

Mydasd

PIX 日志管理系统操作手册

用 户 手 册

北京迪威达康科技

前言	3
第 1 章 系统简介.....	3
1.1 系统特点.....	3
1.2 运行环境.....	4
1.3 功能简介.....	4
1.4 系统原理.....	5
第 2 章 系统安装说明.....	6
第 3 章 MYDASD 日志管理系统使用说明	6
3.1 系统菜单与高级管理.....	6
3.1.1 系统	6
3.1.1.1 注销.....	8
3.1.1.2 权限管理.....	8
3.1.1.4 管理菜单.....	13
3.1.2 日志管理.....	16
3.1.2.1 浏览日志	16
3.1.2.2 模糊搜索日志	17
3.1.2.3 详细搜索日志	18
3.1.2.4 日志导出	20
3.1.2.5 日志清理	21
3.1.2.6 日志统计	21
3.1.2.7 历史日志统计	22
3.1.2.8 排名统计.....	23

前言

在互联网技术日益发达的今天，网络犯罪和不良信息的传播有不断上升的趋势。为了有效防范和监控网络犯罪，打击各种不良信息的网上传播，规范人们的网上行为，同时可以监控分析人们网络行为的趋势，为运营提供指导行的必要数据，所以有必要对通过网络的数据信息进行记录和分析。

Mydasd 可以与路由器、交换机、BAS 等网络设备共同组网，根据用户要求采集不同类型的网络流量信息，并通过聚合、分析与统计，为网络管理员提供用户行为审计、流量异常监控和网络部署优化的数据基础和决策依据。

Mydasd 是一种低成本、可扩展的网络日志信息审计与分析系统，能够与路由器、以太网交换机、BAS 设备等共同组网，完成对 NAT、FLOW、DIG 等多种网络日志的采集、统计与分析，可以追溯网络使用行为，监视异常活动，为合理的网络规划提供重要参考。

第 1 章 系统简介

1.1 系统特点

系统包括两部分：PIX日志采集服务程序，PIX日志WEB管理系统。PIX日志采集服务程序完成PIX日志的采集功能，PIX日志WEB管理系统负责用户管理、参数设置、日志查询等功能。

该系统具有如下特点：

➤ 系统稳定、安全性高

该系统的核心服务程序运行于Linux操作系统平台，能保证系统稳定高效的运行。

➤ 实时响应

实时采集PIX的日志信息，随时通过管理界面可以查询到。

➤ 容量大、速度快

配合硬件设备，系统能支持百万级的用户，并达到很快的响应速度。

➤ 跨平台、易移植

该系统的设计开发采用了标准的Radius协议和网络协议。该系统以Linux为运行平台设计，能够很容易地移植到Unix、FreeBSD。同时，该系统本身涉及到 linux 和Windows两种平台。

➤ 多层分布式结构

该系统采用多层分布式系统结构设计，支持并行操作，性能卓越。在不同的地域可以并行进行用户的管理，包括开户、查询等操作。该系统还支持将采集日志服务器放在不同的地域，但同时共享一个用户数据库。分布式系统结构对业务范围覆盖全国的ISP和大型企业特别实用。

➤ 支持标准协议，硬件适应性较高

支持标准的Syslog协议，IEEE 802.1x协议。只要硬件支持标准的Syslog协议/802.1x协议即可。

➤ 操作简便、功能完备

该系统的操作界面简单，一目了然，人机交互环境非常友好。

➤ 透明度高

管理员可实时查询客户的上网时间、地址转换信息，随时了解自己的帐号使用情况。

1.2 运行环境

1.2.1 硬件环境

PIX 日志采集服务器：中高端服务器配置，集采集服务器、数据库服务器于一身。根据用户需求，可选用以下四种配置方案中的一种：

- 1)高档微机一台
- 2)服务器一台
- 3)服务器两台+双机热备软件
- 4)服务器两台+双机热备软件+磁盘阵列柜

Web 服务器：中高端服务器配置，或高档 PC 机

防火墙： 可选设备，可用软防火墙+双网卡代替

管理微机： 一般计算机配置。

Hub,网线等。

1.2.2 软件环境

认证服务器： Linux 2.6 以上，Mysql 5.0 以上版本

Web 服务器:Win2K/NT+tomcat

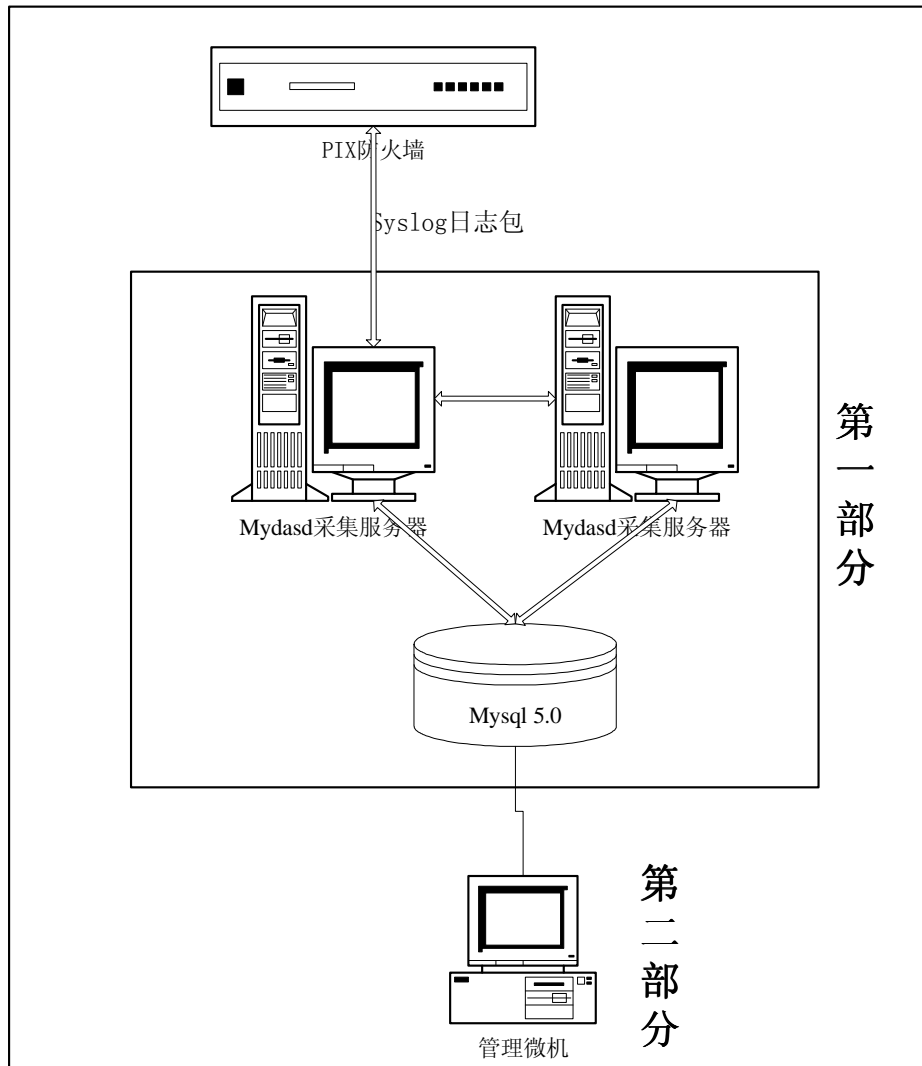
管理微机: windows+IE4.0 以上

1.3 功能简介

该系统从软件结构和硬件平台的角度都可以划分为二部分：

划分	软件	硬件
第一部分	PIX 日志采集服务程序	PIX 日志服务器
第二部分	PIX 日志管理系统	PIX 日志服务器

其结构简图如下：



(在上图中: PIX 代表 PIX 防火肋骨设备。Mydasd 采集服务器、管理微机、Mysql 5.0 数据库服务器可以分开, 也可以合三为一。)

各部分的基本功能为:

- 第一部分: PIX 采集服务器与 PIX 防火墙进行 syslog 协议交互, 采集 PIX 防火墙上的日志数据记录下来。
- 第二部分: 管理微机实现日志数据的查询、管理、下载等等功能。

1.4 系统原理

NAT 设备在网络上日益广泛的应用给安全审计带来了一些问题——NAT 转换屏蔽了内网 IP 地址, 造成用户访问外网的源 IP 地址丢失, 给定位和审计用户不法行为(如访问非法网站)带来了困难。Mydasd 旁路方式记录路由器、BAS 等设备记录 NAT 转换前的源 IP 地址、源端口, 经过 NAT 转换后的源 IP 地址、源端口, 以及所访问的目的 IP、目的端口、协议号、开始时间和结束时间等关键信息。通过 XLog 对 NAT 日志的采集、聚合和记录, 管理员就可方便地跟踪用户通过 NAT 设备访问网络的详细情况, 从而轻易的解决这类安全审

计问题。

第 2 章 系统安装说明

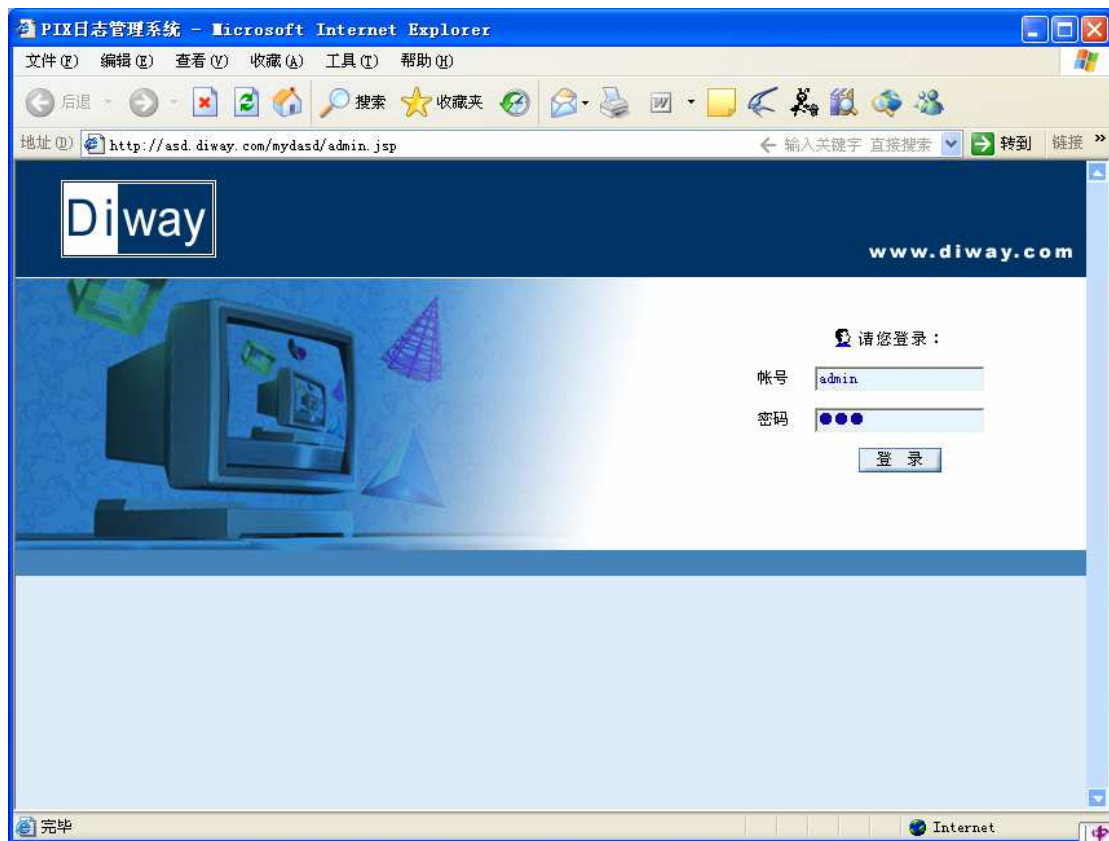
详细操作步骤请参见《Mydasd 1.5 日志服务器安装说明》。

第 3 章 Mydasd 日志管理系统使用说明

3.1 系统菜单与高级管理

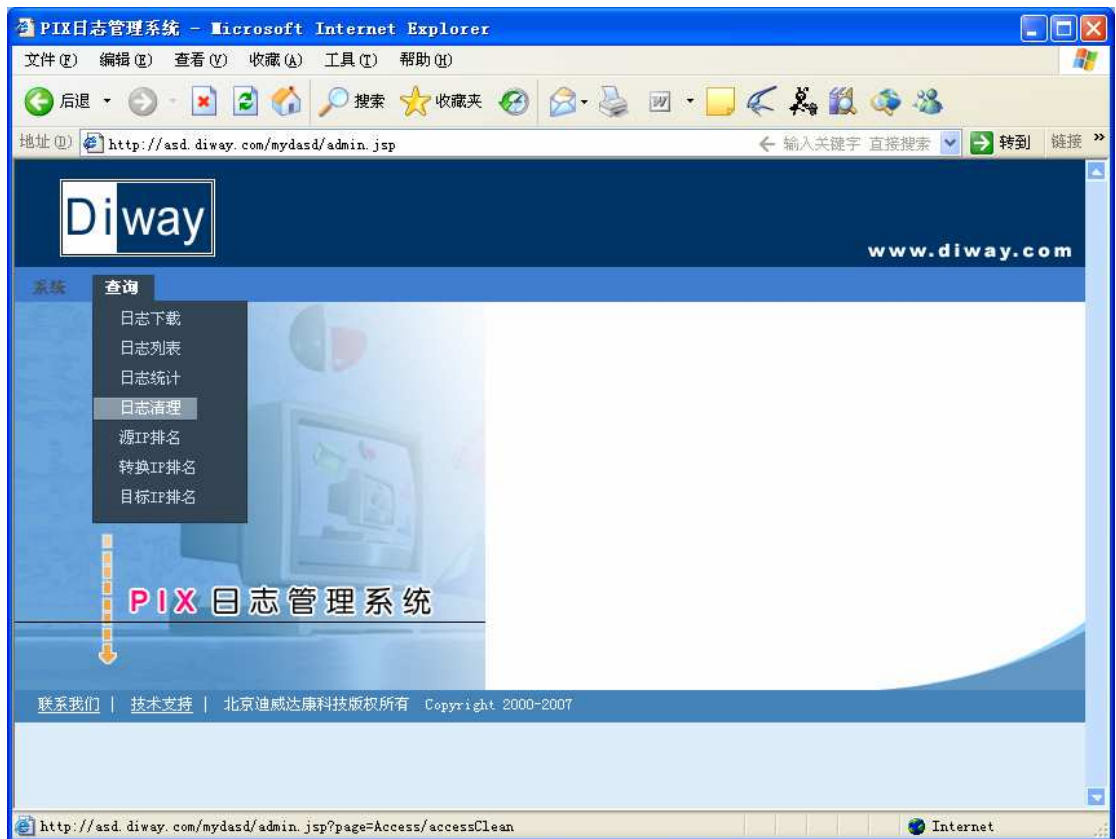
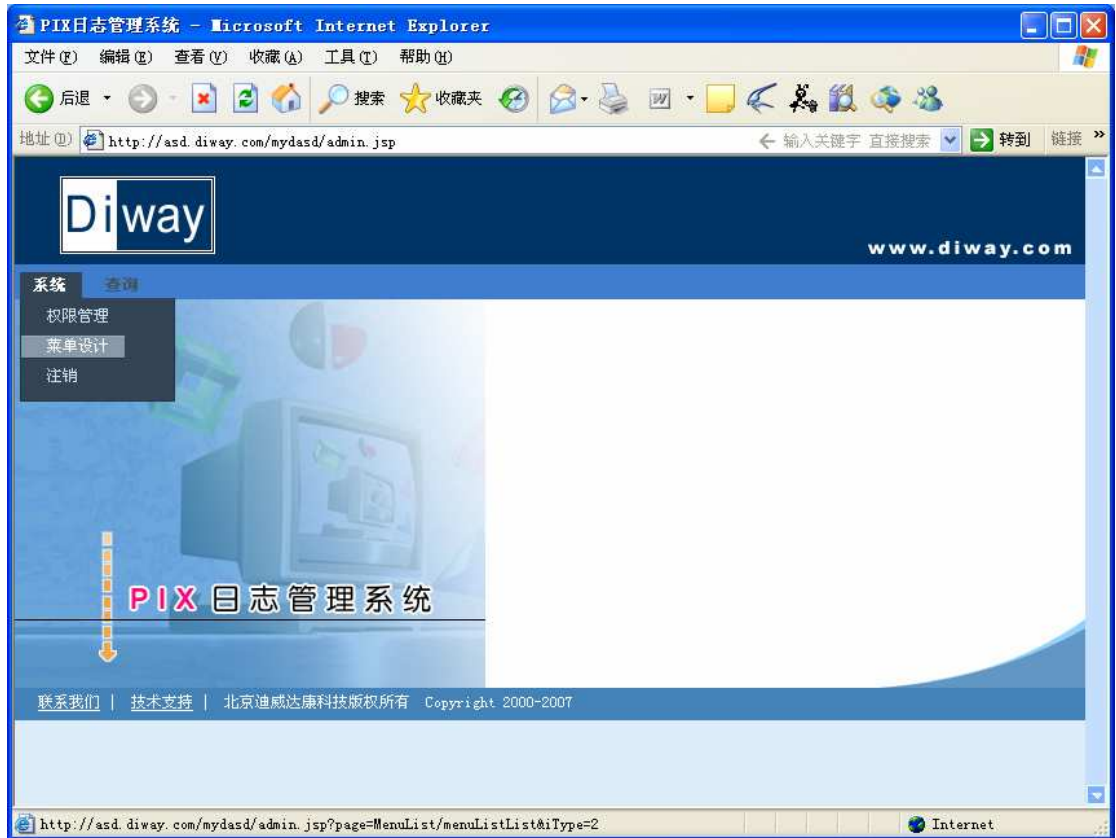
3.1.1 系统

登录本系统时，用户需要输入系统提供的账号和密码后，方可使用本系统。



(图 3.1.1)

【注意事项】：无

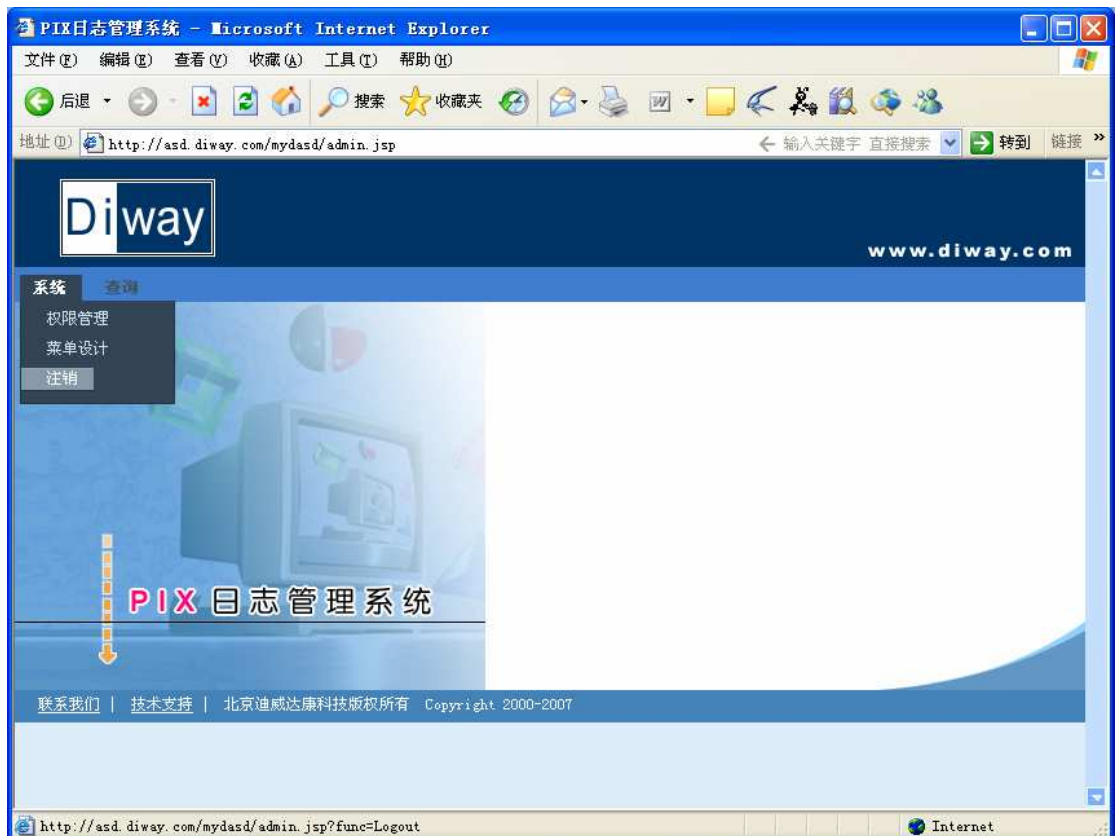


3.1.1.1 注销

【功能】: 退出 Mydasd 日志管理系统。

【概念】: 无

【操作说明】: 单击“注销”，则关闭该 Mydasd 日志管理系统。



【注意事项】: 无

3.1.1.2 权限管理

【功能】: 可以对系统操作的权限进行管理。

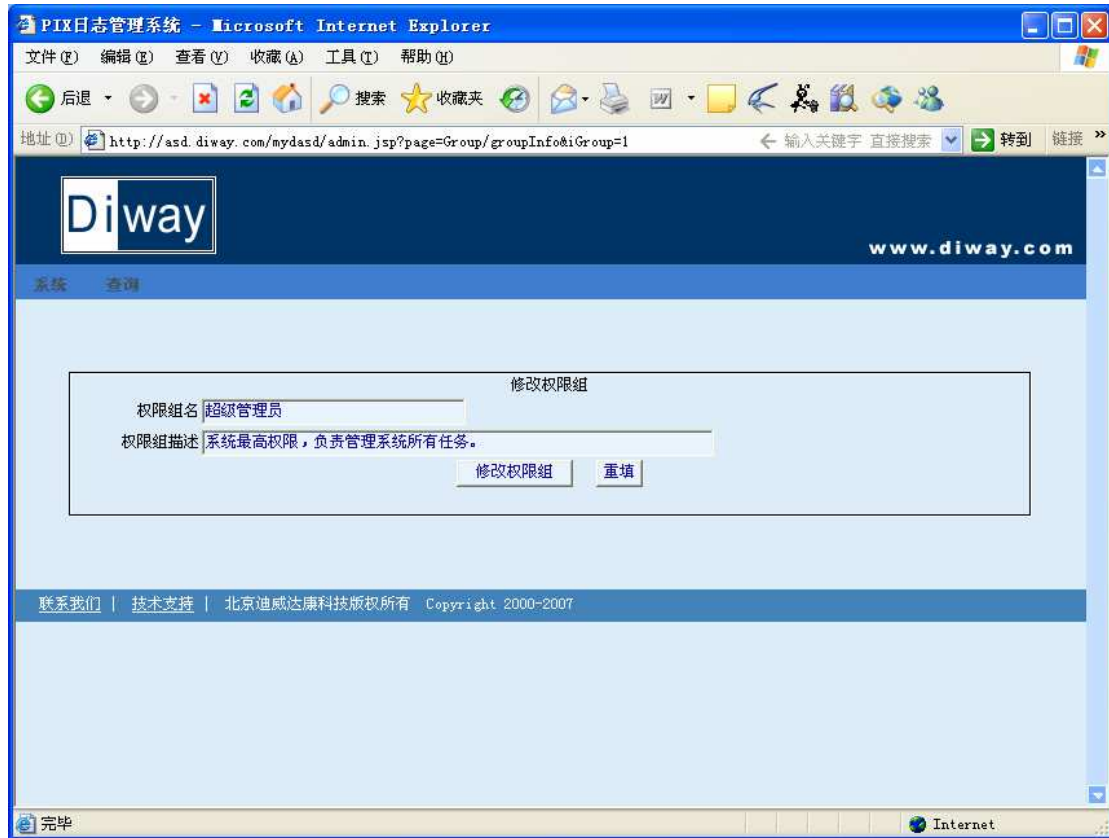
【概念】: 工作组：可以将类型相同的用户归并到一个工作组，然后对工作组设置相应的权限。

【操作说明】:



(图 3.1.1.1)

1. 单击“工作组名称”中的超链接，可以更改该工作组的名称和权限描述，该权限描述将出现在工作组说明中。如果需要更改，可在对应的方框中直接更改，更改完毕后，点《修改权限组》，则退回到主界面。如果需要全部更改，可选择《重填》按钮，则将方框中文字完全清理。



(图 3.1.1.2)

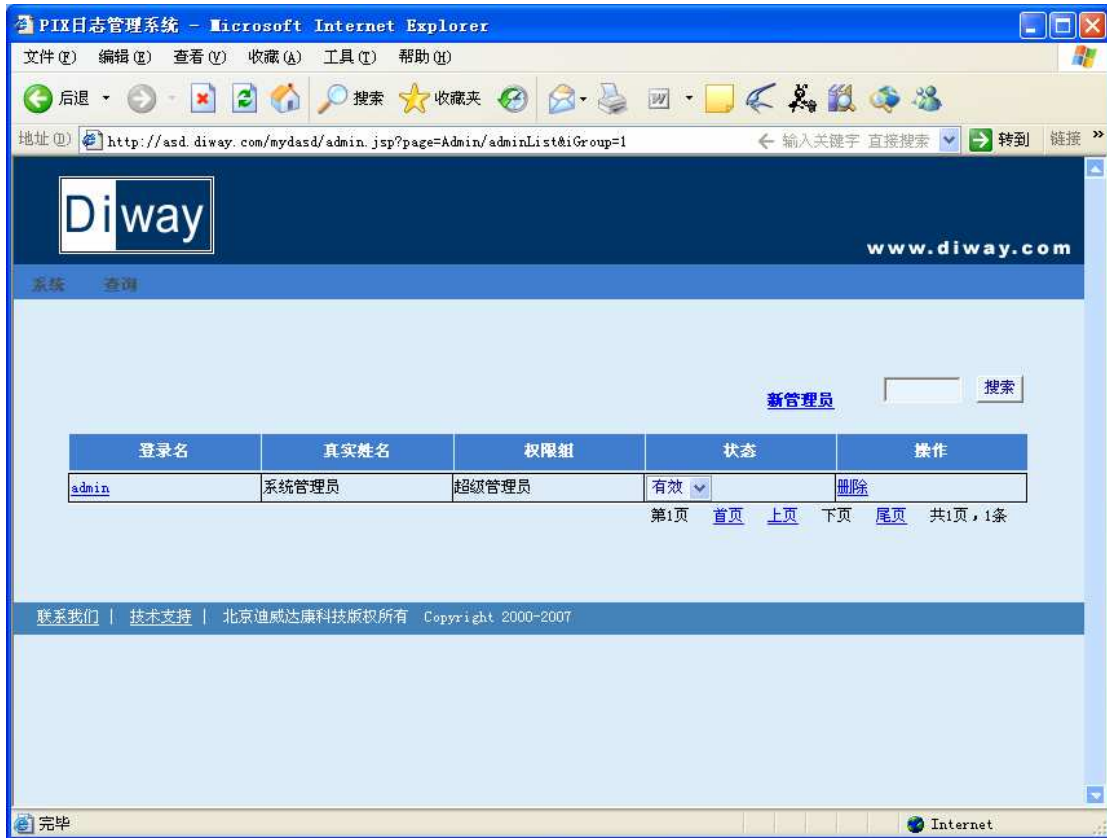
- 工作组说明：说明本行工作组的职能。所有属于同一个工作组的操作员具有相同的权限
- 操作权限：单击“修改”中的超链接，可以修改本工作组的权限（如图 3.1.1.3）。
- 按钮说明：需要全部更新权限时，点击《重填》按钮，则会清除所有选项。然后在要选择的权限前边方框，打上“√”，选择完毕，点击《更新》即可。如果需要全部选择，则在全部选择文字前对应方框中打“√”，就会选中所有权限。



(如图 3.1.1.3)

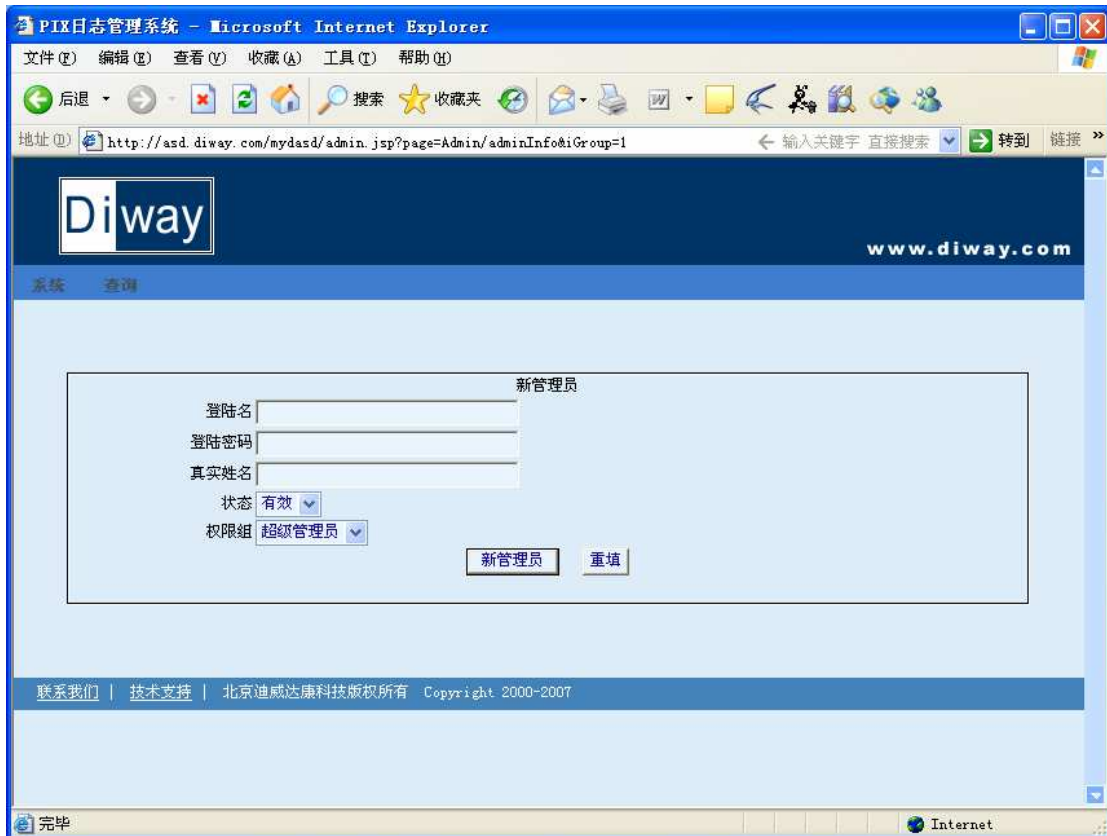
4. 成员：显示该工作组包括的所有成员名单。

4.1 如下图所示，在这里仍然能够继续添加隶属于该组的新用户。



(图 3.1.1.4)

4.2 新管理员：可以继续添加该组的新成员。



(图 3.1.1.5)

选择“权限组”时，可对应身份来选择用户的工作组。在上图中，已经有两个工作组：系统管理员和一般操作员，用户可以自由选择。

例如：“登陆名”，文本框填写 hk.最好是和别人的账号是不重复的；

“登陆密码”：最好是选择和别人的密码不重复的。

“真实姓名”，文本框填写 cathy。

“状态”可根据实际选择“有效”或者“无效”。

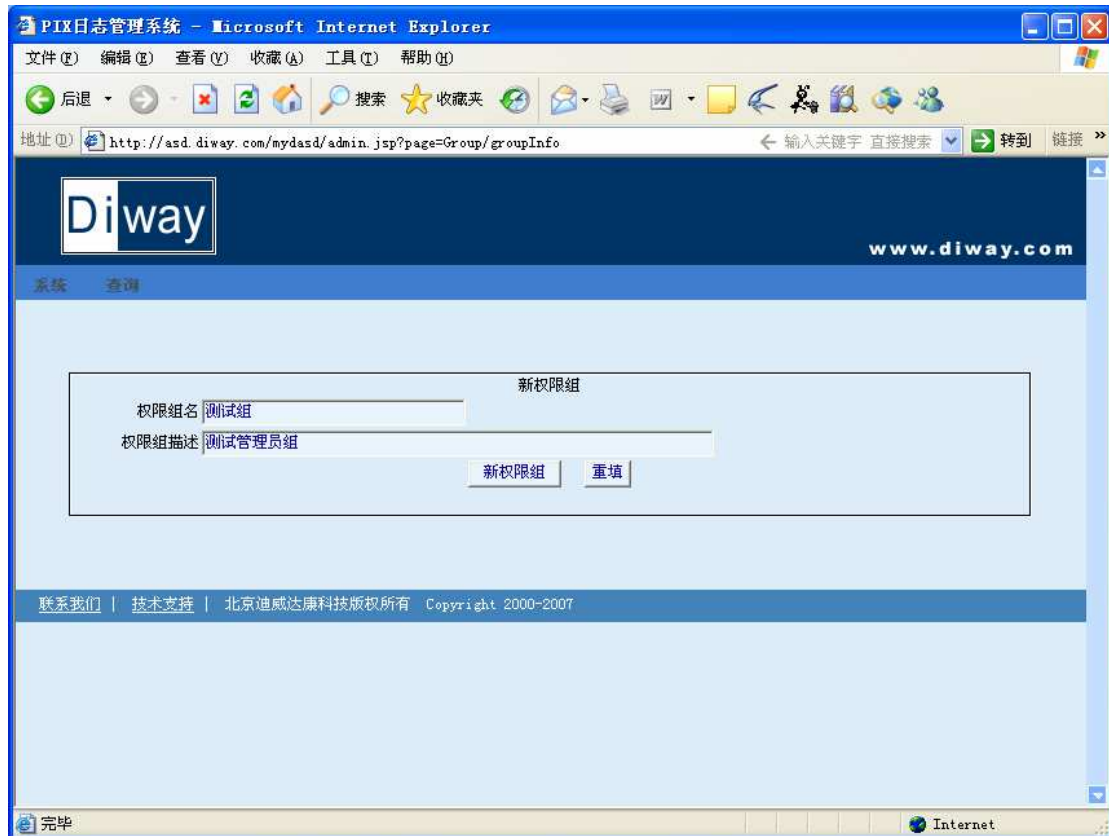
填写完毕后，按《新管理员》按钮，则新管理员添加成功。如果需要重新填写，则按《重填》按钮，则恢复到全空状态。

4.3 删除：对该行管理员进行删除。如果要删除某个管理员，直接点击后边对应的“删除”即可。

4.4 搜索：如果有多名管理员时，可在搜索对应的方框中，输入要搜索的管理员名称，然后点击《搜索》按钮，则对应的选项就出现在下方列表中。

5. 删除：同 4.4。对该行工作组进行删除

6. 新权限组：用户可以自定义一个新的工作组类别。操作类似于工作组超级连接。



(图 3.1.1.6)

如果有多页工作组，可通过点击首页、下页、上页、尾页等超级连接来查看。

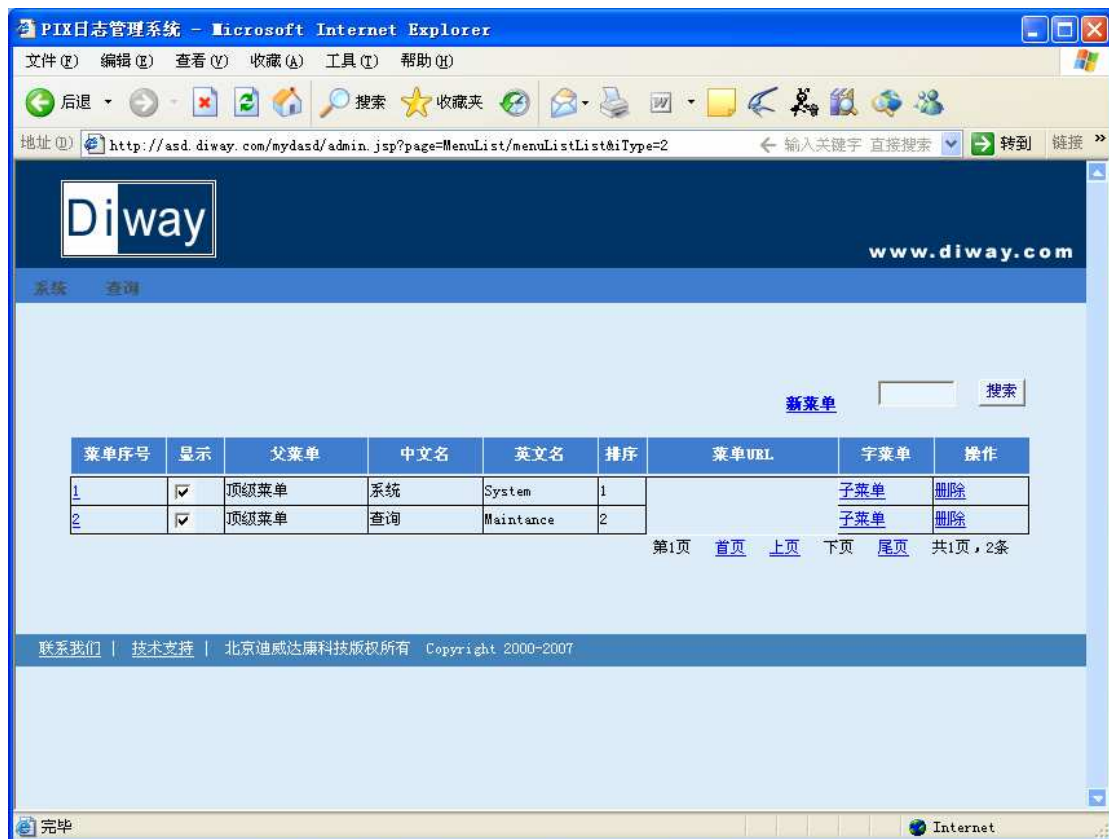
3.1.1.4 管理菜单

【功能】：可以将系统功能灵活组合到菜单上。可根据用户的意愿自行设计菜单。

【概念】：无

【操作说明】

从“系统”中点击“管理菜单项”，进入如下页面。



(图 3.1.1.4.1)

1. 单击“菜单序号”，可以对该菜单进行修改。

单击“子菜单”对应的“查看”链接，可以对该子菜单进行删除、修改、增加，

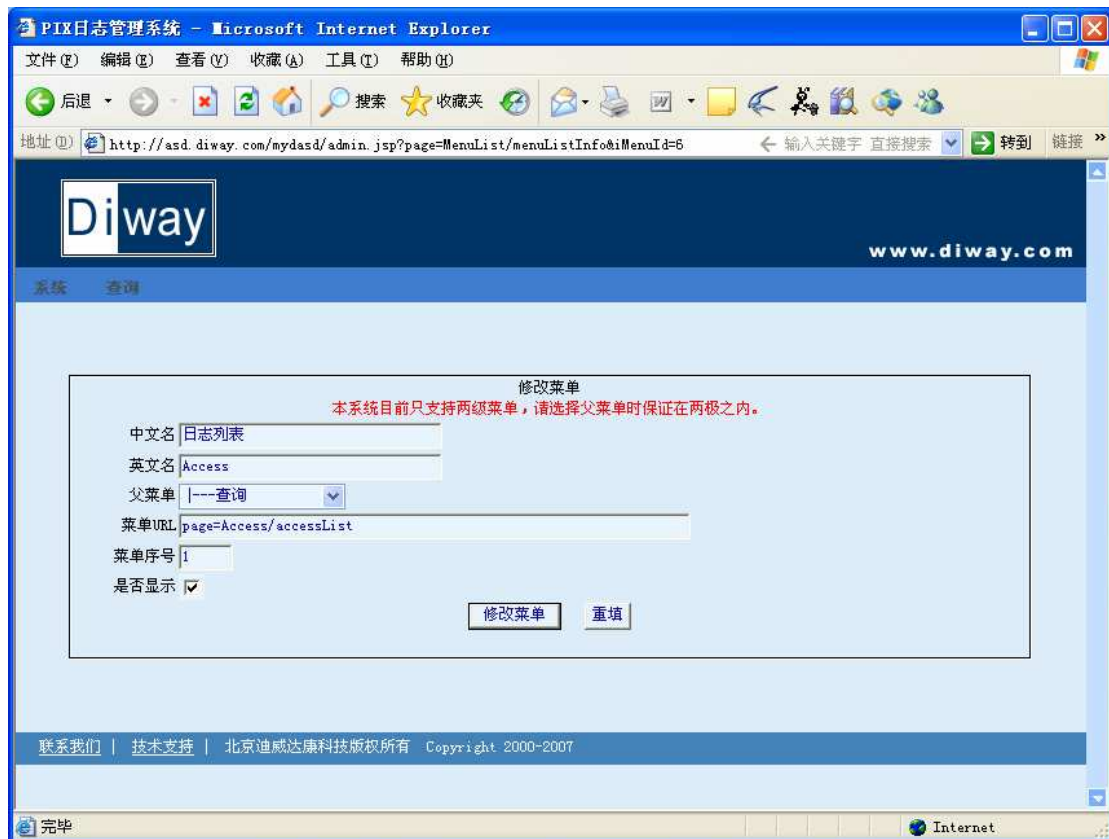
单击“删除”可以对该级菜单和子菜单进行全部删除。

例如：对于菜单项“系统”，属于一级菜单，处于本系统的第一项，所以“菜单序号”显示为 10，点击“子菜单”，则会把属于“系统”的下级菜单全部显示出来，如图 3.1.1.4.2



(图 3.1.1.4.2)

2. **修改:** 单击“序号”对应的超级连接,可弹出一个新的窗口(如下图 3.1.1.4.3),在新窗口中,可以重新定义该菜单的“中文名称”、“英文名称”,并可以对父菜单进行选择,“菜单项 URL”对应的文本框中输入相应的内容,同时更改菜单的序号。



(图 3.1.1.4.3)

单击“修改菜单”，可以对菜单修改进行保存。其他菜单修改类似。

新增： 如果要增加新菜单，则点击“新菜单”超级连接，则弹出类似图 3.1.1.4.3 的窗口，在窗口中输入相应内容后，点《新菜单》按钮即可。

删除： 如果要删除菜单时，可直接在列表中，选择要删除的项，然后点击后边对应的“删除”超级连接便可直接删除。

子菜单操作类似。

如果有多页菜单，可通过点击首页、下页、上页、尾页等超级连接来查看，一下皆同。

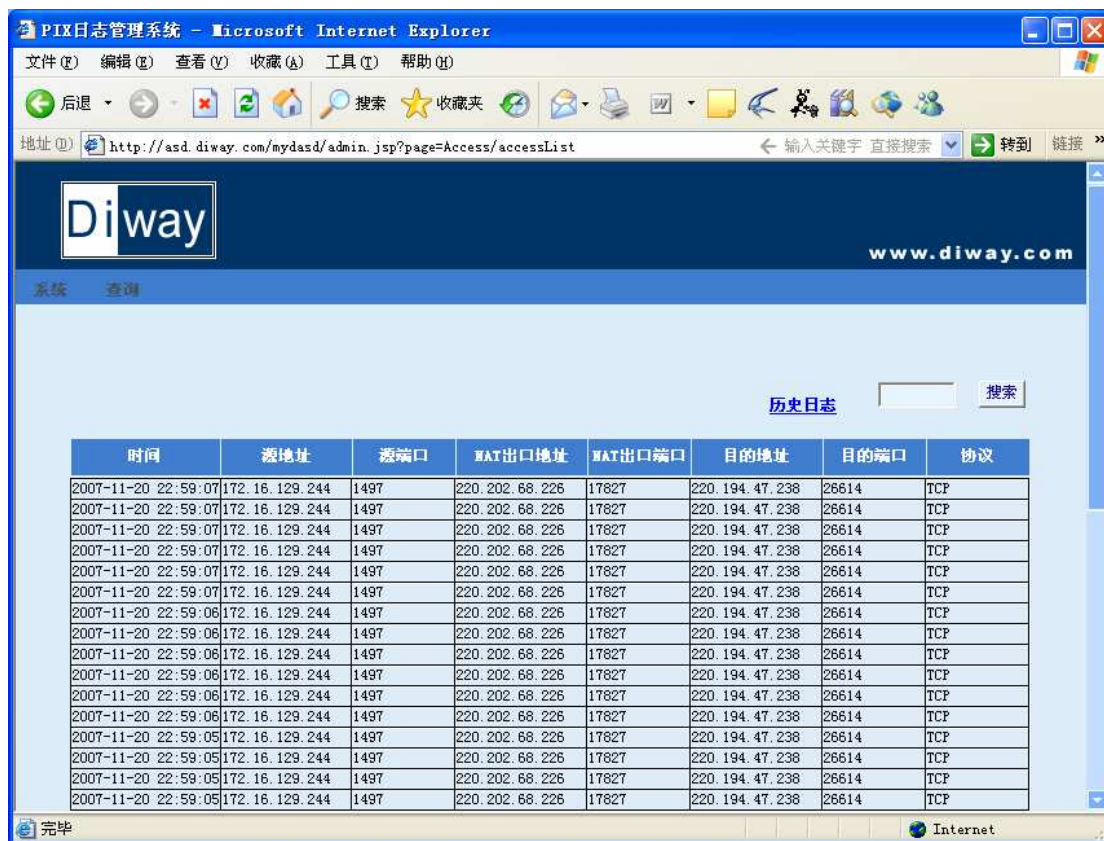
【注意事项】： 无

3.1.2 日志管理

3.1.2.1 浏览日志

【功能】 对各种日志进行总体查询，也可以对日志进行搜索。

【操作说明】 从“日志”中选择“日志列表”，出现一个操作日志记录列表。如下图

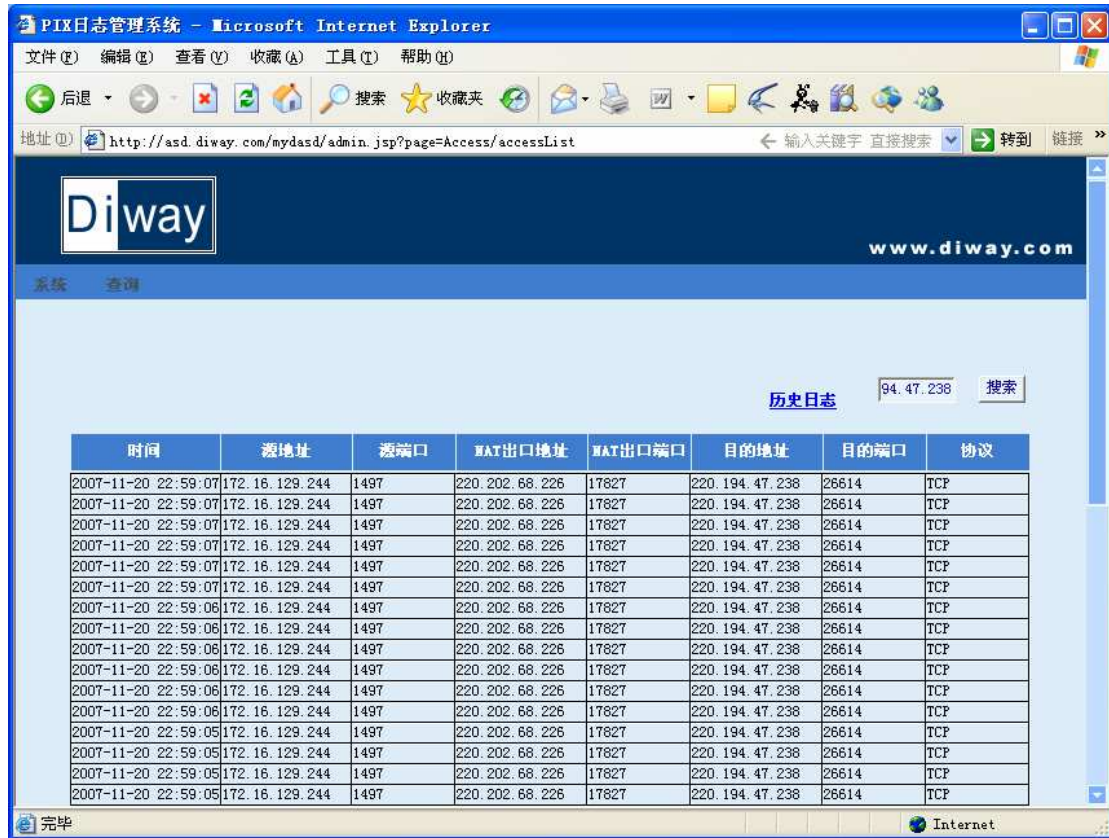


在该列表中，可对所有操作人员的工作情况记录进行查询。

3.1.2.2 模糊搜索日志

【功能】对各种日志进行总体查询，也可以对日志进行搜索。

【操作说明】在日志列表页面输入 IP 地址或者端口或者时间，则自动列出当前的符合条件的数据。如下图

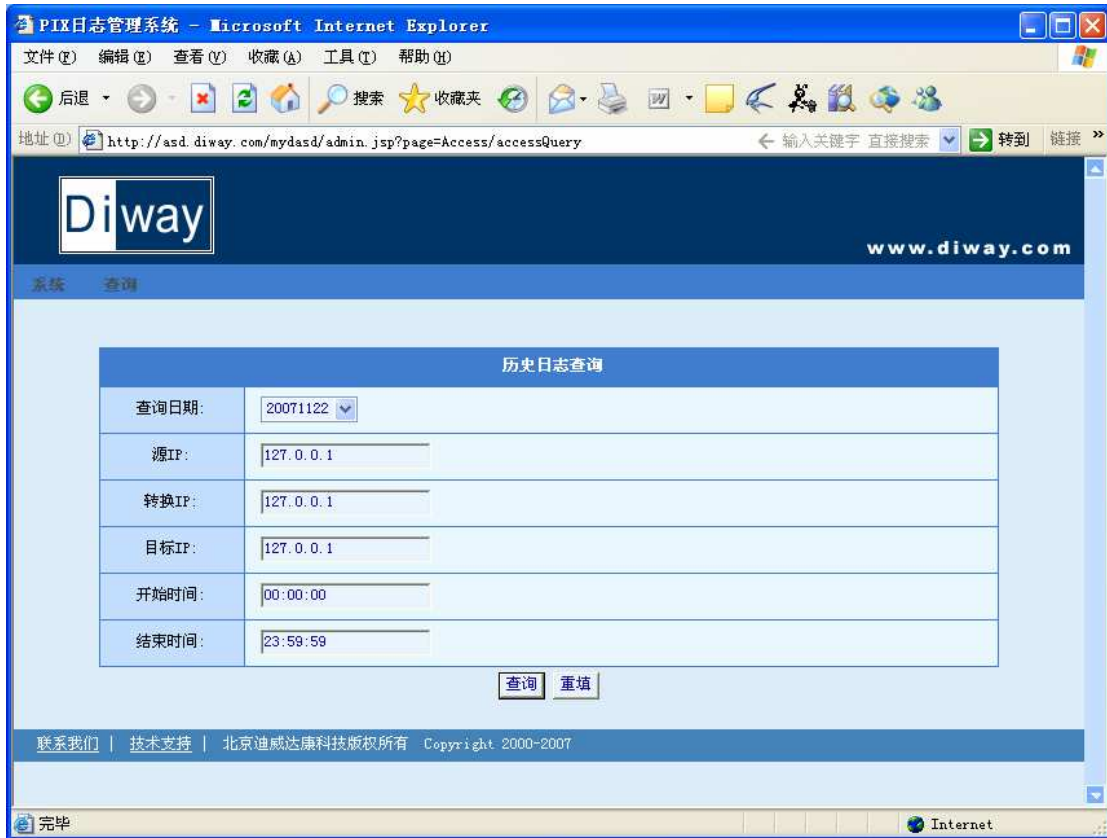


在该列表中，可对所有操作人员的工作情况记录进行查询。

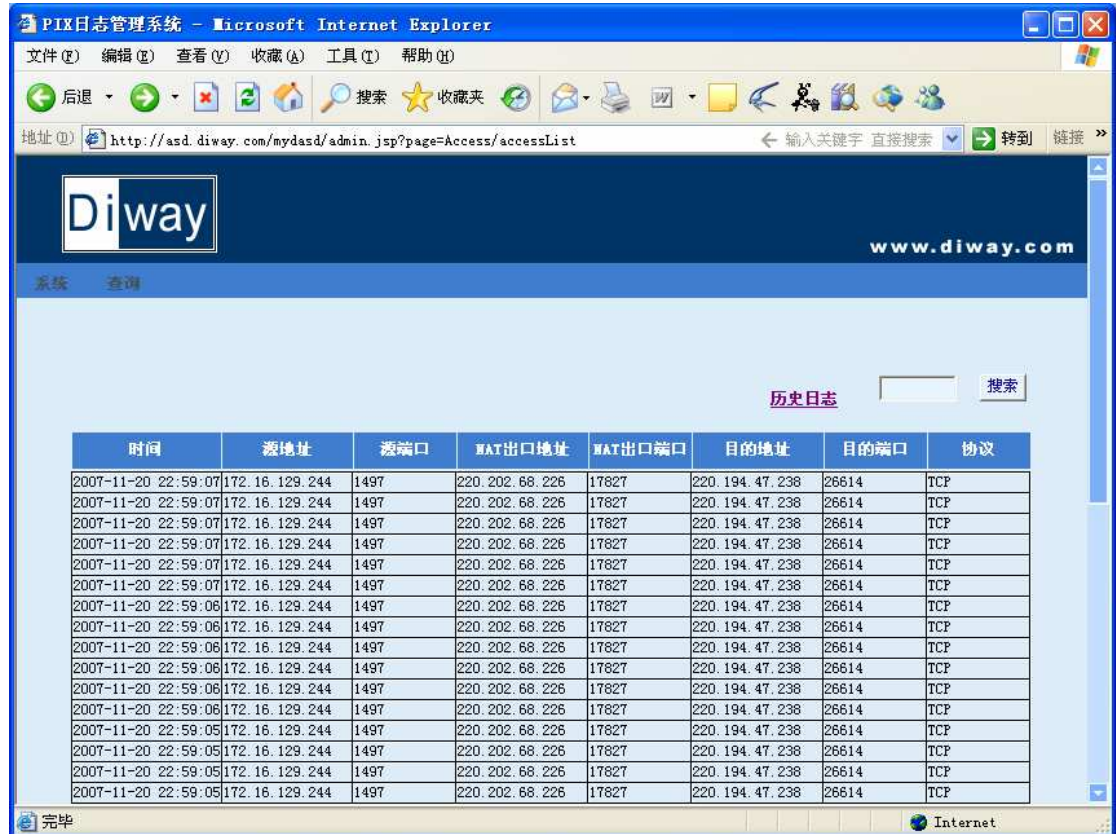
3.1.2.3 详细搜索日志

【功能】对各种日志进行总体查询，也可以对日志进行搜索。

【操作说明】点日志列表页面，点击“历史访问”，则进入高级查询界面。如下图



在该界面上，可以按照日期、时间区段、IP 地址进行综合查询，结果如下图：



3.1.2.4 日志导出

【功能】将日志明细以文本方式保存到本地。

【操作说明】从“查询”中选择“日志下载”，出现一个日期选择表，



选择要保存的明细日期，点击《查询》按钮，出现一个询问对话框，如图：



点击《保存》按钮，然后选择要保存的盘符，边可将该明细保存到硬盘上。

3.1.2.5 日志清理

【功能】将日志明细从数据库中删除。

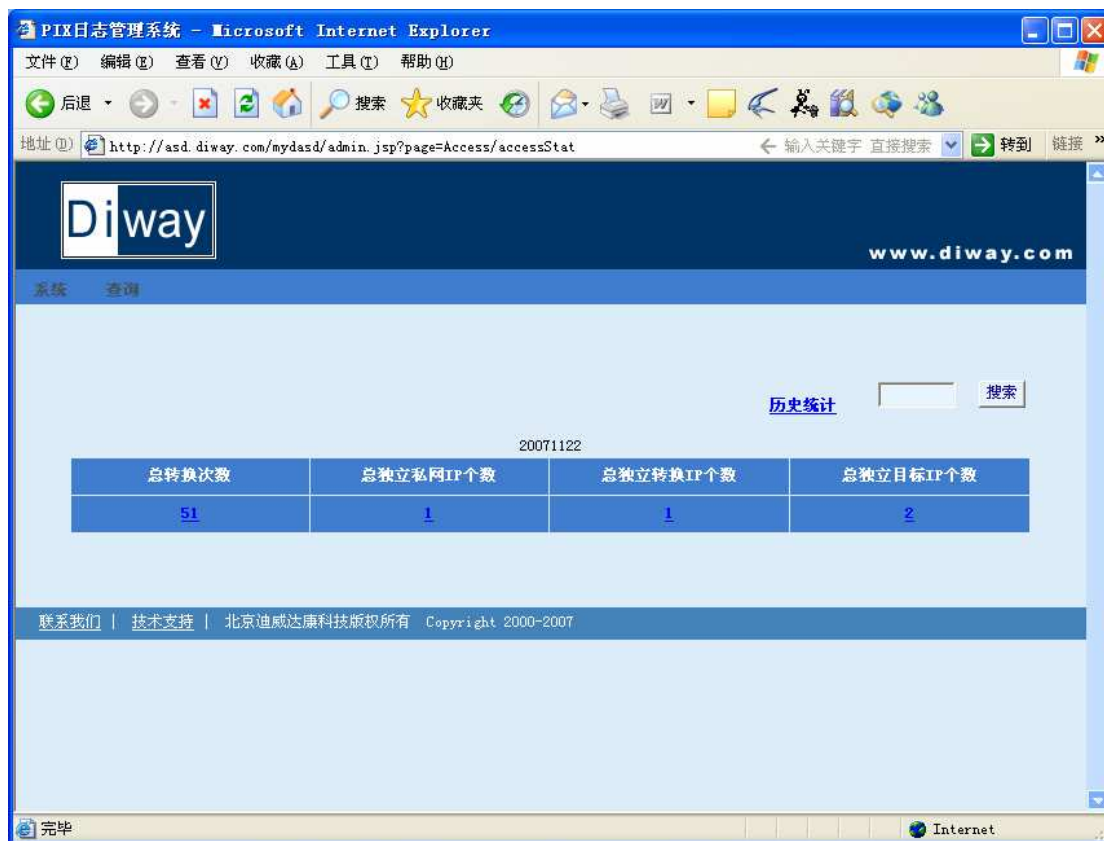
【操作说明】从“查询”中选择“日志清理”，出现一个日期选择表，



3.1.2.6 日志统计

【功能】将日志明细从数据库进行统计，显示每天的记录数、源 IP 个数、转换 IP 个数、目标 IP 个数。

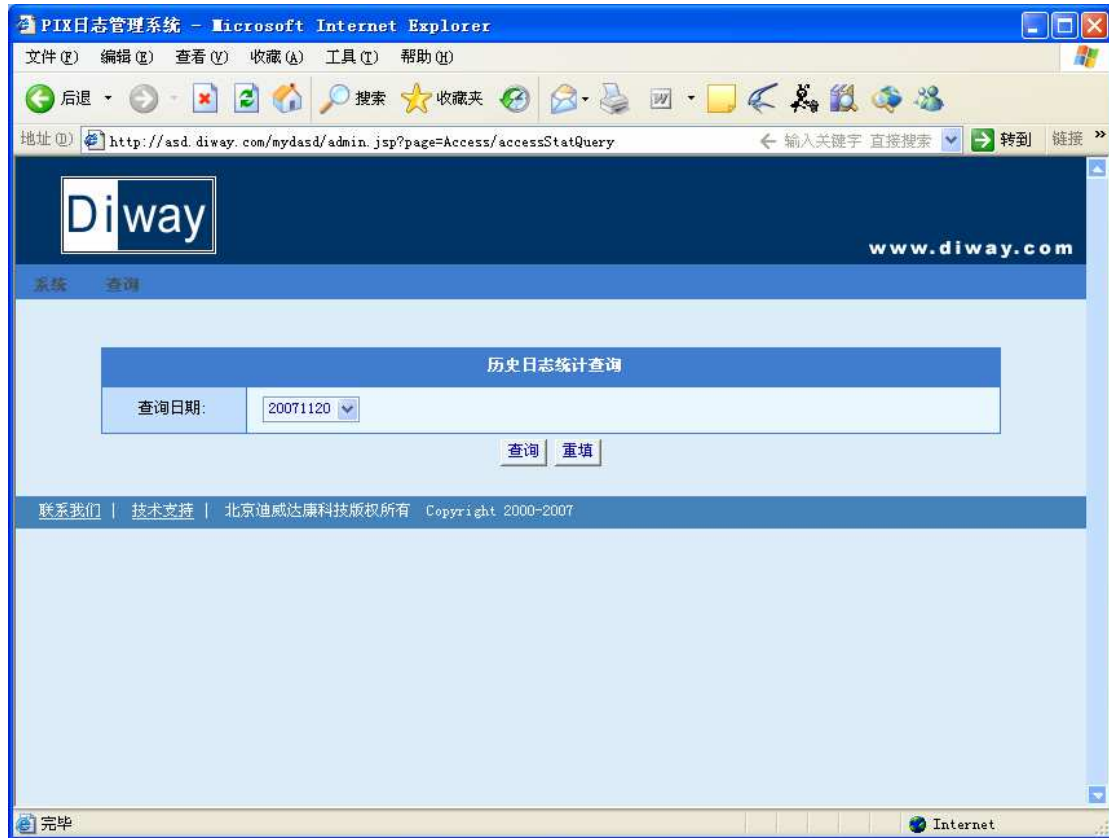
【操作说明】从“查询”中选择“日志统计”，出现一个日期选择表，



3.1.2.7 历史日志统计

【功能】将日志明细从数据库进行统计，显示每天的记录数、源 IP 个数、转换 IP 个数、目标 IP 个数。

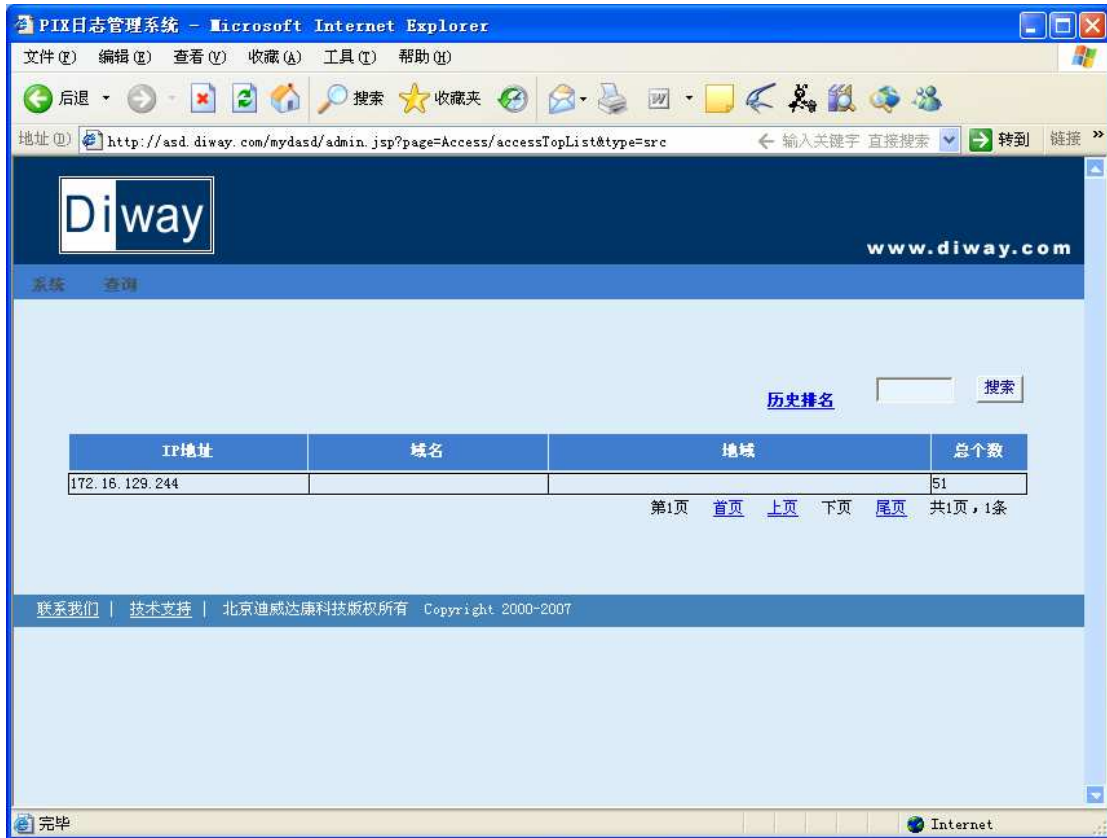
【操作说明】从“日志统计”的列表界面选择“历史统计”，出现一个日期选择表，可以选择对某一天进行统计显示。



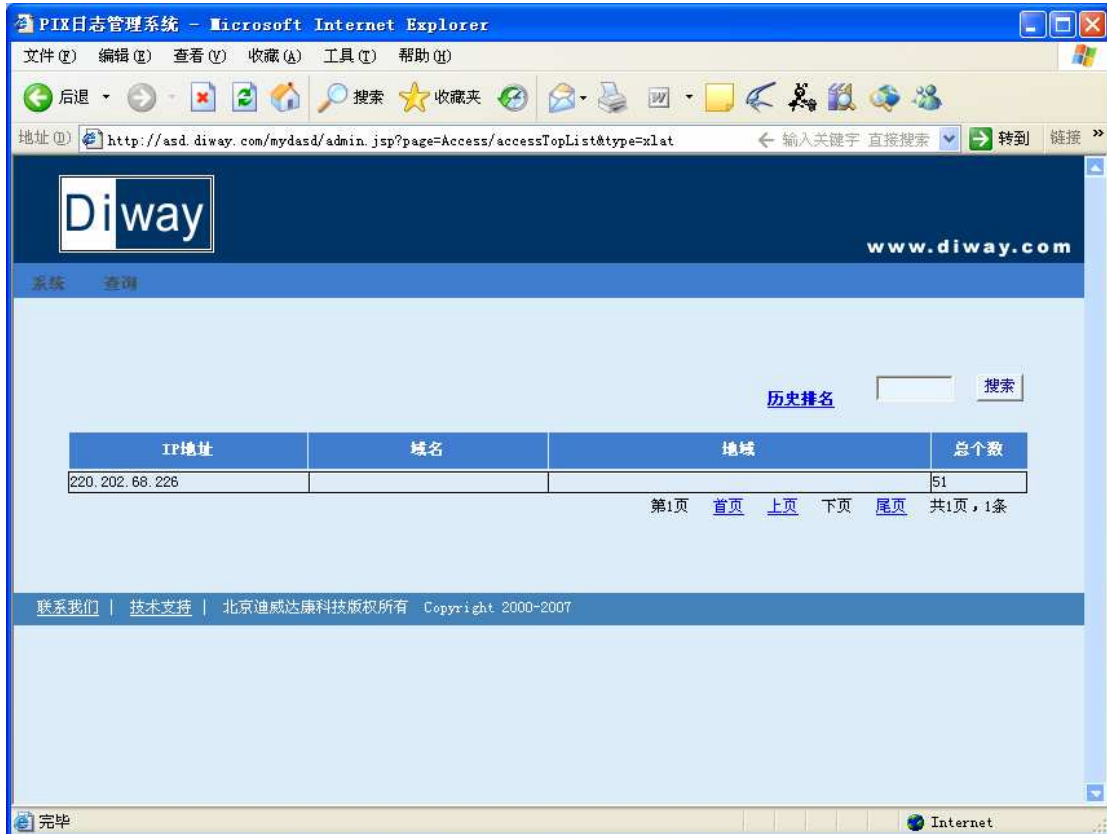
3.1.2.8 排名统计

【功能】 将日志明细从数据库进行排名统计，可以按照源 IP 个数、转换 IP 个数、目标 IP 个数进行排名显示。

【操作说明】 从“查询”的列表界面选择“源 IP 排名”、“目的 IP 排名”、“转换 IP 排名”，出现一个日期选择表，可以选择对某一天进行统计显示。



上图为按照源 IP 进行排名。



上图为按照转换后的 NAT 地址进行排名。

以下图按照目标 IP 进行排名显示，将显示目标 IP 的地域信息：

