所示配置页面。通过该页面您可以查看当

前已经创建的免审免控网站列表，并可以继续创建新的网站列表或删除已有列表信息。

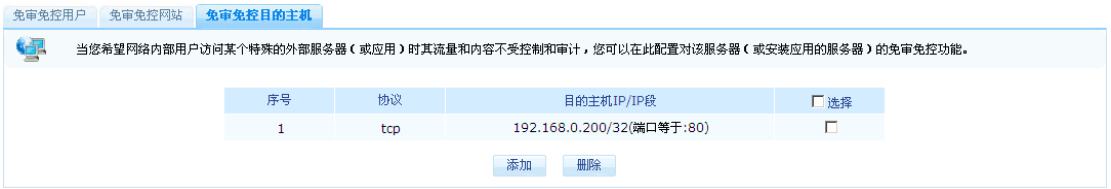
免审免控网站

设备中默认已经将部分补丁更新、杀毒软件更新等网址内置到免审免控列表中，另外，您还可以根据自身管理的需求添加新的或删除已有的免审免控网站。

免审免控目的主机

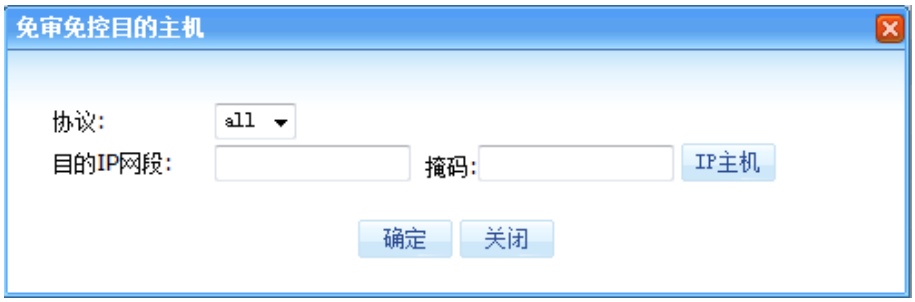
当您希望对去往某些特殊主机的流量（如网络中的某些服务器）不进行审计和控制时，你可以使用本功能。

如需配置免审免控目的主机功能，请在配置界面左侧的主菜单栏中依次选择＜上网行为管理＞→＜免审免控配置＞→＜免审免控目的主机＞，进入下图所示配置页面。通过该页面您可以查看当前已经创建的免审免控主机列表，并可以继续创建新的主机列表或删除已有列表信息。



免审免控目的主机

在上图所示页面中点击【添加】按钮您可以进入如下所示的免审免控目的主机配置对话框：



添加免审免控目的主机

配置项及其说明：

配置参数	说明
协议	包括 All、TCP 和 UDP 三个选项。其中 ALL 代表所有协议（或忽略协议类型），而如果选择 TCP 或 UDP 则还需要配置协议端口
目的 IP 网段	配置免审免控的目的主机 IP 或网段

流量控制

传统的 IP 网络无区别地对待所有的报文，它依照报文到达时间的先后顺序分配转发所需要的资源。所有报文共享网络和设备的资源，至于得到资源的多少完全取决于报文到达的时机，对报文转发的延迟、抖动、丢包率和可靠性等需求不提供任何承诺和保证。

随着计算机网络的高速发展，越来越多的网络接入互联网。越来越多的用户使用互联网作为数据传输的平台，开展各种应用，比如远程教学、远程医疗、可视电话、电视会议、视频点播等。企业用户也希望通过 VPN 技术，将分布在各地的分支机构连接起来，开展一些事务性应用：比如访问公司的数据库或通过 Telnet 管理远端设备。这些新业务有一个共同特点，即对带宽、延迟、抖动等传输性能有着特殊的需求。比如电视会议、视频点播需要高带宽、低延迟和低抖动的保证。事务处理、Telnet 等关键任务虽然不一定要求高带宽，但对网络时延却非常敏感，在拥塞发生时要求优先获得处理。新业务的不断涌现对 IP 网络的服务能力提出了更高的要求，用户已不再满足于能够简单地将报文送达目的地，而是还希望在转发过程中得到更好的服务，诸如支持为用户提供专用带宽、减少报文的丢失率、管理和避免网络拥塞、调控网络的流量、设置报文的优先级。所有这些，都要求网络应当具备更为完善的服务能力。Smart 设备可提供最大带宽、保证带宽、弹性带宽及面向应用和用户的 QOS 功能，满足现代化网络对服务质量方面的需求。

QOS基本配置

此处的配置内容是您后续进行其它高级 QOS 配置的基础，当您需要在网络中实施 QOS 部署时，请务必首先配置该部分内容。

如需进行 QOS 基本配置，则在配置界面左侧的主菜单栏中依次选择＜流量控制＞→＜QOS 流量控制＞→＜QOS 基本配置＞进入下图所示页面。通过该页面您可以查看当前 QOS 基本配置信息，并可以修改配置信息。

QOS 基本配置

配置项及其说明：

配置参数	说明
QOS 服务状态	显示及控制设备的 QOS 功能状态
启用接口 QOS 功能	打开或关闭相应接口上的QOS功能
线路实际带宽	线路实际带宽是指您从运营商处申请到的出口线路的实际带宽，单位：kbps

提示

1. 需要配置本页面 QOS 参数的功能包括：对象 QOS、应用 QOS、保证带宽及弹性带宽功能。
2. 线路实际带宽指该接口在实际网络应用中所能容纳的最大上、下带宽值。如：WAN0 口（100M 端口）接入上、下行均为 512kbps 的 ADSL 线路时，则该 WAN0 口的上、下行实际带宽即为 512kbps，并非接口的物理速率 100Mbps。

流量控制策略

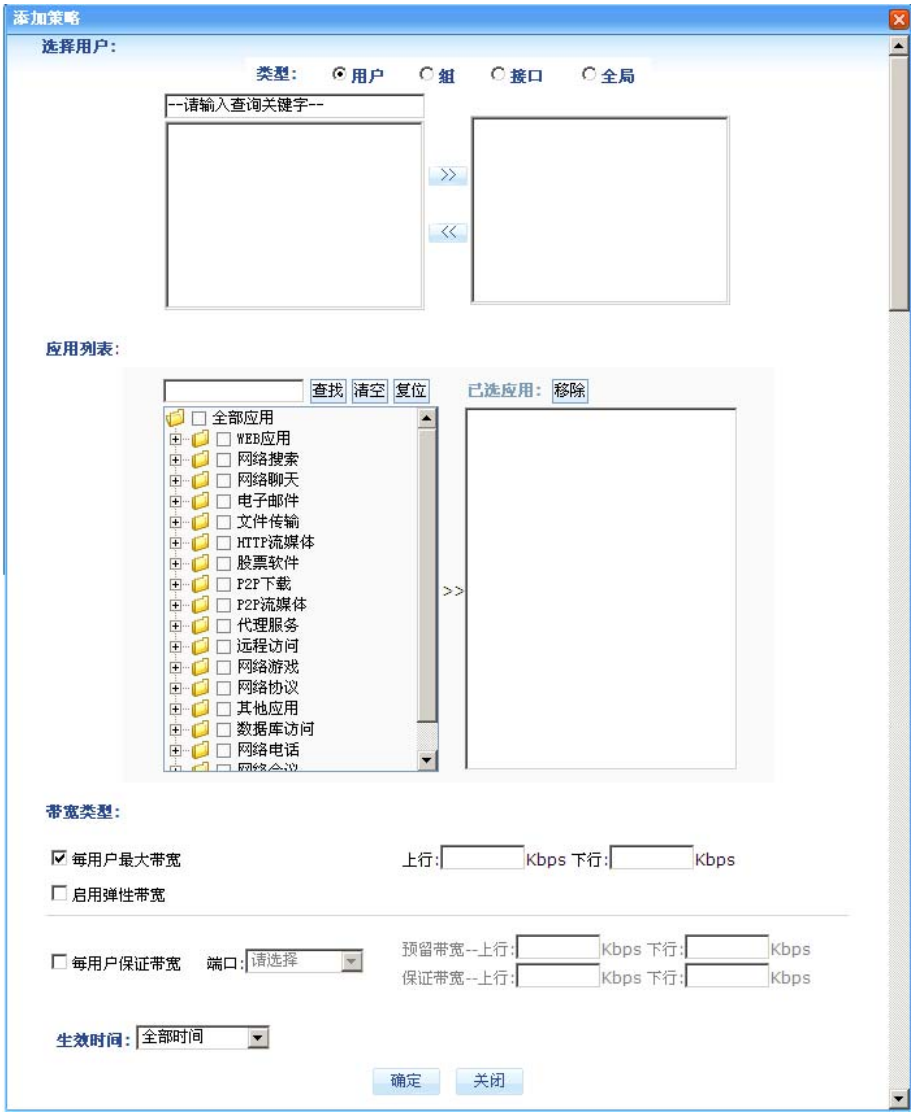
随着企业网络规模的不断发展以及网络应用的持续丰富，对网络流量的需求也在不断提高，科学合理的利用网络带宽资源成为网络管理的重要工作之一。对带宽资源的科学管理可以有

效提高企业网络的稳定性和可用性，同时可以充分利用企业有限的网络带宽资源。当前设备可为用户提供最大带宽、保证带宽、弹性带宽三种流量控制功能，帮助企业有效管理网络带宽资源的分配和利用。

如需配置流量控制策略，请在配置界面左侧的主菜单栏中依次选择＜流量控制＞→＜QOS 流量控制＞→＜流量控制策略＞进入下图所示页面。通过该页面您可以查看当前已经创建的流量控制策略，并可以继续创建新的策略或删除、编辑已有策略。

流量控制策略

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加流量控制策略对话框：



添加流量控制策略

流量控制策略可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内容。

三种带宽控制功能说明：

最大带宽

最大带宽是受控对象在通常情况下（指未使用弹性带宽功能情况下）允许使用的带宽上限。当受控对象为“组”时您可以为每个组以及所选各组中每个用户配置最大带宽限制。但各组内所有用户的实际使用带宽之和不能超过分配给该组的最大带宽。通过合理配置和使用最大带宽控制功能，即可以满足用户正常网络应用的需求，还可以有效避免由于少数受控对象（例如某些用户大量使用 P2P 下载）大量侵占网络资源而造成整个网络不可用的问题。

保证带宽

保证带宽功能是为了确保网络中关键业务和应用始终能够获得稳定可靠的带宽资源而提出的带宽管理技术。通过使用该技术，管理者可以根据网络管理的切实需求为关键业务和应用

预先分配合适的独占带宽资源，从而保证网络拥塞时这些关键业务和应用仍能保持良好的运行状态。值得注意的是：保证带宽策略所指定的保证带宽资源可以不预先被全部预留（当配置的预留带宽值小于保证带宽值时）。因此当网络中不存在受保证带宽策略所保护的网络流量时，则由该保证带宽策略所指定分配的保证带宽资源将可以被其它应用或用户分享。而一旦网络中出现需要保护的流量，则设备将重新分配当前正在使用的带宽资源，为受保护流量分配独占的保证带宽资源。

保证带宽功能中的预留带宽配置选项其主要目的是向受保护的关键业务和应用提供快速建立连接所需的带宽。一旦保证带宽策略配置成功，在策略生效期内其所对应的预留带宽将始终被设备保留，这部分带宽不会被其他任何流量所占用。对于除受保护的网络业务和应用之外的其它网络应用而言这相当于网络中能够使用的实际网络带宽变小了。因此，管理员需要仔细规划预留带宽的数值，以确保带宽资源的有效利用。

弹性带宽

前面在介绍最大带宽时，可以发现纯粹的最大带宽限制功能存在一定的弊端：即无论网络是否空闲，受控对象都将只能使用最大带宽限制值指定的带宽。设备提供弹性带宽功能解决上述弊端以充分利用网络带宽资源，当为受控对象配置了弹性带宽功能后，一旦网络资源出现空闲则该受控对象将被临时允许占用空闲的带宽资源，使其实际所用带宽突破最大带宽的限制值。而一旦网络恢复繁忙，受控对象就会释放占用的空闲带宽资源。

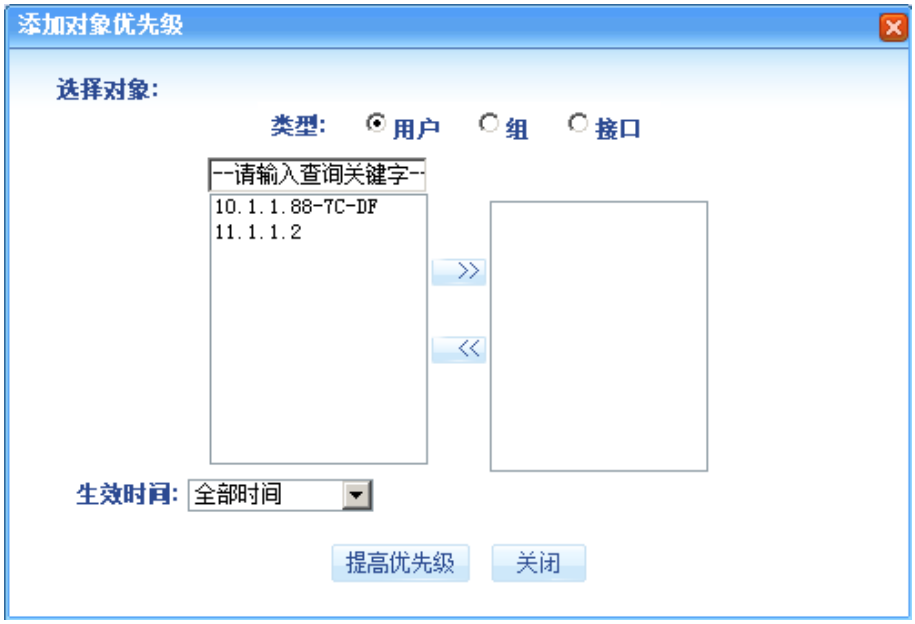
对象QOS配置

本配置功能允许您提升重要用户或用户组的网络数据处理优先级别，以保证在网络产生拥塞时重要用户或用户组的网络数据能优先处理。

如需配置对象 QOS 策略，请在配置界面左侧的主菜单栏中依次选择＜流量控制＞→＜QOS 流量控制＞→＜对象 QOS 配置＞进入下图所示页面。通过该页面您可以查看当前已经创建的对象 QOS 配置信息，并可以继续创建新的配置或删除已有配置。

对象QOS配置

在上图所示页面中点击【添加】按钮您可以进入如下所示的对象 QOS 配置对话框：



添加对象QOS

对象 QOS 优先级策略可绑定四类对象的详细说明请参考第六章中“应用控制”章节相关内容。

在上图所示对象QOS配置对话框中，您可以选择需要提升QOS优先级的用户、用户组以及接口，还可以选择需要提升优先级的时间，从而实现基本时间的QOS功能。

提示

1. 设备具有“普通”和“高优先级”两个优先级别，默认情况下所有对象的数据流量均位于普通优先级中。
2. 设备的对象 QOS 优先级列表中仅显示具有高优先级的对象。

应用QOS配置

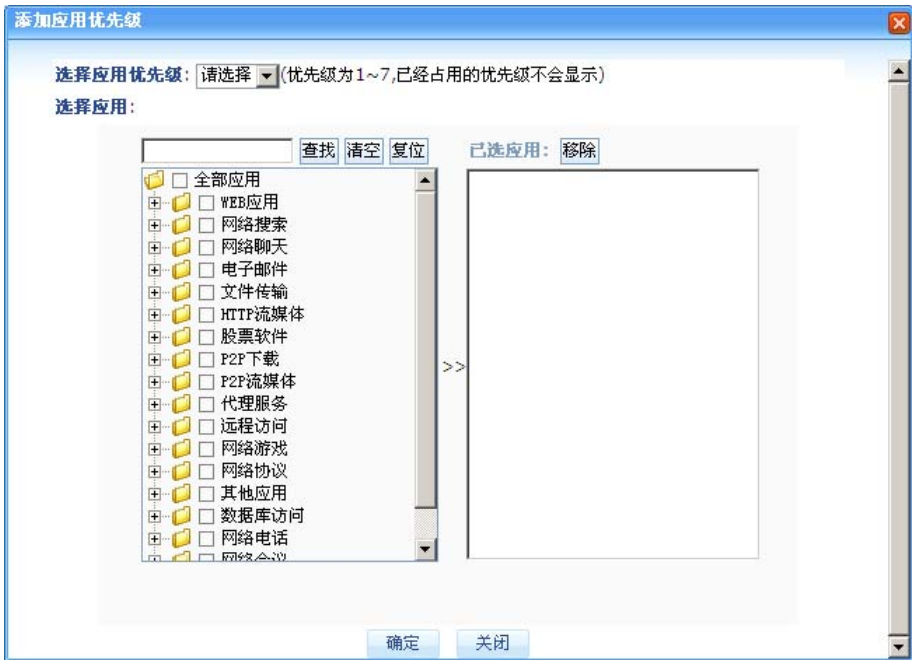
本配置功能允许您根据网络应用的重要程度为其指定不同的数据处理优先级，从而实现基于

应用的QOS功能，并保证在网络产生拥塞时重要应用的正常运行。

如需配置应用 QOS 策略，请在配置界面左侧的主菜单栏中依次选择＜流量控制＞→＜QOS 流量控制＞→＜应用 QOS 配置＞进入下图所示页面。通过该页面您可以查看当前已经创建的应用 QOS 配置信息，并可以继续创建新的配置或删除已有配置。

应用QOS配置

在上图所示页面中点击【添加】按钮您可以进入如下所示的应用 QOS 配置对话框：



添加应用QOS配置

提示

设备具有 7 个优先级别，其中数值越小优先级别越高，因此你需要为重要应用设置数值更小的优先级。

并发连接数限制

并发连接数指网络用户在某一时刻进行网络访问所产生的有效连接数总和，其中包括已建立的 TCP 和 UDP 连接以及 TCP 半连接。在实际网络应用中由于中病毒、进行恶意扫描或使用 P2P 软件均可能导致该用户的并发连接数过大，通过使用并发连接数限制功能网络管理员可以在一定程度上改善以上问题对网络的影响。

如需使用并发连接数限制功能，请在配置界面左侧的主菜单栏中依次选择＜流量控制＞→＜并发连接数限制＞进入下图所示页面。通过该页面您可以查看当前已经创建的并发连接数限制规则，并可以继续创建新的规则或删除已有规则。

并发连接数限制

在上图所示页面中点击【添加】按钮您可以进入如下所示的并发连接数限制配置对话框：

添加并发连接数限制

提示

通常网络中的服务器需要与其客户端建立大量的数据连接，因此当您使用并发连接数限制功能时，务必对服务器进行特殊处理。如：不对服务器进行并发连接数限制或根据经验和统计分析结果为每台服务器设定一个合理的并发连接数值。

网络安全

随着互联网的快速发展和广泛普及，它已经完全融入到人们日常的工作、学习和生活中，并发挥着极其重要的作用。当今的互联网就象一个巨大的信息宝藏，同时也是众多企业的赖以发展的信息平台。网络安全因此变得比以往任何时候都更重要，也更受到管理者的关注。Smart 设备为用户提供丰富的安全特性，帮助网络使用者有效解决网络安全问题，并加固网络安全防护。

防火墙规则

Smart 设备提供防火墙功能，使用户能够创建适合网络管理需求的安全访问规则，从而防止外部网络的危险蔓延到内部网络中，并可以有效控制内部网络对外部资源的访问授权，最终帮助用户构建坚固的网络安全防护体系。

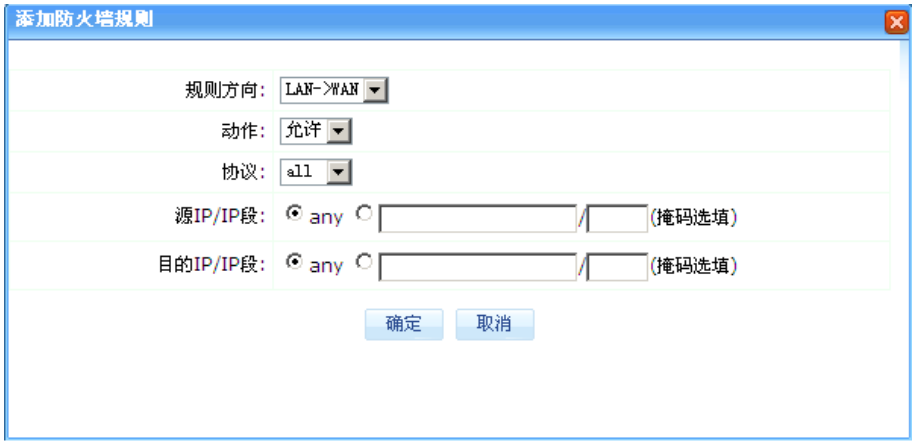
Smart 设备提供灵活的防火墙控制策略，可以控制内网到外网、外网到内网、内网到内网的数据流，并可基于网络协议及其端口号、IP 地址、IP 地址段以及时间计划进行控制。

如需使用防火墙功能，请在配置界面左侧的主菜单栏中依次选择＜网络安全＞→＜防火墙规则＞进入下图所示页面。通过该页面您可以查看当前已经创建的防火墙规则，并可以继续创建新的规则或删除、移动已有规则。

防火墙规则

新建防火墙规则

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加防火墙规则对话框：



添加防火墙规则

配置项及其说明：

配置参数	说明
规则方向	选择被防火墙规则控制的数据流方向，分别为：LAN→WAN 表示从 LAN 口到 WAN 口的数据流；WAN→LAN 表示从 WAN 口到 LAN 口的数据流；LAN→LAN 表示从 LAN 口到 LAN 口的数据流量。
动作	选择规则的动作：允许或拒绝。 如果选择动作为“允许”则匹配规则的流量将被放行通过； 如果选择动作为“拒绝”则匹配规则的流量将被阻断丢弃；
协议	选择规则匹配的协议类型并指定其协议端口号，可选协议包括：All、ICMP、TCP、UDP。其中 All 表示不关注协议类型（或匹配所有协议类型）。如果选择 TCP 或 UDP 您还可以指定源和目的协议端口号。
源 IP/IP 段	指定匹配规则的数据包源 IP 地址（或地址段），默认为“any”，表示匹配来自任意源 IP 地址的数据包。
目的 IP/IP 段	指定匹配规则的数据包目的 IP 地址（或地址段），默认为“any”，表示匹配去往任意目的 IP 地址的数据包。

改变防火墙规则的匹配顺序

每一个流量方向上的防火墙规则是按序号从小到大的顺序进行匹配的，您可通过移动规则的顺序来更改防火墙规则的执行顺序，如下图。

改变防火墙规则匹配顺序

提示

启用防火墙功能后，默认情况下设备将仅允许内部网络主机访问外部网络应用（LAN→WAN），而不允许从外部网络主机访问内部网络中的服务器或主机（WAN→LAN）。

ARP欺骗防范

ARP欺骗病毒是近年来网络中高发性的常见病毒，它通过伪造并发送错误的ARP报文来对网络中的设备和用户主机实施欺骗，使得网络中的设备或用户主机将数据发送到错误的地方，从而造成网络时断时续，并可能造成网络数据被窃听从而导致安全问题。Smart设备提供ARP欺骗防范和静态ARP绑定功能，有效避免和缓解ARP欺骗病毒对网络造成的危害。

ARP欺骗防范

Smart设备通过定期向网络中的主机发送带有正确网关IP地址信息的ARP报文来防范ARP欺骗病毒的危害。

如需使用 ARP 欺骗防范功能，请在配置界面左侧的主菜单栏中依次选择＜网络安全＞→＜ARP 欺骗防范＞进入下图所示页面。通过该页面您可以查看当前已经配置的 ARP 欺骗防范信息，并可以修改这些信息。

Arp欺骗防范

配置项及其说明：

配置参数	说明
启用 ARP 欺骗防范	开启指定内网口上的 ARP 防欺骗功能。一旦开启该功能则相应接口就会向内网周期性发送带有正确网关 IP 信息的 ARP 报文
ARP 发送间隔	配置发送ARP报文的时间间隔，单位：秒

静态ARP绑定

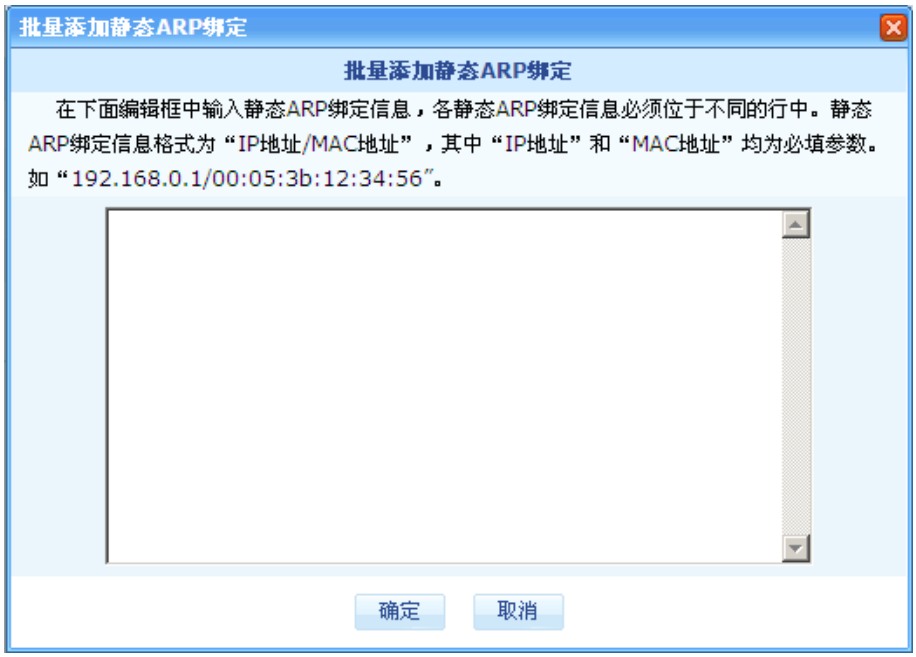
ARP欺骗病毒最大的特点就是通过发送错误的ARP报文来刷新网络设备和用户主机中的ARP表，从而达到破坏和欺骗的目的。因此，通过在设备和用户主机上绑定正确的静态ARP表项可以有效避免ARP欺骗病毒的危害，提高网络的稳定性。

如需使用设备上的静态 ARP 绑定功能，请在配置界面左侧的主菜单栏中依次选择＜网络安全＞→＜ARP 欺骗防范＞→＜静态 ARP 绑定＞进入下图所示页面。通过该页面您可以查看当前已经创建的 ARP 绑定条目，并可以继续创建新的条目或删除已有条目。

静态ARP绑定

用户可以通过逐个添加和批量添加两种方式来添加静态ARP绑定条目，如下图所示：

逐个添加静态ARP绑定



批量添加静态ARP绑定

IP/MAC绑定

IP/MAC 绑定通过对用户主机的 IP 地址和 MAC 地址进行唯一绑定，以防止其他未被授权（即未绑定）的用户主机接入到网络中，从而保障和加固网络的安全性。

IP/MAC绑定

如需使用设备上的 IP/MAC 绑定功能，请在配置界面左侧的主菜单栏中依次选择＜网络安全＞→＜IP/MAC 绑定＞进入下图所示页面。通过该页面您可以查看当前已经创建的 IP/MAC 绑定条目，并可以创建新的条目或删除已有条目。

IP/MAC 绑定

“禁止未被 IP/MAC 绑定的主机通过”选项说明：

当您勾选此选项后，所有未进行 IP/MAC 绑定的用户主机将无法通过设备访问外网。

未勾选此选项时，未进行 IP/MAC 绑定的用户主机可以通过设备访问外网，但进行 IP/MAC 绑定的用户主机其 IP 和 MAC 地址必须与绑定信息完全对应时才能通过设备访问外网。

添加 IP/MAC 绑定条目

提示

您只能对固定用户进行 IP/MAC 绑定操作，“添加 IP/MAC 绑定”配置对话框中的“未选用户”选择框中也仅显示设备中的固定用户。

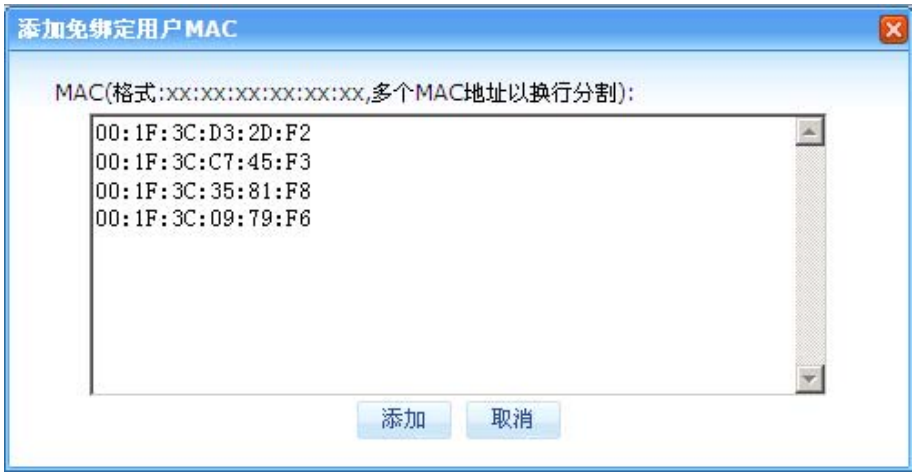
免绑定用户

在使用 IP/MAC 绑定的过程中，对某些特殊的用户（如企业领导、公司高层等）如果您不希望其受 IP/MAC 绑定的限制，则可以使用免绑定用户功能。使用该功能时，您需要输入具有免 IP/MAC 绑定需求的用户主机的网卡 MAC 地址，以后凡是从具有该 MAC 地址的网卡发出的网络数据设备将不再进行 IP/MAC 绑定的检查。

如需使用免绑定用户功能，请在配置界面左侧的主菜单栏中依次选择＜网络安全＞→＜IP/MAC 绑定＞→＜免绑定用户＞进入下图所示页面。通过该页面您可以查看当前已经创建的免绑定用户配置，并可以继续添加新的配置或删除已有配置。

免绑定用户

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加免绑定用户对话框：



添加免绑定用户

高级选项

Smart 设备除为用户提供常用的网络功能，还提供包括 NAT 地址转换、DHCP 服务器、策略路由、智能选路、链路负载均衡、高级 DNS 等多种高级网络功能，以满足用户在网络管理方面的多种需求。

NAT配置

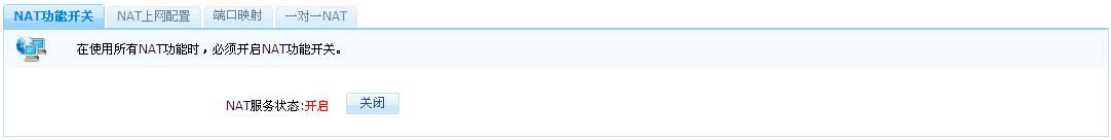
NAT（网络地址转换）是一个为减缓互联网中公网 IP 地址耗尽问题而提出的网络技术。当前 NAT 技术被广泛使用在局域网络中，它使得局域网中的用户主机能够实现共享上网，使得局域网中的内部服务器（如企业内部的 WEB 和 E-Mail 服务器）能够为外网用户提供服务。Smart 设备为用户提供 NAT 上网、端口映射、一对一 NAT 三种 NAT 功能。下面分别介绍这三种 NAT 功能的配置方法。

NAT功能开关

在您使用和配置任何 NAT 功能前，请您务必开启 NAT 功能开关，它是设备上任何 NAT 功能保持正常工作的基础。

如需打开设备上的 NAT 功能开关，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜NAT 配置＞→＜NAT 功能开关＞进入下图所示页面。在该页面中您可以开启或关闭 NAT 功

能服务。



NAT 功能开关

NAT上网配置

当您希望内网中的用户主机能够共享上网时，您可以使用 NAT 上网功能。NAT 上网功能使您能够让内网用户共享设备外网口的 IP 地址或者共享多个外网 IP 地址上网。

如需使用 NAT 上网功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜NAT 配置＞→＜NAT 上网配置＞进入下图所示页面。通过该页面您可以查看当前已经创建的 NAT 上网规则，并可以继续创建新的规则或删除已有规则。

NAT 上网配置

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加 NAT 上网配置对话框：

添加 NAT 上网配置

配置项及其说明：

配置参数	说明
内网接口	选择需要进行 NAT 转换的内网接口
外网接口	选择需要进行 NAT 转换的外网接口。如果外网口采用 PPPoE 接入方式，请选择 PPPoE0 或 PPPoE1，否则请选择 WAN0 或 WAN1。
需转换的内网地址	指定内网中能够通过 NAT 转换共享上网的 IP 地址（或地址段）。可选项为“任意 IP”和“指定网段”。默认值为“任意 IP”，其意味

	着网络中的所有主机均可通过 NAT 转换共享上网。如果选择“指定网段”，则您需要输入内网中能够进行 NAT 转换的 IP 地址段。
使用外部地址段	可选配置。如果希望将内网所有上网主机的 IP 使用多个外网 IP 转换出去，则可以使用该选项。

未选择“使用外部地址段”选项时，内网所有上网主机的 IP 将全部被转换为指定外网接口的 IP 地址

端口映射

端口映射是企业内部服务器向外网用户提供访问服务时常用的功能，它可以将内网服务器的端口映射到公网中，从而使得外网用户可以访问内网服务器。

如需使用端口映射功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜NAT 配置＞→＜端口映射＞进入下图所示页面。通过该页面您可以查看当前已经创建的端口映射规则，并可以继续创建新的规则或删除已有规则。

端口映射

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加端口映射配置对话框：

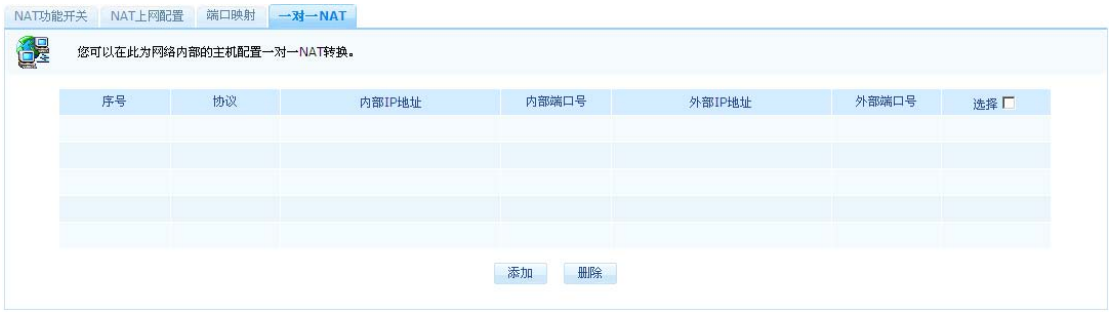
添加端口映射

配置项及其说明：

配置参数	说明
外网接口	选择对外提供端口映射服务的外网接口
外部 IP 地址	可选配置。设置外网用户访问内部服务器时所使用的公网 IP 地址。如不填写该选项，则使用上述选择的外网接口的 IP 地址作为内网服务器对外提供服务时的公网 IP 地址。
内部地址	内网服务器的真实 IP 地址
协议	选择服务器中需要映射的协议类型，可选择 TCP 或 UDP 两种协议类型。
外部端口号	外网用户访问服务器时所使用的外网端口号，即被映射的公网端口号。
内部端口号	内网服务器提供服务时所使用的真实端口号

一对一NAT

当您希望将内部网络中某一主机的 IP 地址（及协议端口号）映射成固定的外网 IP 地址（及协议端口号）时，可以使用一对一 NAT 功能。当内部主机 IP 地址（及协议端口号）通过一对一 NAT 映射到一个公网 IP 地址（及协议端口号）后，外网用户将可以使用这个公网 IP 地址（及协议端口号）对该内部主机进行访问。另外，如果您仅配置了 IP 地址间（未指定协议类型）的一对一映射那么该内部主机所有的上网流量也被固定映射到这个公网 IP 上。如需使用一对一 NAT 功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜NAT 配置＞→＜一对一 NAT＞进入下图所示页面。通过该页面您可以查看当前已经创建的一对一 NAT 规则，并可以继续创建新的规则或删除已有规则。



一对一 NAT

在上图所示页面中点击【添加】按钮您可以进入如下所示的一对一 NAT 配置对话框：

添加一对一 NAT

配置项及其说明：

配置参数	说明
协议	选择需要进行转换的协议类型并指定其协议端口号，可选协议包括：全部、TCP、UDP。其中全部表示转换所有协议类型的数据。如果选择 TCP 或 UDP 您还需要指定内部和外部协议端口号。
内部 IP 地址	需要进行转换的内部主机真实 IP 地址
外部 IP 地址	被转换后的外部公网 IP 地址（可以使用外网口 IP 地址）

DHCP配置

DHCP 全称为动态主机配置协议，该协议可以为网络中的用户主机动态分配 IP 地址以及各种网络参数（如 DNS 服务器、WINS 服务器、网关地址等），从而方便管理员对网络主机 IP 地址的管理，并可有效避免手动配置 IP 地址环境下经常出现的地址冲突问题。在使用 DHCP 动态分配地址的网络中，用户上网位置无论移动到那里，都只需将电脑连接接到网络中即可使用，由此大大简单化了网络管理和主机配置的难度。

设备仅支持在路由模式下使用 DHCP 服务器功能

LAN口DHCP配置

Smart 设备可以分别通过两个 LAN 口向内网用户动态分配 IP 地址，您可以为接在不同 LAN 口上的用户分配不同网段的 IP 地址。

如需配置设备 LAN 口上的 DHCP 功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项

＞→＜DHCP 配置＞→＜LAN0/1 口 DHCP 配置＞进入下图所示页面。通过该页面您可以查看当前的 DHCP 配置信息，并可以修改这些配置信息。

LAN 口 DHCP 配置

DHCP 配置参数

配置参数	说明
DHCP Server 服务状态	显示及控制接口上的 DHCP Server 服务状态
租约时间	设置动态分配地址的租约时间
DHCP 地址池	设置为 DHCP 客户端分配的 IP 地址范围
DNS 服务器	设置为 DHCP 客户端分配的 DNS 服务器 IP 地址，最多可配置两个 DNS 服务器
静态地址分配	可选配置。 当您需要通过 DHCP 为网络中某些特殊主机（如服务器）分配固定 IP 地址时，可在静态地址分配选项中进行指定。

提示

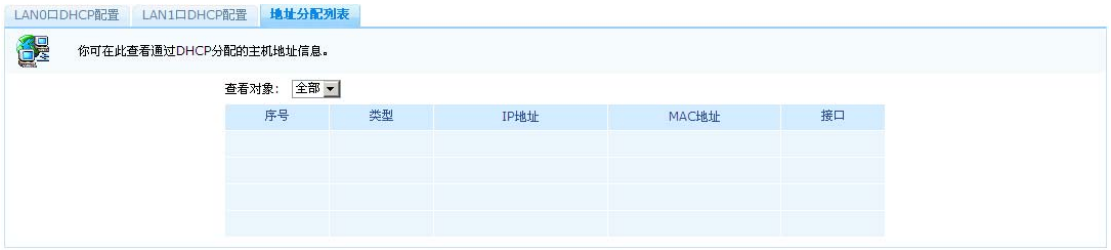
LAN 口上开启 DHCP 服务器功能后，DHCP 客户端分配得到的网关地址即为该 LAN 口上配置的 IP 地址。

地址分配列表

地址分配列表显示了设备当前的 DHCP 地址分配情况。您可以分别查看设备中通过 DHCP 分配的所有 IP 地址以及从不同接口上分配的 IP 地址。

如需查看设备上通过 DHCP 分配的 IP 地址，请在配置界面左侧的主菜单栏中依次选择＜高级

选项＞→＜DHCP 配置＞→＜地址分配列表＞进入下图所示页面。



地址分配列表

路由管理

相对同类产品，Smart 设备支持更丰富的路由特性和更强大的路由功能，其中包括静态路由、策略路由、智能选路，充分满足小型企业在网络管理方面对路由功能的需求。

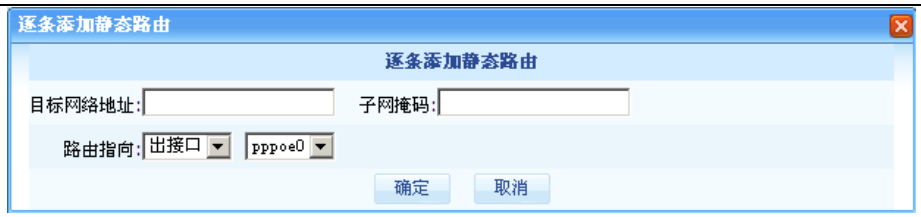
静态路由

静态路由是由管理员手工配置的路由条目。在结构比较简单的小型网络中，只需使用静态路由即可使网络良好运行。但在大型复杂网络中完全使用静态路由时会存在不足之处：当网络发生故障或者拓扑发生变化时可能会出现路由不可达，并导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

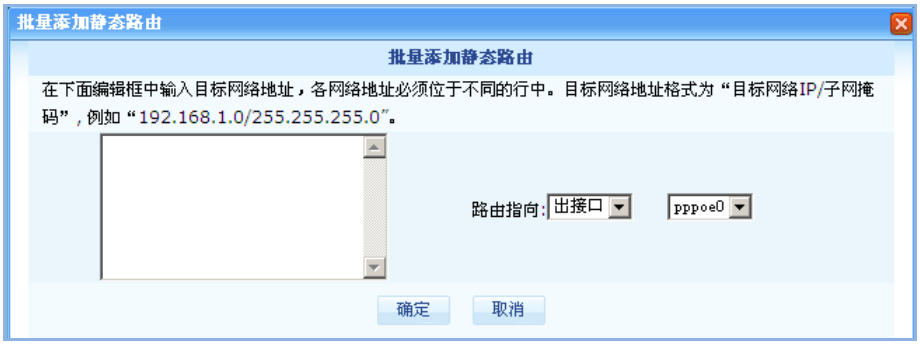
如需配置静态路由，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜路由配置＞→＜静态路由＞进入下图所示页面。通过该页面您可以查看当前的静态路由配置，并可以新建和删除静态路由。

静态路由

在上图所示配置界面中，通过选择不同的按钮管理员可以逐条添加和批量添加静态路由条目，如下图所示：



逐条添加静态路由条目



批量添加静态路由条目

配置项及其说明（逐条添加静态路由）：

配置参数	说明
目标网络地址	设置静态路由的目的网络地址
子网掩码	设置目的网络地址的子网掩码
路由指向	选择静态路由的下一跳指向方式，并配置相关参数。指向方式包括“出接口”和“网关 IP”两种。 当您需要配置一条与 PPPoE 拨号相关的静态路由时，请在路由指向选择框中选择“出接口”，并指定相应的 PPPoE 接口。其它情况下请选择“网关 IP”并正确配置下一路网关 IP 地址。

策略路由

正常路由情况下设备将依据数据包的目的 IP 地址查找路由表实现数据的路由转发。但在一些特殊情况下，用户希望能够将来自网络中某些主机、某些网段或某个网络接口的数据人为指定从特定的接口转发出去，这样的需求可以使用策略路由功能来实现。

如需配置策略路由，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜路由配置＞→＜策略路由＞进入下图所示页面。通过该页面您可以查看当前的策略路由配置，并可以新建和删除策略路由规则。

策略路由

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加策略路由配置对话框：

配置项及其说明：

配置参数	说明
入接口	设置需要使用策略路由功能的内网端口
源 IP 网段 源 IP 主机	设置需要进行策略路由转发的内网主机 IP 地址或内网网段地址。
路由指向	选择路由的下一跳指向方式，并配置相关参数。指向方式包括“出接口”和“网关 IP”两种。 当您需要配置一条与 PPPoE 拨号相关的策略路由时，请在路由指向选择框中选择“出接口”，并指定相应的 PPPoE 接口。其它情况下请选择“网关 IP”并正确配置下一路网关 IP 地址。

提示

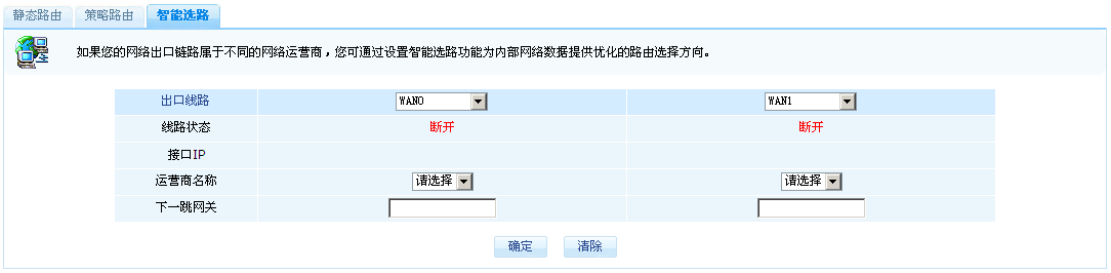
1. 策略路由的优先级高于普通路由。
2. 设备仅支持在路由模式下使用策略路由功能

智能选路

当前为了增加网络出口带宽很多企业申请了多条出口线路，并且这些出口线路大多由不同的运营商提供。在这样的网络环境中，由于通常的网络设备无法智能识别用户访问互联网的数据流量是去往那个运营商，可能导致访问电信的流量被发送到联通的出口线路中，从而造成

网络出现网速慢，甚至无法打开网页的问题。针对这样的问题 Smart 设备为用户提供智能路由选路功能，使去往不同运营商的流量被发送到与其对应的出口线路中，从而提高网络速度，增加网络的稳定性。

如需配置智能选路功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜路由管理＞→＜智能选路＞进入下图所示页面。通过该页面您可以查看当前的智能选路配置信息，并可以修改这些配置。



智能选路

配置项及其说明：

配置参数	说明
出口线路	选择外网出口线路 在 PPPoE 拨号接入环境下请选择 PPPoE0 或 PPPoE1，其它情况下请选择 WAN0 或 WAN1。
运营商名称	指定外网线路的提供商 当前支持电信、联通、教育网、移动四个运营商
下一跳网关	指定下一跳网关的 IP 地址 如果出口线路为PPPoE拨号类型，则设备会自动完成本部分配置


提示

设备仅支持在路由模式下使用智能选路功能

链路负载均衡

当您的网络中有多条出口线路，而您希望网络中访问互联网的流量能够按一定的比例从各条线路中发送出去，以充分利用线路带宽资源，加强网络的可靠性，则您可以使用设备中的链路负载均衡功能。

如需配置链路负载均衡功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜路由管理＞→＜链路负载均衡＞进入下图所示页面。通过该页面您可以查看当前的链路负载均

衡配置信息，并可以修改这些配置。

链路负载均衡

配置项及其说明：

配置参数	说明
出口线路	选择参与负载均衡工作的出口线路 在如果出口线路是 PPPoE 拨号接入请选择 PPPoE0 或 PPPoE1，其它情况下请选择 WAN0 或 WAN1。
带宽分配比例	设置各线路间进行负载均衡的流量比例 可选择 1 到 9 之间的任意一个数字，设备按设定比例分配流量，即权重大小与流量分配多少成正比，数字相同时平均分配流量。

提示

1. 设备仅支持在路由模式下使用链路负载均衡功能
2. 当所有出口线路由同一运营商提供时，链路负载均衡将工作得非常出色，当出口线路由不同的运营商提供时，为了达到更好的使用效果，建议将链路负载均衡与智能选路功能结合使用。

DNS高级配置

DNS 是互联网中广泛应用的协议，该协议主要用于将网络中的域名地址解释为网络通信所使用的 IP 地址，从而减少人们对 IP 地址记忆的难度并方便用户对互联资源的访问。为了方便网络管理并满足用户对 DNS 的特殊需求，Smart 设备还提供 DNS 中继及 DNS 重定向两个 DNS 高级功能。

DNS中继

当您希望将 Smart 设备指定为内部网络主机的 DNS 解析服务器时（在内网主机的 TCP/IP 配置中将设备内网接口 IP 指定其 DNS 服务器 IP），可以使用设备上的 DNS 中继功能。在开启 DNS 中继功能情况下，Smart 设备将处理来自内网主机的 DNS 请求，并将 DNS 解析的结果返

回给内网主机，使其能够正常上网。

如需配置 DNS 中继功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜DNS 高级配置＞→＜DNS 中继＞进入下图所示页面。通过该页面您可以查看当前的 DNS 中继配置信息，并可开启或关闭 DNS 中继服务。

DNS 中继

DNS 中继配置说明：

当您的外网接入方式为 PPPoE 或 DHCP 动态获取地址方式时，DNS 中继配置中的 DNS 服务器信息将由 Smart 设备根据从运营商处动态获取的 DNS 服务器地址自动添加到上述 DNS 中继配置列表中。如果您的外网采用静态 IP 地址接入方式，则您在进行外网接口参数配置时必须配置该接口上的主 DNS 服务器，随后该配置的 DNS 服务器的即成为设备实现 DNS 中继时的外网 DNS 解析服务器。

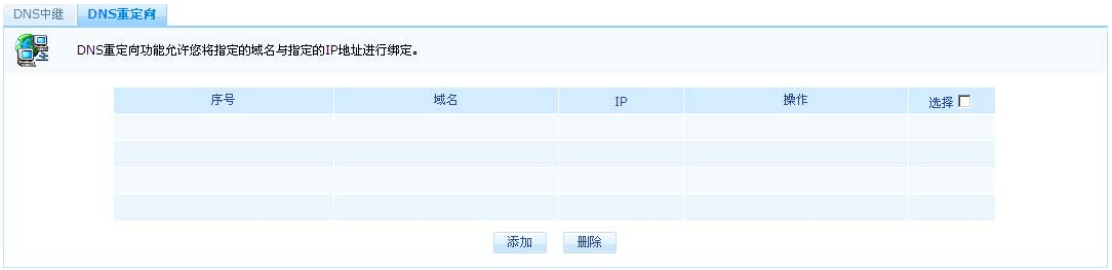
DNS重定向

在网络管理过程中，如果您希望改变某一特定域名与其真实 IP 地址的映射关系时，可以使用 DNS 重定向功能。在企业网络应用中 DNS 重定向功能可用于下图所示场景：

企业内部有一 WEB 服务器，其域名为 www.byzoro.com，其真实 IP 地址为 192.168.0.100。通常情况下用户（包括外网和内网用户）访问该服务器域名时将会被互联网中的 DNS 服务器解析为企业出口公网地址 10.0.0.100。但现在企业希望外网用户访问该服务器时使用互联网中 DNS 服务器解析的出公网地址进行访问，而内网用户访问时则使用该服务器真实 IP（192.168.0.100）进行访问。在此使用场景下，只需在 Smart 设备上针对 www.byzoro.com 域名配置 DNS 重定向即可。

DNS 重定向应用案例

如需配置 DNS 中继功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜DNS 高级配置＞→＜DNS 重定向＞进入下图所示页面。通过该页面您可以查看当前的 DNS 重定向配置信息，并可添加、删除和编辑 DNS 重定向信息。



DNS 重定向

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加 DNS 重定向配置对话框：

添加 DNS 重定向条目

配置项及其说明：

配置参数	说明
域名	设置需要进行 DNS 重定向的域名

IP	设置上述域名所对应的目的 IP 地址，即被重定向后的 IP 地址。

URL重定向

URL 重定向功能使得您可以改变用户的 URL 访问行为。如用户想要访问网址为 www.sina.com 的网站，通过配置 URL 重定向功能，您可以使其实际访问的网址变为 www.sohu.com。

如需配置 DNS 中继功能，请在配置界面左侧的主菜单栏中依次选择＜高级选项＞→＜URL 重定向＞进入下图所示页面。通过该页面您可以查看当前的 URL 重定向规则，并可添加、删除和编辑 URL 重定向规则。

URL 重定向

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加 URL 重定向配置对话框：

添加 URL 重定向

配置项及其说明：

配置参数	说明
原始 URL 地址	设置需要被重定向的 URL
重定向后的 URL 地址	设置重定向后的 URL

提示

1. 原始 URL 不支持 www.baidu.com，www.google.com，www.hao123.com 等搜索引擎。
2. 若多条配置规则的原始 URL 相同，则最先配置的重定向规则生效。

用户认证

为了规范网络的接入行为，加固网络的安全性，Smart 设备为用户提供 WEB 认证功能。近年来 WEB 认证以其无客户端依赖特性获得了用户的认可并因此而被广泛应用，同时 WEB 认证无客户端依赖特性还有效避免了其它认证方式所普遍存在的客户端软件安装和维护方面的问题。

WEB认证

Smart 设备提供的 WEB 认证功能可以基于用户网段来开启，并可以在认证成功后向用户推送指定的页面，使得网络管理员能够有针对性的对内网用户进行认证管理。

如需使用 WEB 认证功能，请在配置界面左侧的主菜单栏中依次选择＜用户认证＞→＜WEB 认证＞进入下图所示页面。通过该页面您可以查看当前的 WEB 认证配置信息，并可修改这些配置。

WEB 认证配置

配置项及其说明：

配置参数	说明
指定认证用户网段	开启按网段认证功能 开启该功能后您需要指定网段，可设置多个认证网段
用户下线检测	设置用户下线检测时间间隔 在设定的时间间隔内设备没有检测到认证用户的数据流量则将该用户的状态设置为下线状态，此时用户需重新认证才能上网。
认证注销功能配置	设置是否向认证客户端推送注销页面 此处您需要指定设备向客户端推送注销页面时使用的接口 IP 地址
强制推出页面配置	设置用户认证成功后是否强制推出特定的页面，以及该页面的 URL 地址

提示	1. 未启用网段认证功能时（即未勾选“指定认证用户网段”选项），所有用户都需要认证。 2. 启用网段认证功能，但未设置认证网段，则所有用户均不需要进行认证。

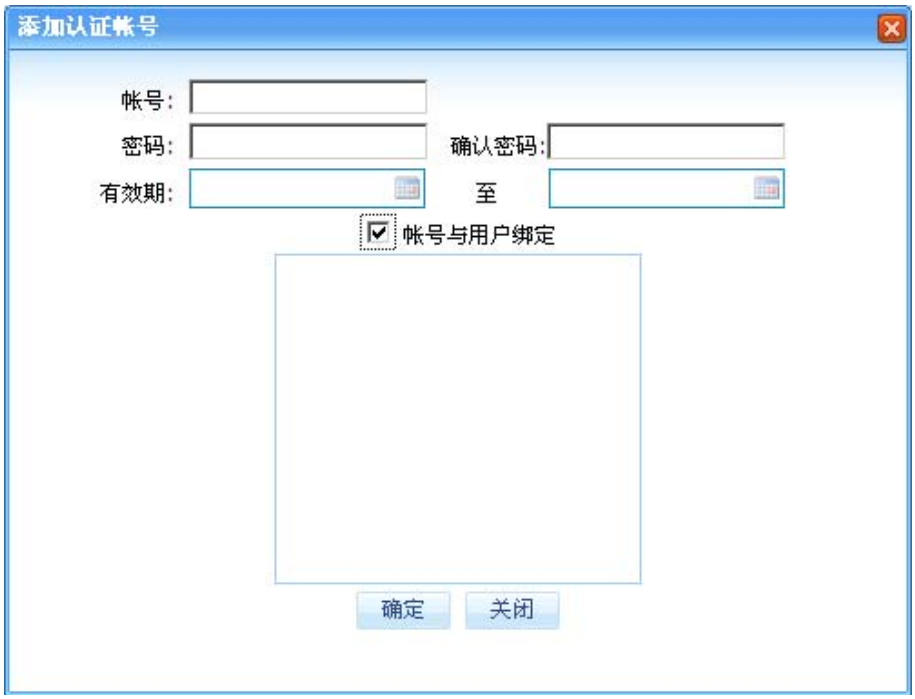
认证帐号

Smart 设备提供 WEB 认证及 LT2P VPN 远程拨号接入功能。您可以在此为这两个功能设置用户认证所需的帐号信息。

如需配置用户认证帐号，请在配置界面左侧的主菜单栏中依次选择＜用户认证＞→＜认证帐号＞进入下图所示页面。通过该页面您可以查看当前的认证帐号配置信息，并可添加、修改和删除帐号信息。

认证帐号

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加认证帐号配置对话框：



添加认证帐号

配置项及其说明：

配置参数	说明
帐号	设置用户认证的帐号名称
密码	设置用户认证的帐号密码
有效期	设置上述帐号的使用有效期，超出有效期帐号将不可用
帐号与用户绑定	设置认证帐号与上网用户的绑定关系，仅支持帐号与固定用户的绑定

流量分析

全面、准确的网络流量分析是实施科学化网络带宽管理的基础，Smart 设备具有丰富的流量分析手段，提供对流量的实时分析和历史分析能力，并能输出各类流量分析报表。让用户即能够随时掌握网络流量的实时使用情况，又能够了解网络流量的发展趋势，从而为科学管理网络流量、解决网络问题及进行网络规划提供了有效依据。

流量分析配置

本页面提供流量分析功能开关及与流量分析相关的基本参数配置。

在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜流量分析配置＞可进入下图所示

的流量分析配置页面。

流量分析配置

配置项及其说明：

配置参数	说明
实时流量分析开关	打开或关闭设备的实时流量分析功能。如果您关闭该功能，所有与实时流量分析有关的页面将无法显示分析数据。
实时流量刷新间隔	调整设备对实时流量进行分析时的时间间隔。可根据实际需要进行调整，时间间隔最小值 1 秒，最大值 512 秒，建议值为 16 秒。
历史流量分析开关	打开或关闭设备的历史流量分析功能。如果您关闭该功能，所有与历史流量分析有关的页面将无法显示分析数据。

实时流量分析

Smart 设备可提供基于各种对象的实时流量分析数据，这些对象包括用户、用户组、应用、应用类、目的 IP 地址以及接口等。

实时流量走势

通过本页面您可以查看端口，用户，用户组以及全局等五类对象的实时流量趋势分析信息。实时流量趋势分析的结果包括：实时流量趋势图、实时包速率趋势图、实时连接数趋势图。如需查看实时流量走势信息，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜实时流量分析＞→＜实时流量走势＞进入下图所示页面。

实时流量分析

参数说明：

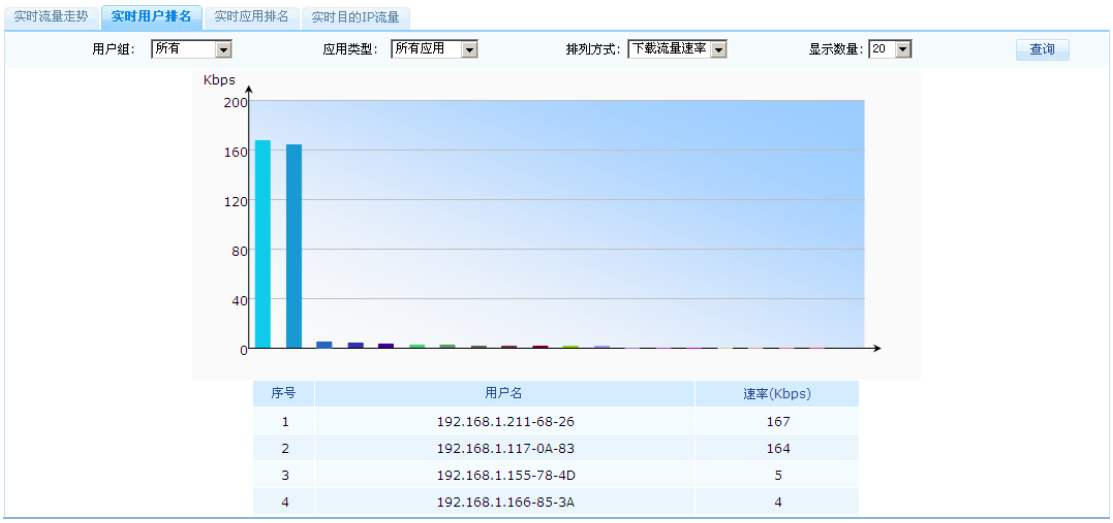
参数	说明
上传流量速率	绿色曲线代表被分析对象的接收流量分析结果
下载流量速率	蓝色曲线代表被分析对象的发送流量分析结果
最大值	在当前时间横轴显示范围内，被分析对象的流量分析数据最大值
最小值	在当前时间横轴显示范围内，被分析对象的流量分析数据最小值
平均值	在当前时间横轴显示范围内，被分析对象的流量分析数据平均值

提示	1. 当流量曲线贯穿整个时间横轴时看到的是实际的平均值，在流量曲线未贯穿时间横轴时，看到的平均值比实际的小。 2. 为了更方便流量信息的查看，在流量较小时使用 bps 做为流量单位，在流量较高时使用 Kbps，在流量更高时用 Mbps 或 Gbps。

实时用户排名

本页面为您显示当前网络中的用户实时流量排名情况，您即可以根据选定的条件查看用户的络流量排名信息。

如需查看实时用户排名信息，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜实时流量分析＞→＜实时用户排名＞进入下图所示页面。



实时用户排名

配置项及其说明：

参数	说明
用户组	指定需要进行流量排名的用户组 如果指定了具体的用户组则只针对该组内用户进行流量排名 否则对网络中的所有用户进行流量排名
应用类型	指定需要进行流量排名的应用类别 如果指定了具体的应用类型，则只对使用该应用类型的流量进行排名 否则对网络中的所有流量进行排名
排列方式	指定流量排名的流量方向及流量参数 可选项包括：上传、下载流量速率和上传、下载 IP 包速率
显示数量	指定显示用户排名的数量，可选择显示流量排名前 20、50、100 名的用户。

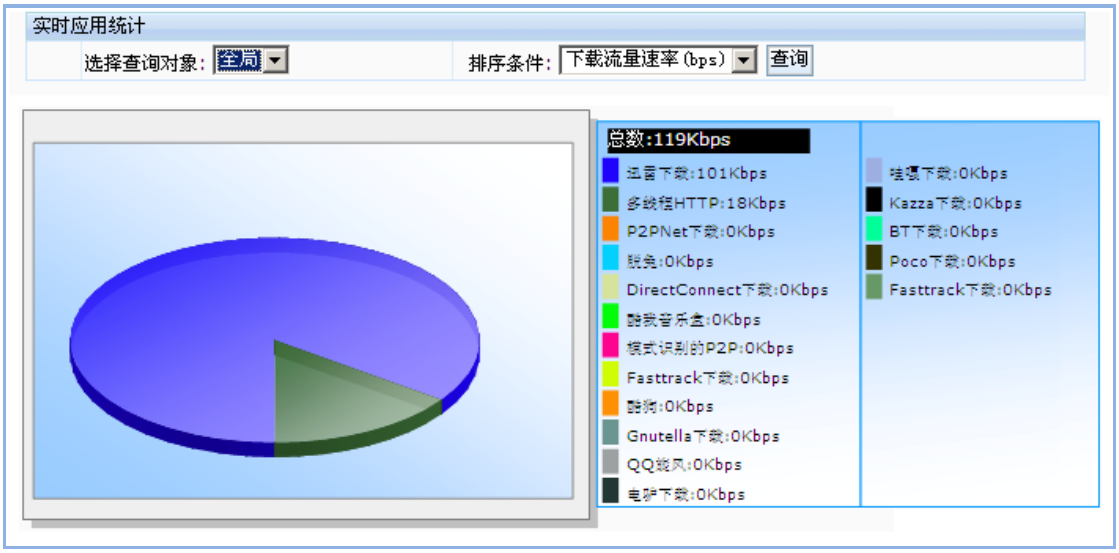
实时应用排名

实时应用排名功能可用于查询当前网络中各应用类的流量排名情况，同时您还可以查看这些应用类中的具体应用流量排名。

如需查看实时应用排名信息，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜实时流量分析＞→＜实时应用排名＞进入下图所示页面。

实时应用排名

当您将鼠标指针移动到上图所示柱状图上并点击鼠标左键，则可以查看该柱状图所代表的应用类所包含具体应用的流量统计及排名情况，如下图所示：



实时应用统计百分比

实时目的IP流量

通过本页面您可以查看最近 10 分钟内外网 IP 主机为内网用户提供服务时所产生的流量排名信息。由此您可以发现近段时间内内网用户集中访问的外网主机 IP 地址，针对用户集中访问的外网主机 IP 您可以根据网络管理的需求进行限速或阻断。

如需查看实时目的 IP 流量信息，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜实时流量分析＞→＜实时目的 IP 流量＞，并点击页面上的【查询】按钮显示下图所示页

面。

排名	目的IP	报文数	上传流量 (KB)	下载流量 (KB)	网络应用
1	119.188.1.13	8866	0	89744	网络视频[8864] 网页浏览(HTTP)[2]
2	221.201.59.192	3746	360	31344	迅雷下载[3762]
3	123.125.115.40	2162	0	17288	WEB下载[2162]
4	58.22.145.207	1155	72	8296	迅雷下载[1157]
5	111.126.0.97	781	7680	0	QVOD(P2P)[781]
6	222.50.181.110	1659	7416	32	迅雷下载[1683]
7	58.19.239.98	856	4080	2136	迅雷下载[866]
8	60.216.5.179	573	72	4480	迅雷下载[573]
9	125.34.7.140	419	4144	0	QVOD(P2P)[419]
10	125.39.155.234	884	112	3536	迅雷下载[903]

实时目的 IP 流量

查询结果参数说明：

参数	说明
目的 IP	内网用户访问的外网目的主机 IP 地址
报文数	十分钟以内，内网所有用户访问该目的 IP 主机产生的 IP 包总数
上传流量	十分钟以内，内网所有用户访问该目的 IP 主机的上传流量字节统计
下载流量	十分钟以内，内网所有用户访问该目的 IP 主机的下载流量字节统计
网络应用	显示到此目的 IP 主机的流量应用类型

提示

1. 使用该功能首先要开启目的 IP 流量开关
2. 实时目的IP流量的统计时间间隔是十分钟，可以查询到前200个目的IP。

历史流量分析

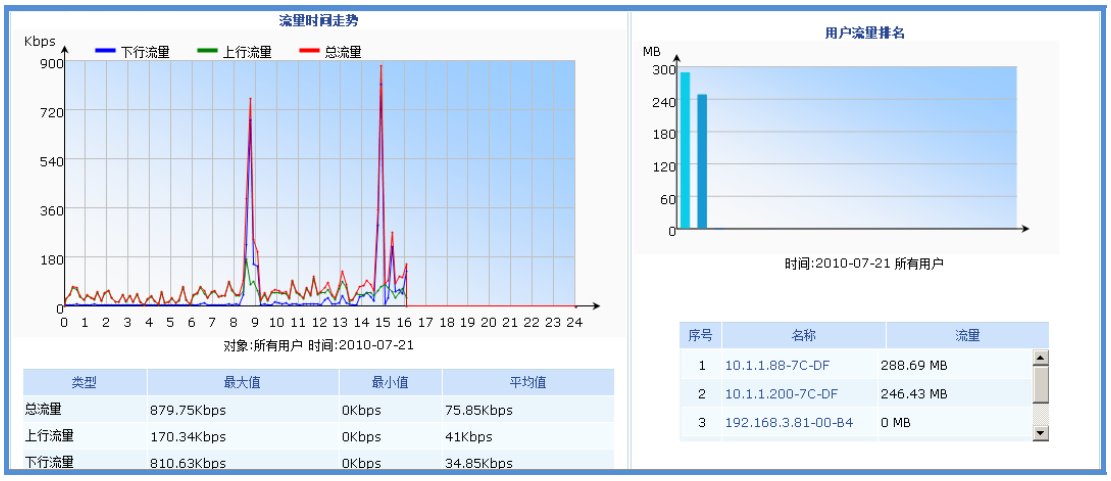
通过查看网络的历史流量分析数据，您可以了解网络的流量特征、为网络流量建立基线数据，并掌握网络流量的长期发展趋势。从为网络流量的科学管理以及未来网络的发展规划提供依据，并可以在网络出现异常时，通过分析该时间点的历史流量情况排查网络故障。

历史流量综合分析

历史流量综合分析页面为您提供历史流量走势、用户历史流量排名、应用类历史流量排名等综合流量分析信息。

如需查看历史流量综合分析信息，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→

＜历史流量分析＞→＜历史流量综合＞进入下图所示页面。

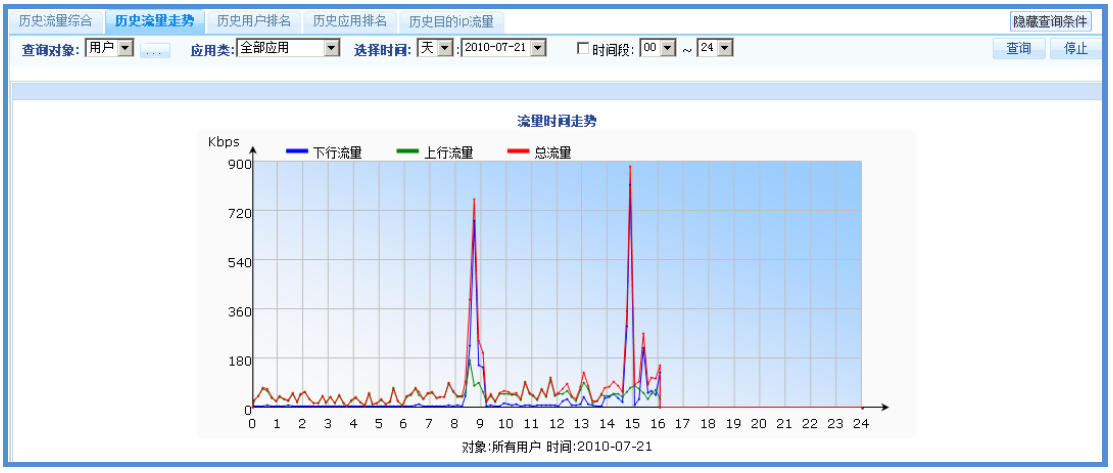


历史流量综合分析

历史流量走势

历史流量走势允许您根据选定的条件查看网络流量的历史走势情况。

如需查看历史流量走势，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜历史流量分析＞→＜历史流量走势＞进入下图所示页面。



历史流量走势

配置项及其说明：

参数	说明
查询对象	选择需要查看历史流量的对象，包括用户和接口两种对象
应用类	选择需要查看历史流量应用类
选择时间	选择需要查看历史流量的时间范围，可以查看一天、一周或一个月的流量走势

时间段	上述时间范围内每一天中的具体时间段

历史用户排名

历史用户排名允许您根据选定的条件查看用户流量的排名情况。

如需查看历史用户排名情况，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜历史流量分析＞→＜历史用户排名＞进入下图所示页面。

历史用户排名

配置项及其说明：

参数	说明
选择用户	选择需要进行流量排名的用户
应用类	选择需要进行流量排名的应用类
选择时间	选择需要进行流量排名的时间范围，可以根据一天、一周或一个月的流量进行排名
时间段	上述时间范围内每一天中的具体时间段

历史应用排名

历史应用排名允许您根据选定的条件查看网络中各应用类及具体应用的流量排名情况。

如需查看历史应用排名情况，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜历史流量分析＞→＜历史应用排名＞进入下图所示页面。

历史应用排名

配置项及其说明：

参数	说明
查询对象	指定需要进行应用流量排名的对象，包括用户和接口两种对象
应用类	选择需要进行流量排名的应用类
选择时间	选择需要进行流量排名的时间范围，可以根据一天、一周或一个月的流量进行排名
时间段	上述时间范围内每一天中的具体时间段

历史目的IP流量

查询指定时间范围内的目的 IP 流量排名情况。

如需查看历史目的 IP 流量排名情况，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜历史流量分析＞→＜历史目的 IP 流量＞进入下图所示页面。

历史目的 IP 流量排名

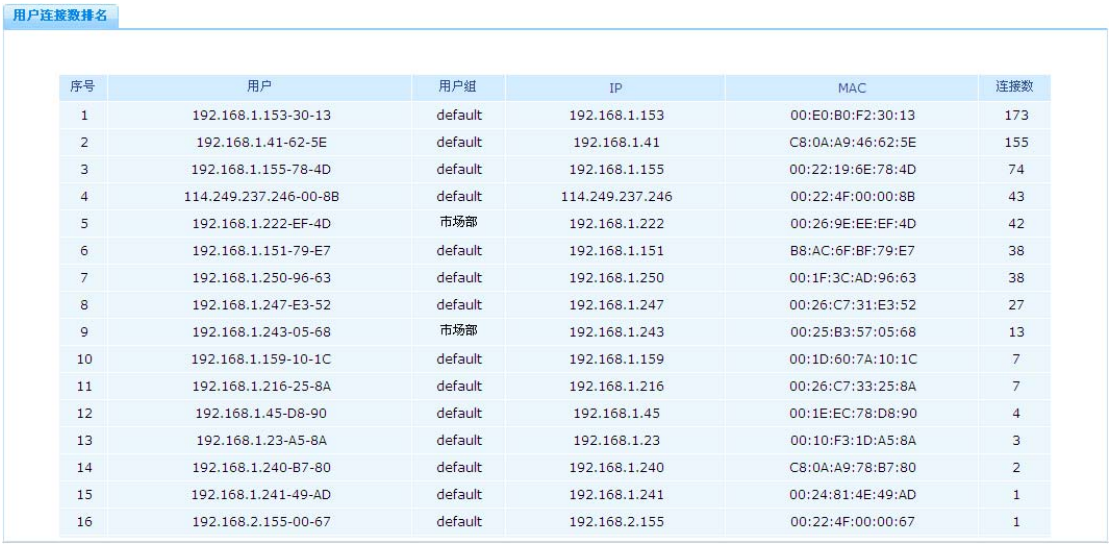
查询结果参数说明：

参数	说明
目的 IP	内网用户访问的外网目的主机 IP 地址
报文数	十分钟以内，内网所有用户访问该目的 IP 主机产生的 IP 包总数
上传流量	十分钟以内，内网所有用户访问该目的 IP 主机的上传流量字节统计
下载流量	十分钟以内，内网所有用户访问该目的 IP 主机的下载流量字节统计
网络应用	显示到此目的 IP 主机的流量应用类型

用户连接数排名

显示当前网络中所有用户的连接数排名信息。

如需查看用户连接数排名情况，请在配置界面左侧的主菜单栏中依次选择＜流量分析＞→＜用户连接数排名＞进入下图所示页面。


用户连接数排名

序号	用户	用户组	IP	MAC	连接数
1	192.168.1.153-30-13	default	192.168.1.153	00:E0:B0:F2:30:13	173
2	192.168.1.41-62-5E	default	192.168.1.41	C8:0A:A9:46:62:5E	155
3	192.168.1.155-78-4D	default	192.168.1.155	00:22:19:6E:78:4D	74
4	114.249.237.246-00-8B	default	114.249.237.246	00:22:4F:00:00:8B	43
5	192.168.1.222-EF-4D	市场部	192.168.1.222	00:26:9E:EE:EF:4D	42
6	192.168.1.151-79-E7	default	192.168.1.151	B8:AC:6F:BF:79:E7	38
7	192.168.1.250-96-63	default	192.168.1.250	00:1F:3C:AD:96:63	38
8	192.168.1.247-E3-52	default	192.168.1.247	00:26:C7:31:E3:52	27
9	192.168.1.243-05-68	市场部	192.168.1.243	00:25:B3:57:05:68	13
10	192.168.1.159-10-1C	default	192.168.1.159	00:1D:60:7A:10:1C	7
11	192.168.1.216-25-8A	default	192.168.1.216	00:26:C7:33:25:8A	7
12	192.168.1.45-D8-90	default	192.168.1.45	00:1E:EC:78:D8:90	4
13	192.168.1.23-A5-8A	default	192.168.1.23	00:10:F3:1D:A5:8A	3
14	192.168.1.240-B7-80	default	192.168.1.240	C8:0A:A9:78:B7:80	2
15	192.168.1.241-49-AD	default	192.168.1.241	00:24:81:4E:49:AD	1
16	192.168.2.155-00-67	default	192.168.2.155	00:22:4F:00:00:67	1

审计查询

Smart 提供对各种网络内容进行审计和查询的能力，当前设备提供对八类应用的审计结果查询。下面分别对这八类应用的审计查询操作进行介绍。

浏览网站

通过本页面您可以查询网络用户进行浏览网站的上网行为记录。这些记录包括浏览网站的用户名称及其 IP 地址，所访问网页的标题及 URL 地址，网站所属的网址分类，访问网站的时

间等。

如需查看用户浏览网站的记录，请在配置界面左侧的主菜单栏中依次选择＜审计查询＞→＜浏览网站＞进入下图所示页面。

浏览网站

当网页标题显示为乱码时，您可以尝试点击上图所示的转换编码图标切换到正常文字显示。另外，您还可以点击上图右上角所示的图标设置和编辑查询条件。查询条件设置对话框如下图：

设备查询条件

配置项及其说明：

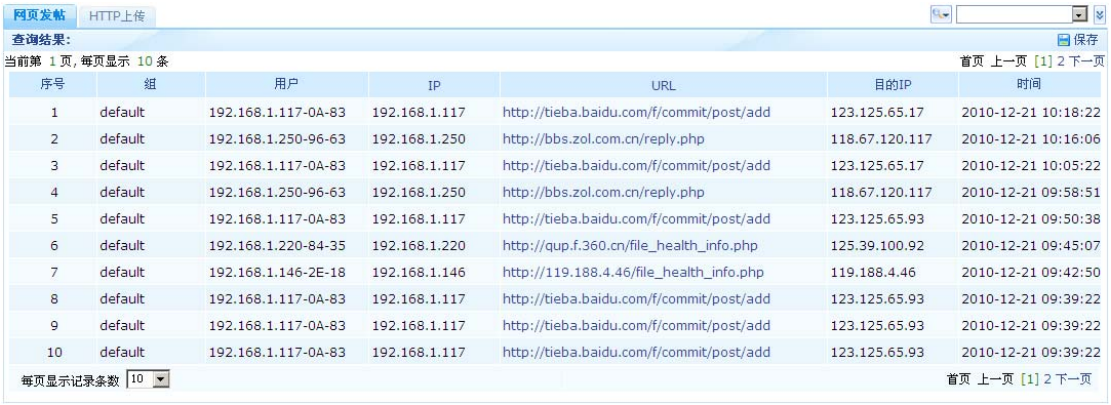
参数	说明
查询对象	选择需要查询的组、用户或 IP 地址
关键字	可以按照填写的关键字查询符合要求的网页，可指定 URL 和 Title 关键字

时间范围	选择要查询的起始时间和截止时间
排序	设备查询结果的排序方式，可选择“按时间升序”和“按时间降序”两种方式。
搜索	按照查询条件进行搜索符合条件的内容
保存	保存设置的查询条件

网页发贴

通过本页面您可以查询网络用户进行网页发贴的行为及内容。其中查看发贴内容需要使用设备随机附带的 USB KEY。

如需查看用户网页发贴的记录，请在配置界面左侧的主菜单栏中依次选择＜审计查询＞→＜网页发帖＞进入下图所示页面。


网页发帖

查询结果：

保存

当前第 1 页，每页显示 10 条　　首页 上一页 [1] 2 下一页

序号	组	用户	IP	URL	目的IP	时间
1	default	192.168.1.117-0A-83	192.168.1.117	http://tieba.baidu.com/f/commit/post/add	123.125.65.17	2010-12-21 10:18:22
2	default	192.168.1.250-96-63	192.168.1.250	http://bbs.zol.com.cn/reply.php	118.67.120.117	2010-12-21 10:16:06
3	default	192.168.1.117-0A-83	192.168.1.117	http://tieba.baidu.com/f/commit/post/add	123.125.65.17	2010-12-21 10:05:22
4	default	192.168.1.250-96-63	192.168.1.250	http://bbs.zol.com.cn/reply.php	118.67.120.117	2010-12-21 09:58:51
5	default	192.168.1.117-0A-83	192.168.1.117	http://tieba.baidu.com/f/commit/post/add	123.125.65.93	2010-12-21 09:50:38
6	default	192.168.1.220-84-35	192.168.1.220	http://qup.f.360.cn/file_health_info.php	125.39.100.92	2010-12-21 09:45:07
7	default	192.168.1.146-2E-18	192.168.1.146	http://119.188.4.46/file_health_info.php	119.188.4.46	2010-12-21 09:42:50
8	default	192.168.1.117-0A-83	192.168.1.117	http://tieba.baidu.com/f/commit/post/add	123.125.65.93	2010-12-21 09:39:22
9	default	192.168.1.117-0A-83	192.168.1.117	http://tieba.baidu.com/f/commit/post/add	123.125.65.93	2010-12-21 09:39:22
10	default	192.168.1.117-0A-83	192.168.1.117	http://tieba.baidu.com/f/commit/post/add	123.125.65.93	2010-12-21 09:39:22

每页显示记录条数 10　　首页 上一页 [1] 2 下一页

有关网页发贴查询条件的设置方法请参考审计查询一章中“浏览网站”相关部分内容。

电子邮件

通过本页面您可以查询网络用户发送和接收电子邮件的行为及内容（包括邮件附件）。其中查看邮件内容需要使用设备随机附带的 USB KEY。下面以发送邮件为例介绍电子邮件审计查询的操作方法，其它电子邮件查询操作与其相似在此不做赘述。

发送邮件

如需查看用户发送电子邮件的记录，请在配置界面左侧的主菜单栏中依次选择＜审计查询＞→＜电子邮件＞→＜发送邮件＞进入下图所示页面。

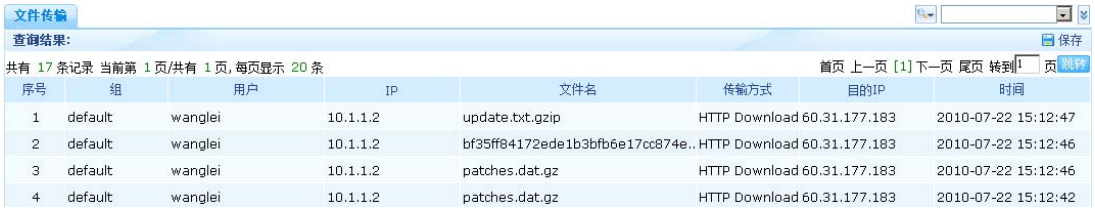
发送邮件

有关发送邮件查询条件的设置方法请参考审计查询一章中“浏览网站”相关部分内容。

文件传输

通过本页面您可以查询网络用户进行文件传输的行为。

如需查看用户进行文件传输的记录，请在配置界面左侧的主菜单栏中依次选择＜审计查询＞→＜文件传输＞进入下图所示页面。



文件传输

有关文件传输查询条件的设置方法请参考审计查询一章中“浏览网站”相关部分内容。

聊天信息

通过本页面您可以查询网络用户通过聊天工具进行聊天的行为及内容。其中查看聊天内容需要使用设备随机附带的 USB KEY。

如需查看用户的聊天记录，请在配置界面左侧的主菜单栏中依次选择＜审计查询＞→＜聊天信息＞进入下图所示页面。

聊天信息

有关聊天信息查询条件的设置方法请参考审计查询一章中“浏览网站”相关部分内容。

网络搜索

通过本页面您可以查询网络用户通过搜索引擎进行网络搜索的行为及内容。其中查看搜索关键字内容需要使用设备随机附带的 USB KEY。下面以百度搜索为例介绍网络搜索审计查询的操作方法，其它网络搜索审计查询操作与其相似在此不做赘述。

如需查看用户的聊天记录，请在配置界面左侧的主菜单栏中依次选择＜审计查询＞→＜网络搜索＞→＜网络搜索＞进入下图所示页面。

序号	组	用户	IP	主机	关键字	目的IP	时间
1	default	wangpeng	192.168.1.206	Baidu	********	61.135.169.105	2010-12-21 10:41:21
2	default	wangpeng	192.168.1.206	Baidu	********	61.135.169.105	2010-12-21 10:41:21
3	default	wangpeng	192.168.1.206	Baidu	********	61.135.169.105	2010-12-21 10:38:02
4	default	192.168.1.89-2C-51	192.168.1.89	Baidu	********	61.135.169.105	2010-12-21 10:36:13
5	default	192.168.1.89-2C-51	192.168.1.89	Baidu	********	61.135.169.105	2010-12-21 10:36:13
6	default	192.168.1.89-2C-51	192.168.1.89	Baidu	********	61.135.169.105	2010-12-21 10:36:13
7	default	192.168.1.89-2C-51	192.168.1.89	Baidu	********	61.135.169.105	2010-12-21 10:36:13
8	default	192.168.1.89-2C-51	192.168.1.89	Baidu	********	61.135.169.105	2010-12-21 10:36:13
9	default	192.168.1.89-2C-51	192.168.1.89	Baidu	********	61.135.169.105	2010-12-21 10:36:13
10	default	192.168.1.89-2C-51	192.168.1.89	Baidu	********	61.135.169.105	2010-12-21 10:34:52

网络搜索

有关网络搜索查询条件的设置方法请参考审计查询一章中“浏览网站”相关部分内容。

网络游戏

通过本页面您可以查询网络用户使用网络游戏的行为。

如需查看用户使用网络游戏的记录，请在配置界面左侧的主菜单栏中依次选择＜审计查询＞→＜网络游戏＞进入下图所示页面。

序号	组	用户	IP	应用名称	游戏帐号	目的IP	时间
1	default	wanglei	10.1.1.2	腾讯网游		218.6.12.99	2010-07-22 15:09:26
2	default	wanglei	10.1.1.2	天龙八部_搜狐畅游		112.91.130.195	2010-07-22 14:53:15
3	default	wanglei	10.1.1.2	天书奇谈		123.129.235.216	2010-07-22 14:47:03
4	default	wanglei	10.1.1.2	天书奇谈		123.129.235.216	2010-07-22 14:47:03
5	default	wanglei	10.1.1.2	天书奇谈		123.129.235.216	2010-07-22 14:47:00

网络游戏

有关网络游戏查询条件的设置方法请参考审计查询一章中“浏览网站”相关部分内容。

视频播放

通过本页面您可以查询网络用户观看网络视频的行为。

如需查看用户观看网络视频的记录，请在配置界面左侧的主菜单栏中依次选择＜审计查询＞→＜视频播放＞进入下图所示页面。


网站视频

查询结果：

保存

当前第 1 页，每页显示 20 条　　当前第 1 页，每页显示 20 条 首页 上一页 [1] 下一页

序号	组	用户	目的IP	网站名称	标题	时间
1	default	192.168.1.117-0A-83	113.31.34.183	土豆	preload static	2010-12-21 10:24:46
2	default	192.168.1.117-0A-83	114.112.182.56	土豆	小酒窝-林俊杰（高清版）_在线视频观...	2010-12-21 10:23:57
3	default	192.168.1.117-0A-83	114.112.182.56	土豆	林俊杰 - 小酒窝_在线视频观看_土豆网...	2010-12-21 10:23:47
4	default	192.168.1.117-0A-83	113.31.34.183	土豆	nothing here	2010-12-21 10:23:47
5	default	192.168.1.117-0A-83	114.112.182.56	土豆	林俊杰 - 小酒窝（高清MV）_在线视频...	2010-12-21 10:22:52
6	default	192.168.1.117-0A-83	60.217.58.140	酷6	空间精华	2010-12-21 10:20:22
7	default	192.168.1.117-0A-83	123.125.114.32	video_other	百度视频搜索_水木年华 水	2010-12-21 09:54:23
8	default	192.168.1.117-0A-83	125.39.101.5	酷6	空间精华	2010-12-21 09:52:03
9	default	192.168.1.117-0A-83	202.108.251.84	酷6	酷溜网	2010-12-21 09:52:03
10	default	192.168.1.117-0A-83	123.125.114.32	video_other	百度视频搜索_高级搜索	2010-12-21 09:51:24

每页显示记录条数 20　　当前第 1 页，每页显示 20 条 首页 上一页 [1] 下一页

视频播放

有关视频播放查询条件的设置方法请参考审计查询一章中“浏览网站”相关部分内容。

应用统计

应用统计

应用统计可以帮助您根据指定查询条件查看当前网络用户使用各种网络应用的频度。

如需查看应用统计信息，请在配置界面左侧的主菜单栏中依次选择＜应用统计＞→＜应用统计＞进入下图所示页面。


应用统计

隐藏统计条件

统计条件：

指定用户：　选择　　时间范围：2010-12-21 00:00:00 ~ 2010-12-21 11:04:16　　搜索　取消

统计结果：

共有 5 条记录 当前第 1 页/共有 1 页，每页显示 20 条　　首页 上一页 [1] 下一页 尾页 转到 1 页 跳转

序号	应用类型	用户数量	应用数量
1	网站访问	28	1343
2	在线聊天	28	836
3	邮件接收	13	105
4	论坛发帖	3	23
5	邮件发送	6	13

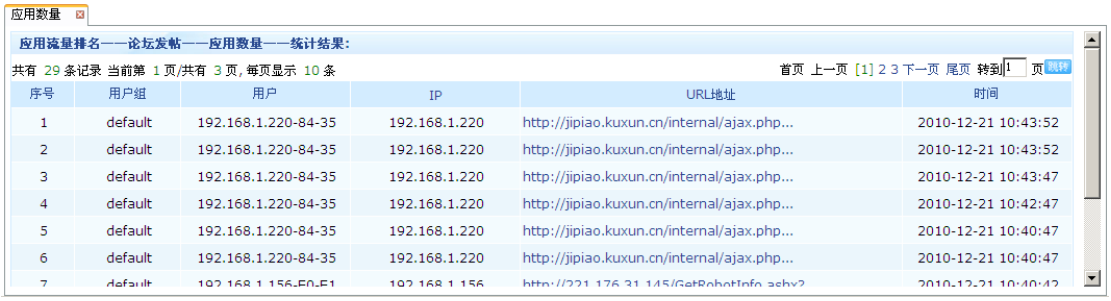
每页显示记录条数 20　　首页 上一页 [1] 下一页 尾页 转到 1 页 跳转

应用统计

通过点击应用统计查询结果中“用户数量”一列的数字，您还可以进一步查看指定时间内使用该应用的具体用户。

应用统计－用户数量

通过点击应用统计查询结果中“应用数量”一列的数字, 您还可以进一步查看指定时间内某一应用类中的具体应用使用情况。



应用统计－应用数量

目的IP统计

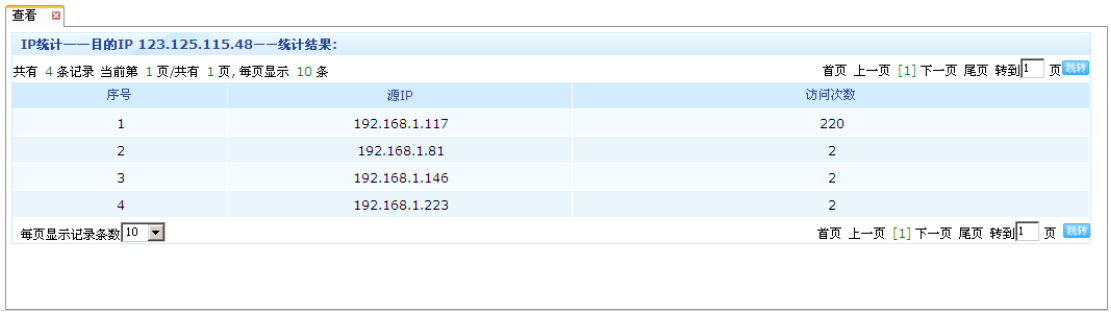
目的 IP 统计可以帮助您了解网络用户对某个特定目的 IP 主机的访问频度。

如需查看目的 IP 统计信息，请在配置界面左侧的主菜单栏中依次选择＜应用统计＞→＜目的 IP 统计＞进入下图所示页面。

目的 IP 统计

通过点击上图表格最右边一列中的“查看”按钮您可以详细了解访问了该目的 IP 的内网主

机。



访问目的 IP 的源主机列表

网站访问统计

网站访问统计可以帮助您根据指定查询条件查看当前网络中网站访问的统计信息。

如需查看网站访问统计信息，请在配置界面左侧的主菜单栏中依次选择＜应用统计＞→＜网站访问统计＞进入下图所示页面。

网站访问统计

通过点击网站访问统计查询结果中“网站类型”一列的数字，您还可以进一步查看用户所访问网站的所属的网址类别。

网站访问统计－网站类型

通过点击网站访问统计查询结果中“网站访问量”一列的数字，您还可以进一步查看用户在指定条件下访问的所有网站地址。

网站访问统计－网站访问量

邮件收发统计

邮件收发统计可以帮助您根据指定查询条件查看当前网络中邮件收发的统计信息。

如需查看邮件收发统计信息，请在配置界面左侧的主菜单栏中依次选择＜应用统计＞→＜邮件收发统计＞进入下图所示页面。

邮件收发统计

通过点击邮件收发统计查询结果中“邮件类型”一列的数字，您还可以进一步查看用户在指定条件下所收发的邮件类型。

邮件收发统计－邮件类型

通过点击邮件收发统计查询结果中“邮件数量”一列的数字，您还可以进一步查看用户在指定条件下所收发的全部邮件。

邮件收发统计-1

在线聊天统计

在线聊天统计可以帮助您根据指定查询条件查看当前网络中用户聊天的统计信息。

如需查看在线聊天统计信息，请在配置界面左侧的主菜单栏中依次选择＜应用统计＞→＜在线聊天统计＞进入下图所示页面。

在线聊天统计

通过点击聊天信息统计查询结果中“聊天类型”一列的数字，您还可以进一步查看用户在指定条件下所使用聊天工具的类型。


聊天类型

在线聊天——用户 192.168.1.163-A7-2C——聊天类型——统计结果：

共有 3 条记录 当前第 1 页/共有 1 页，每页显示 10 条　　首页 上一页 [1] 下一页 尾页 转到 1 页 跳转

序号	聊天类型	聊天数量	上传流量速率	下载流量速率	字节总数
1	MSN聊天	1	5.0KB	5.6KB	10.6KB
2	MSN在线	3	2.4KB	3.2KB	5.6KB
3	QQ聊天	56	50.6KB	51.3KB	101.8KB

每页显示记录条数 10　　首页 上一页 [1] 下一页 尾页 转到 1 页 跳转

在线聊天统计－聊天类型

通过点击聊天信息统计查询结果中“聊天数量”一列的数字，您还可以进一步查看用户在指定条件下的聊天记录。


聊天数量

在线聊天——用户 192.168.1.146-2E-18——聊天数量——统计结果：

共有 27 条记录 当前第 1 页/共有 3 页，每页显示 10 条　　首页 上一页 [1] 2 3 下一页 尾页 转到 1 页 跳转

序号	用户组	用户	IP	聊天类型	聊天帐号	目的IP	发送时间
1	default	192.168.1.146-2E-18	192.168.1.146	MSN在线	l.wch	64.4.45.62	2010-12-21 11:50:19
2	default	192.168.1.146-2E-18	192.168.1.146	QQ聊天	516656373	58.251.58.239	2010-12-21 11:48:34
3	default	192.168.1.146-2E-18	192.168.1.146	QQ聊天	516656373	121.14.75.189	2010-12-21 11:48:34
4	default	192.168.1.146-2E-18	192.168.1.146	QQ聊天	516656373	112.90.138.137	2010-12-21 11:47:43
5	default	192.168.1.146-2E-18	192.168.1.146	QQ聊天	516656373	58.251.58.239	2010-12-21 11:33:34
6	default	192.168.1.146-2E-18	192.168.1.146	QQ聊天	516656373	121.14.75.189	2010-12-21 11:33:34
7	default	192.168.1.146-2E-18	192.168.1.146	QQ聊天	516656373	121.14.75.189	2010-12-21 11:18:34

在线聊天统计－聊天数量

论坛发帖统计

论坛发贴统计可以帮助您根据指定查询条件查看当前网络中论坛发贴的统计信息。

如需查看论坛发贴统计信息，请在配置界面左侧的主菜单栏中依次选择＜应用统计＞→＜论坛发贴统计＞进入下图所示页面。


论坛发帖统计　　隐藏统计条件

统计条件：

指定用户：　选择　　时间范围：2010-12-21 00:00:00 ~ 2010-12-21 11:59:04　　搜索　取消

统计结果：

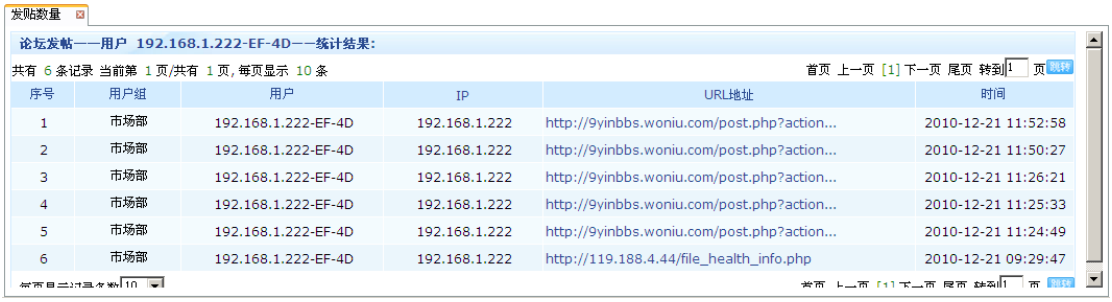
共有 6 条记录 当前第 1 页/共有 1 页，每页显示 20 条　　首页 上一页 [1] 下一页 尾页 转到 1 页 跳转

序号	用户	IP	发贴数量	上传流量速率	下载流量速率	字节总数
1	192.168.1.117-0A-83	192.168.1.117	18	102.3KB	132.0KB	234.3KB
2	192.168.1.220-84-35	192.168.1.220	8	73.0KB	93.2KB	166.1KB
3	192.168.1.222-EF-4D	192.168.1.222	6	29.8KB	4.6KB	34.5KB
4	192.168.1.146-2E-18	192.168.1.146	3	6.5KB	3.2KB	9.8KB
5	192.168.1.250-96-63	192.168.1.250	3	68.1KB	10.1KB	78.2KB
6	192.168.1.156-E0-E1	192.168.1.156	1	1.4KB	834Byte	2.2KB

每页显示记录条数 20　　首页 上一页 [1] 下一页 尾页 转到 1 页 跳转

论坛发贴统计

通过点击论坛发贴统计查询结果中“发贴数量”一列的数字，您还可以进一步查看用户在指定条件下的发贴记录。



序号	用户组	用户	IP	URL地址	时间
1	市场部	192.168.1.222-EF-4D	192.168.1.222	http://9yinbbs.woniu.com/post.php?action...	2010-12-21 11:52:58
2	市场部	192.168.1.222-EF-4D	192.168.1.222	http://9yinbbs.woniu.com/post.php?action...	2010-12-21 11:50:27
3	市场部	192.168.1.222-EF-4D	192.168.1.222	http://9yinbbs.woniu.com/post.php?action...	2010-12-21 11:26:21
4	市场部	192.168.1.222-EF-4D	192.168.1.222	http://9yinbbs.woniu.com/post.php?action...	2010-12-21 11:25:33
5	市场部	192.168.1.222-EF-4D	192.168.1.222	http://9yinbbs.woniu.com/post.php?action...	2010-12-21 11:24:49
6	市场部	192.168.1.222-EF-4D	192.168.1.222	http://119.188.4.44/file_health_info.php	2010-12-21 09:29:47

论坛发贴统计－发贴数量

报表中心

设备内置了丰富的数据分析报告，并且各种报告还支持导出以便于存档或作为网络工作汇报的资料。设备中的报告类型分为流量分析报告，用户分析报告，应用分析报告和时间分析报告。

流量分析报告

如需使用设备中的流量分析报告功能，请在配置界面左侧的主菜单栏中依次选择＜报表中心＞→＜流量分析报告＞进入下图所示页面。

类型	最大值	最小值	平均值
总流量	1.15Mbps	0Mbps	0.25Mbps

序号	名称	流量
1	192.168.1.117-0A-83	165.17 MB
2	192.168.1.159-10-1C	153.85 MB
3	wangpeng	121.11 MB

流量分析报告

用户分析报告

如需使用设备中的用户分析报告功能，请在配置界面左侧的主菜单栏中依次选择＜报表中心＞→＜用户分析报告＞进入下图所示页面。

用户分析报告

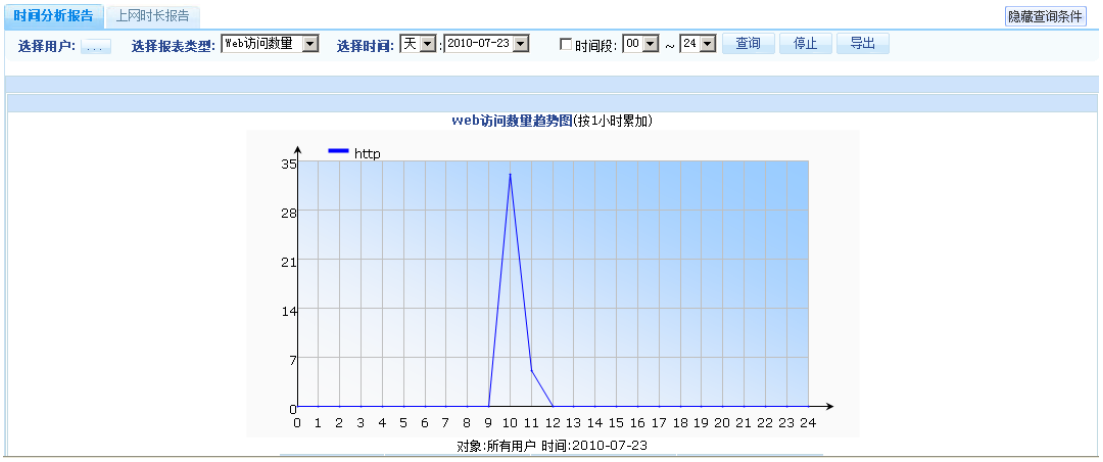
应用分析报告

如需使用设备中的应用分析报告功能，请在配置界面左侧的主菜单栏中依次选择＜报表中心＞→＜应用分析报告＞进入下图所示页面。

应用分析报告

时间分析报告

如需使用设备中的时间分析报告功能，请在配置界面左侧的主菜单栏中依次选择＜报表中心＞→＜时间分析报告＞进入下图所示页面。



时间分析报告

日志管理

网站封堵日志

当您启用网站分类封堵功能后，如果有用户的上网行为触犯相应的封堵策略则设备会生成日志。通过查看这些日志，您将可以了解网络中那些用户试图访问了这些被封堵的网站。

如需查看网站封堵日志，请在配置界面左侧的主菜单栏中依次选择＜日志管理＞→＜网站封堵日志＞进入下图所示页面。

网站分类封堵日志

应用控制日志

当您启用应用控制功能后，如果有用户的上网行为触犯相应的应用控制策略则设备会生成日志。通过查看这些日志，您将可以了解网络中那些用户试图使用这些被控制的应用。

如需查看应用控制日志，请在配置界面左侧的主菜单栏中依次选择＜日志管理＞→＜应用控制日志＞进入下图所示页面。

应用控制日志

内容过滤日志

当您启用内容过滤功能后，如果有用户的上网行为触犯相应的内容过滤策略则设备会生成日志。通过查看这些日志，您将可以了解网络中那些用户试图发送或接收了包含被过滤关键字的内容。

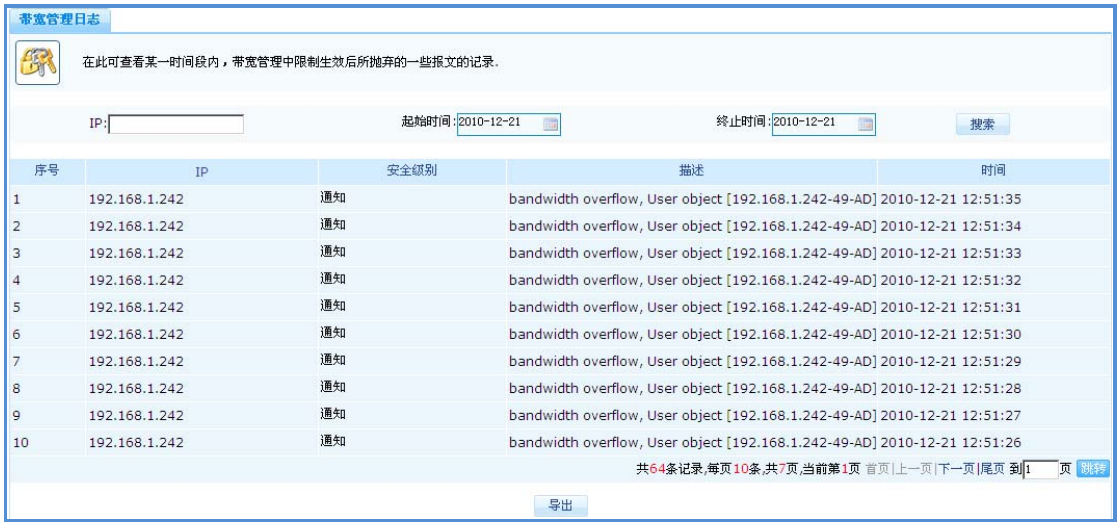
如需查看内容过滤日志，请在配置界面左侧的主菜单栏中依次选择＜日志管理＞→＜内容过滤日志＞进入下图所示页面。

内容过滤日志

带宽管理日志

当您启用了带宽管理功能后，如果用户的上网流量超出了流量管理的限制值则设备会生成日志。通过查看这些日志，您将可以了解网络中那些用户的流量超出了其授权使用范围。

如需查看带宽管理日志，请在配置界面左侧的主菜单栏中依次选择＜日志管理＞→＜带宽管理日志＞进入下图所示页面。

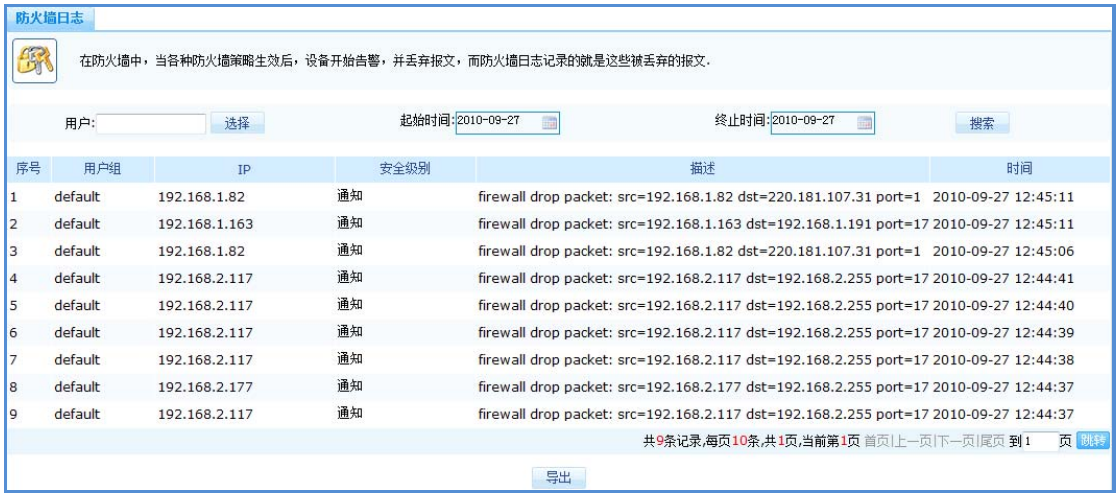


带宽管理日志

防火墙日志

当您启用了防火墙功能后，如果有用户的上网行为触犯相应的防火墙策略则设备会生成日志。通过查看这些日志，您将可以了解网络中那些用户进行了违反防火墙规则的操作。

如需查看防火墙日志，请在配置界面左侧的主菜单栏中依次选择＜日志管理＞→＜防火墙日志＞进入下图所示页面。



防火墙日志

系统日志

系统日志记录一切与设备管理相关的日志信息，包括网络管理者登录设备进行管理和操作的信息。

如需查看系统日志，请在配置界面左侧的主菜单栏中依次选择＜日志管理＞→＜系统日志＞进入下图所示页面。

系统日志

设备管理

Smart 设备为网络管理者提供灵活安全的设备管理手段，你可以根据设备管理的需求设置不同权限的管理角色和账号，可以指定允许访问和管理设备的 IP 地址。同时还可以对设备的配置及审计数据进行备份和恢复操作。

时间设置

设备的系统时间是非常重要的系统参数，正确的系统时间是设备能够正确实现按时间控制用户和应用的前提，也是审计记录具有正确时间的前提。

如需设置设备的系统时间，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜时间设置＞进入下图所示页面。通过该页面您可以查看和修改设备当前的系统时间。

时间设置

“提取电脑时间”指提取设备管理主机的操作系统时间做为本设备的系统时间。

管理授权

Smart 设备支持分级分权管理的能力，可根据企业对设备管理需求为管理员设置不同权限的管理角色及管理账号。当使用不同权限账号的管理员登录设备时，其所能查看和配置的信息及功能也是不一样的。

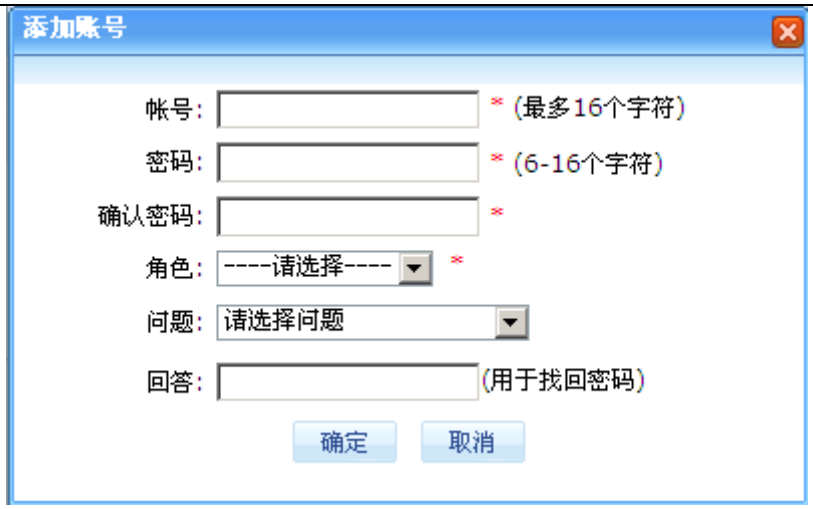
设备管理帐号

帐号管理的作用是通过对设备操作者权限的设定，来控制操作者对系统的操作范围。Smart 设备支持多角色多用户管理。同时设备预置了一个超级管理员的帐号，命名为 admin。默认情况下，只有超级管理员才拥有所有的权限，它能够对设备进行全面的配置，能够查看设备中的所有信息，能够为其它设备管理员进行授权。除超级管理员外，其它设备管理员如需登录 Smart 设备进行操作，都必须预先由超级管理员授权创建管理账号。

如需使用设备管理账号功能，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜管理授权＞→＜设备管理帐号＞进入下图所示页面。通过该页面您可以添加、查看、修改和删除设备管理账号信息。

帐号管理

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加账号配置对话框：



添加帐号

配置项及其说明：

参数	说明
帐号	设置管理员帐号名 只能输入英文字母，符号和数字，最多 16 个字符
密码	设置管理员帐号密码 只能输入英文字母，符号和数字，6-16 个字符
确认密码	重复输入上述管理员帐号密码
角色	为管理员帐号选择相应的管理角色
问题	选择用于找回帐号的问题
回答	对上述问题的回答

设备管理角色

用户帐号的权限由其所归属的管理角色确定，如果您改变了管理帐号所属的管理角色，则它的管理权限也会随之改变。通过使用设备管理角色配置功能，您可以根据设备管理需要创建新的设备管理角色，还可以修改和删除其它非内置的管理角色。

如需使用设备管理角色功能，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜管理授权＞→＜设备管理角色＞进入下图所示页面。通过该页面您可以添加、查看、修改和删除设备管理角色配置。

设备管理角色

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加管理角色配置对话框：

添加设备管理角色

配置项及其说明：

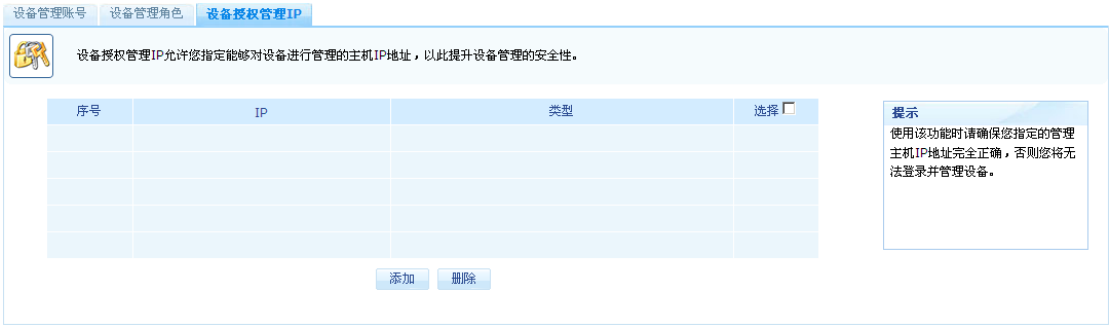
参数	说明
角色名称	设置管理员角色名称 只能输入英文字母，符号和数字，最多 16 个字符
描述	设置管理员角色的描述信息
配置	指定管理员角色对设备的操作权限，即能够查看和操作的设备管理页面。

设备授权管理IP

为了进一步增强设备管理的安全性，Smart 设备允许您指定用于管理设备的网管主机 IP 地

址，以防止非法用户利用未授权管理主机登录设备进行非法操作。

如需配置设备授权管理 IP 功能，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜管理授权＞→＜设备授权管理 IP＞进入下图所示页面。通过该页面您可以添加、查看、修改和删除设备授权管理 IP 信息。



设备授权管理 IP

在上图所示页面中点击【添加】按钮您可以进入如下所示的添加授权管理 IP 对话框：

添加授权管理 IP

配置项及其说明：

参数	说明
授权管理主机 IP 地址	设置允许管理设备的网管主机 IP 地址
授权管理方式	设置允许网管主机使用的设备管理方式，包括 HTTP 和 TELNET 两种方式

软件升级

通过使用软件升级配置页面您可以对设备的软件版本、URL 库及应用协议库进行升级操作。

如需对设备进行软件升级操作，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜软件升级＞进入下图所示页面。

软件升级

版本升级

Smart 设备会不定期发布新的软件版本，通常情况下新的软件版本会增加新的功能或修补已发现的软件问题。您可以根据设备使用情况及网络管理需求升级新的软件版本。

版本升级

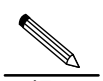
版本升级说明：

Smart 设备支持 HTTP、TFTP 和 FTP 三种升级方式，您可以根据自己的实际情况选择不同的升级方式。

若选择 HTTP 方式，点“浏览”按钮，选择您当前正在操作的网管主机中的软件版本文件，再点击【确定】按钮，即可升级版本。

若选择 TFTP 方式，请正确填写存放版本文件的 TFTP 服务器 IP 地址及需要升级的版本文件名称，点【确定】按钮，即可升级版本。

若选择 FTP 方式，请正确填写存放软版本文件的 FTP 服务器 IP 地址、FTP 登录帐号、密码及需要升级的版本文件名称，点【确定】按钮，即可升级版本。

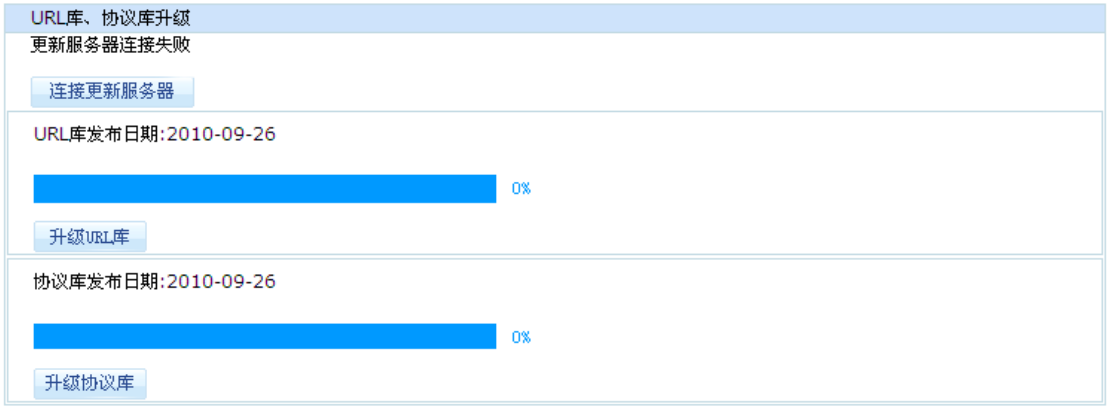


提示

若选择TFTP及FTP方式进行升级，在输入版本文件名称时请注意所输入的文件名需区分大小写，如果文件有后缀名则必须同时输入后缀名。

URL及协议库升级

网络中的应用（或协议）及 URL 随时都在发生变化，为了保证设备中应用及 URL 识别库的准确性和实时性，以满足网络管理的需求。Smart 设备提供 URL 及协议库升级能力。



URL 及协议库升级

配置项及其说明（URL 库及协议库升级）：

参数	说明
连接更新服务器	用于测试设备与更新服务器的通讯是否正常，只有正常通讯情况下才能够成功升级 URL 库和协议库。
升级 URL 库	对 URL 库进行更新操作
升级协议库	对协议库进行更新操作

配置管理

通过配置管理菜单所提供的功能，您可以对 smart 设备中当前正在使用的配置信息备份为文件、将原来备份好的配置文件重新导入设备中，还可以将 smart 设备中的配置信息恢复为出厂默认状态。

备份配置

备份配置功能帮助您将设备当前正在使用的配置信息备份为文件，以便于您对设备配置信息的管理。同时也可作为以后对设备配置进行恢复的源文件。

如需对设备进行备份配置操作，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜配置管理＞→＜备份配置＞进入下图所示页面。

备份配置

备份配置说明：

Smart 设备支持通过 HTTP 下载的方式将设备配置文件直接保存到当前正在操作的网管主机本地硬盘中，还支持通过 FTP 方式将设备配置文件备份外部的 FTP 服务器中。

若选择“备份到管理主机”选项，然后点击【备份】按钮，则设备会自动生成“下载”链接，您可以点击下载链接将配置文件保存到管理主机本地硬盘中。

若选择“备份到 FTP 服务器”选项，则您需要正确填写存放配置文件的 FTP 服务器 IP 地址、登录帐号和密码，然后执行备份操作。

提示

使用FTP方式备份时，请确保您所使用的FTP登录帐号具有写入权限，否则将无法完成配置备份。

导入配置

当您用新设备替换旧设备时，导入配置功能可以帮助您把从旧设备中备份出来的配置信息导入到新设备中，从而使得新设备能够快速配置和使用。另外，当您准备对设备配置作大的改动之前，您也可以先对设备配置进行备份，当新配置出现问题时，您可以导入旧配置使得网络快速恢复。

如需将配置信息导入到设备中，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜配置管理＞→＜导入配置＞进入下图所示页面。

导入配置

导入配置说明：

Smart 设备支持通过 HTTP 上传的方式将设备配置文件从当前正在操作的网管主机本地硬盘导入到设备中，还支持通过 FTP 方式将设备配置文件从外部的 FTP 服务器导入到设备中。

若选择“从管理主机导入”选项，则您可以通过点击【浏览】按钮在随后出来的打开文件对话框中选择相应的配置文件导入到设备中。

若选择“从 FTP 服务器导入”选项，则您需要正确填写存放配置文件的 FTP 服务器 IP 地址、登录帐号和密码，然后执行导入操作。

若选择FTP方式进行配置导入操作，在输入版本文件名称时请注意所输入的文件名需区分大小写，如果文件有后缀名则必须同时输入后缀名。

恢复出厂配置

本页面为您提供恢复设备出厂配置的操作。

数据管理

当您开启设备的“内容分析开关”后，设备会将网络中的用户上网信息记录到内置的硬盘中，同时设备提供对这些数据的备份、恢复及清除的操作。

备份审计数据

备份审计数据功能帮助您将设备中记录的用户上网信息备份设备外部的其它存在介质中，从而方便您对用户上网信息记录的存储和管理。

如需备份设备中的审计数据，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜数据管理＞→＜备份审计数据＞进入下图所示页面。

备份审计数据

配置项及其说明：

参数	说明
起始时间	选择需要进行备份的审计数据的起始时间
终止时间	选择需要进行备份的审计数据的终止时间

导入审计数据

Smart 设备允许您将备份到外部存储介质的审计数据重新导入到设备中。

如需进行审计数据导入操作，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜数据管理＞→＜导入审计数据＞进入下图所示页面。

导入审计数据

导入审计数据说明：

Smart 设备支持通过 HTTP 上传的方式将审计数据从当前正在操作的网管主机本地硬盘导入到设备中，还支持通过 FTP 方式将审计数据从外部的 FTP 服务器导入到设备中。

若选择“从管理主机导入”选项，则您可以通过点击【浏览】按钮在随后出来的打开文件对话框中选择相应的审计数据文件导入到设备中。

若选择“从 FTP 服务器导入”选项，则您需要正确填写存放审计数据文件的 FTP 服务器 IP 地址、登录帐号和密码，然后执行导入操作。

提示

若选择FTP方式进行审计数据导入操作，在输入版本文件名称时请注意所输入的文件名需区分大小写，如果文件有后缀名则必须同时输入后缀名。

清除审计数据

Smart 设备为您提供清除审计数据的功能，审计数据一旦被清除将无法恢复，请您慎重使用该功能。

如需清除设备中的审计数据，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜数据管理＞→＜清除审计数据＞进入下图所示页面。

清除审计数据

配置项及其说明：

配置参数	说明
用户	选择被清除数据的用户
数据类型	选择被清除数据的应用数据类型
起始时间	选择被清除数据的起始时间
终止时间	选择被清除数据的终止时间

提示

审计数据一旦被清除将无法恢复，请您慎重操作。

重启设备

如需对设备进行软件升级操作，请在配置界面左侧的主菜单栏中依次选择＜设备管理＞→＜数据管理＞→＜清除审计数据＞进入下图所示页面。

重启设备

提示

Smart设备重启大约需要1分钟时间，在此期间，请您耐心等候。