发明名称
日志记录方法及其记录系统

摘要
本发明提供一种日志记录方法及其系统，该方法包括步骤：生成 IP 日志，该 IP 日志记录的内容至少包括 IP 地址、进行操作的内容信息；在所述 IP 日志中查找所述 IP 地址；将查找到的所述 IP 地址替换为用户信息，以获得 ID 日志。通过本发明，将 IP 日志转换为 ID 日志，这样，通过 ID 日志可直接获得使用计算机的真实用户，这些日志信息可向系统管理员提供危害安全的非常有用的相关信息，对公司、企业的秘密和网络安全非常有利。
1. 一种日志记录方法，其特征在于，该方法包括步骤:

   生成IP日志，该IP日志记录的内容至少包括IP地址、所进行操作的内容信息；

   在所述IP日志中查找所述IP地址；

   将查找到的所述IP地址替换为用户信息，以获得ID日志。

2. 根据权利要求1所述的方法，其特征在于，所述IP日志记录的内容还包括使用所述IP地址的时间信息。

3. 根据权利要求1或2所述的方法，其特征在于，根据IP地址和用户信息的对应关系将查找到的所述IP地址替换为用户信息；或者根据IP地址、使用该IP地址的时间和用户信息的对应关系将查找到的所述IP地址替换为用户信息。

4. 根据权利要求1或2所述的方法，其特征在于，所述在IP日志中查找所述IP地址，包括:

   判断所述IP日志记录的内容中是否有至少三个点字符；

   若判断的结果为有，则进一步判断所述至少三个点字符中的相邻两点字符之间的信息是否为数字；

   若判断的结果为是，则确定与所述至少三个点字符相邻的信息以及所述点字符构成所述IP地址。

5. 根据权利要求4所述的方法，其特征在于，所述数字的取值范围为1至255。

6. 根据权利要求1或2所述的方法，其特征在于，所述用户信息为用户标识信息、用户真实姓名、用户组、部门或职位。

7. 根据权利要求1或2所述的方法，其特征在于，所述IP日志和ID日志的格式为日志文件或单条的日志记录。

8. 一种日志记录系统，其特征在于，至少包括:

   IP日志生成单元，用于生成IP日志，该IP日志记录的内容至少包括IP地
地址，所进行操作的内容信息；

查找单元，与所述IP日志生成单元连接，接收所述IP日志生成单元传送的所述IP日志，在所述IP日志中查找所述IP地址；

ID日志生成单元，与所述查找单元连接，接收所述查找单元查找到的所述IP地址的信息和IP日志，并将查找到的所述IP地址替换为用户信息，以获得ID日志。

9. 根据权利要求8所述的系统，其特征在于，所述IP日志记录的内容还包括使用所述IP地址的时间信息。

10. 根据权利要求8或9所述的系统，其特征在于，所述ID日志生成单元根据IP地址和用户信息的对应关系将查找到的所述IP地址替换为用户信息；或者根据IP地址、使用该IP地址的时间和用户信息的对应关系将查找到的所述IP地址替换为用户信息。

11. 根据权利要求8或9所述的系统，其特征在于，所述查找单元至少包括：接收单元，与所述IP日志生成单元连接，接收所述IP日志生成单元传送的所述IP日志；

判断单元，与所述接收单元连接，用于判断所述IP日志中是否有至少三个点字符；若判断的结果为有，则进一步判断所述至少三个点字符中的相邻两点字符之间的信息是否为数字；若判断的结果为是，则确定与所述至少三个点字符相邻的信息以及所述点字符构成所述IP地址，并将该IP地址和所述IP日志传送至ID日志生成单元。

12. 根据权利要求11所述的系统，其特征在于，所述数字的取值范围为1至255。

13. 根据权利要求8或9所述的系统，其特征在于，该系统还包括存储单元，与所述ID日志生成单元连接，用于存储所述生成的所述ID日志。

14. 根据权利要求8或9所述的方法，其特征在于，所述用户信息为用户标识信息、用户真实姓名、用户组、部门或职位。
说明 书

日志记录方法及其记录系统

技术领域

本发明涉及日志记录方法，特别涉及一种日志记录方法及其记录系统。

背景技术

计算机系统为了维护自身系统资源的运行状况，一般都会有相应的日志记录系统记录有关日常事件或者误操作警报的日期及时余数等信息。这些日志信息可向系统管理员提供危害安全的非常有用的相关信息，因此，日志对计算机犯罪调查非常有用。

日志（Log）是按照时间有序的、可能含有IP地址的网络行为的记录。日志文件记录的是服务器、工作站、防火墙和应用软件等IT资源相关行为记录必要的、有价值的信息。每个日志文件由日志记录组成，每条日志记录描述了一次单独的系统事件，通常日志记录包括记录用户登录时间、登录地点、进行什么操作等内容。

例如，如图1所示的有关防火墙的日志文件，由日志记录1/2/3/4……等组成，如其中的一个日志记录为"Cisco—PIX—506# 192.168.1.15 2007.6.15:15:31 access 192.168.1.201……”。

另外，以计算机系统为例进行说明。如某公司或企业为了便于管理网络，有时针对所有员工设定不同的权限，如表1所示。

表1

<table>
<thead>
<tr>
<th>ID</th>
<th>姓名</th>
<th>部门</th>
<th>职位</th>
<th>访问内部服务器权限</th>
<th>访问Internet权限</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wang</td>
<td>小王</td>
<td>人事处</td>
<td>经理</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>Gao</td>
<td>小高</td>
<td>人事处</td>
<td>普通员工</td>
<td>有</td>
<td>无</td>
</tr>
<tr>
<td>Li</td>
<td>小李</td>
<td>财务处</td>
<td>普通员工</td>
<td>无</td>
<td>无</td>
</tr>
</tbody>
</table>
为达到上述管理效果，需要配置相应策略。在现有技术中，对访问权限的控制是基于IP来实现的，即分给每个员工不同的IP地址，然后针对不同的IP地址配置相应的策略。

首先，如表2所示为对不同员工分配不同的IP地址。

<table>
<thead>
<tr>
<th>姓名</th>
<th>计算机</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>小王</td>
<td>PC201</td>
<td>192.168.1.8</td>
</tr>
<tr>
<td>小高</td>
<td>PC203</td>
<td>192.168.1.9</td>
</tr>
<tr>
<td>小李</td>
<td>PC205</td>
<td>192.168.1.17</td>
</tr>
</tbody>
</table>

其次，配置每个IP地址的权限，如表3所示。

<table>
<thead>
<tr>
<th>IP</th>
<th>访问内部服务器权限</th>
<th>访问Internet权限</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.8</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>192.168.1.9</td>
<td>有</td>
<td>无</td>
</tr>
<tr>
<td>192.168.1.17</td>
<td>无</td>
<td>无</td>
</tr>
</tbody>
</table>

由上述可知，现有技术中通过上述设置，达到规范管理网络的目的。

同样，对于上述计算机系统也可用日志文件记录用户登录时间、登录地点、进行什么操作等内容，从而在一定程度上起到监督、查询和安全审计作用。如图2所示的计算机系统，如Windows、Unix、Linux系统，可生成的日志文件。

这样，日志文件、日志记录在一定程度上对系统监控、查询、报表和安全审计起着重要的作用。但是，由于现有技术中的安全策略是基于IP地址的，因此，目前的日志记录是基于IP地址的日志记录，查看日志记录时一般只能查看到某个IP地址相应的操作内容。若出现某个用户使用他人的计算机进行操作时，则无法记录真正的使用者。如小高想上网或访问服务器时，那么小
高通过使用小王的计算机来达到目的，这样在日志文件中记录的内容仍然是，
例如 “192.168.1.8 2007.7.21: 11:30:05 浏览网页或访问服务器” ，这
样，通过网络日志还是找不到对应的真实的用户。例如，小高想查会一些财
务报表，这样小高通过使用小李的计算机来达到目的，同样在日志文件中查
不到真实的使用者，因此，这对公司或企业的秘密和网络安全非常不利。

发明内容

鉴于现有技术中存在的上述缺陷，本发明实施例提供一种日志记录方法
及其记录系统。通过本发明实施例，可通过日志记录直接查看计算机的真实
使用者，对公司、企业的秘密和网络安全非常有利。此外，基于身份标识（ID:
Identification）的日志还可提供有价值的信息。

本发明实施例提供一种日志记录方法，该方法包括步骤：

生成IP日志，该IP日志记录的内容至少包括IP地址、所进行操作的内容
信息；在所述IP日志中查找所述IP地址，将查找到的所述IP地址替换为用户
信息，以获得ID日志。

本发明实施例还提供一种日志记录系统，至少包括：

IP日志生成单元，用于生成IP日志，该IP日志记录的内容至少包括IP地
址、所进行操作的内容信息；

查找单元，与所述IP日志生成单元连接，接收所述IP日志生成单元传送
的所述IP日志，在所述IP日志中查找所述IP地址；

ID日志生成单元，与所述查找单元连接，接收所述查找单元查找到的所
述IP地址的信息和IP日志，并将查找到的所述IP地址替换为用户信息，以获
得ID日志。

本发明实施例的有益效果在于，将IP日志转换为基于ID的ID日志，这样，
通过ID日志可直接获得使用计算机的真实用户，这些日志信息可向系统管理
员提供危害安全的非常有用的相关信息，对公司、企业的秘密和网络安全非
常有利；

不仅如此，ID日志产生很多有价值的信息，如通过ID日志分析出很多人的行为信息，并以此为依据帮助网站针对性的推出点击率高的内容和广告等；

ID日志可作为日志数据挖掘、日志分析等软、硬件的输入，用ID日志输入，可得到更准确的结果。

附图说明

此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，并不构成对本发明的限定。在附图中；

图1是现有技术中基于IP的有关防火墙的日志文件中日志记录示意图；
图2是现有技术中基于IP的有关计算机系统的日志文件中日志记录示意图；
图3为本发明实施例基于ID的日志记录系统构成示意图；
图4为本发明实施例基于ID的日志记录方法的流程图；
图5A和图5B为本发明实施例ID日志的示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明实施例做进一步详细说明。在此，本发明的示意性实施例及其说明用于解释本发明，但并不作为对本发明的限定。

本发明实施例提供一种日志记录方法及其记录系统，该方法对于基于ID和基于IP来配置策略的网络系统均适用。该方法包括步骤：

生成IP日志，该IP日志记录的内容至少包括IP地址、所进行操作的内容信息；在所述IP日志中查找所述IP地址；将查找到的所述IP地址替换为用户信息，以获得ID日志。

本实施例中，IP日志记录的内容还可包括使用该IP地址的时间信息。
本实施例中，在将查找到的IP地址替换为用户信息时，可以根据IP地址和用户信息的对应关系将IP地址替换为用户信息；或者还可以根据IP地址、使用该IP地址的时间和用户信息的对应关系将IP地址替换为用户信息。

在本实施例中，用户信息可以为用户身份标识ID，用户组，如部门、职位，或者按照年龄划分的组。但不局限于上述情况，还可以是根据实际所要获得的各种用户信息。

下面结合附图3、4、5A和5B，以IP日志记录的内容还包括使用IP地址的时间信息、以及根据IP地址、使用该IP地址的时间和用户信息的对应关系将IP地址转换为用户信息为例，分别对基于ID和基于IP来配置策略的口志记录方法和日志记录系统进行说明。

实施例一

以下首先以计算机系统为例，对基于ID来配置策略的方式中的日志记录方法进行说明。

首先，对基于ID来配置策略的方式进行说明。

例如，某公司或企业为了便于管理网络，针对所有员工设定不同的权限，如表1所示。

对于基于ID来分配策略的方式，首先设置每个员工对应的用户标识信息和分类信息，如在本实施例中，该用户标识信息（ID）如表4所示，且该分类信息可以按姓名、组，如部门或职位进行划分，如表4所示。

<table>
<thead>
<tr>
<th>ID</th>
<th>姓名</th>
<th>部门</th>
<th>职位</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wang</td>
<td>小王</td>
<td>人事部</td>
<td>经理</td>
</tr>
<tr>
<td>Gao</td>
<td>小高</td>
<td>人事部</td>
<td>普通员工</td>
</tr>
<tr>
<td>Li</td>
<td>小李</td>
<td>财务部</td>
<td>普通员工</td>
</tr>
</tbody>
</table>

然后，设定每个员工使用IP地址的范围，其中设定的方式可按照部门、
职位或其组合任意设定，如表5所示，按照部门来设定IP地址的范围，则如表5所示。此外，设定的IP范围也可以是一个IP地址。

表5

<table>
<thead>
<tr>
<th>部门</th>
<th>IP范围</th>
</tr>
</thead>
<tbody>
<tr>
<td>人事部</td>
<td>192.168.1.1-192.168.1.15</td>
</tr>
<tr>
<td>财务部</td>
<td>192.168.1.17-192.168.1.24</td>
</tr>
</tbody>
</table>

然后，根据部门或职位来设定访问权限，如本实施例中按照部门和职位进行设定，如表7所示。

表7

<table>
<thead>
<tr>
<th>部门</th>
<th>职位</th>
<th>访问内部服务器权限</th>
<th>访问Internet权限</th>
</tr>
</thead>
<tbody>
<tr>
<td>人事部</td>
<td>经理</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>人事部</td>
<td>普通员工</td>
<td>有</td>
<td>无</td>
</tr>
<tr>
<td>财务部</td>
<td>普通员工</td>
<td>无</td>
<td>无</td>
</tr>
</tbody>
</table>

这样，当某个员工，如小王通过ID登录某台终端时，认证通过后，服务器根据小王的ID，即Wang和绑定的表4和表5的对应关系来给小王分配IP地址，给小王分配IP地址可为192.168.1.1-192.168.1.15的其中之一，如分配的IP地址可以为192.168.1.15。但不限于上述方式，若考虑到小王是人事处经理，非普通员工，为保证其拥有更高的权限，也可以为人事处经理单独定义IP范围，如192.168.1.16。

然后，将分配的IP地址和用户ID记录在IP-ID绑定表中，如表8所示，同时还记录该用户登录的时间。

表8

<table>
<thead>
<tr>
<th>ID</th>
<th>IP</th>
<th>起始时间</th>
<th>结束时间</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wang</td>
<td>192.168.1.15</td>
<td>2007-7-20 16:30:00</td>
<td>2007-7-20 17:00:00</td>
</tr>
<tr>
<td>Gao</td>
<td>192.168.1.9</td>
<td>2007-7-20 8:00:30</td>
<td>2007-7-20 17:00:00</td>
</tr>
<tr>
<td>Li</td>
<td>192.168.1.17</td>
<td>2007-7-20 10:30:05</td>
<td>2007-7-20 12:30:00</td>
</tr>
<tr>
<td>------</td>
<td>--------------</td>
<td>--------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Gao</td>
<td>192.168.1.15</td>
<td>2007-7-21 9:45:35</td>
<td>2007-7-21 11:15:00</td>
</tr>
</tbody>
</table>

本实施例中，如表8所示，在不同的时间，对于同一个IP地址，如“192.168.1.15”可以分配给不同的用户，如“Wang”和“Gao”。因此，在将IP日志转换为ID日志时，将时间也作为其中的一个参数，这样使得转换后的ID日志更有效。

下面结合附图4、5A和5B对本发明实施例的基于ID的日志记录方法进行说明。

本发明提供一种日志记录方法，如图4、5A和5B所示，该方法采用如下步骤：

步骤401，生成IP日志，该IP日志记录的内容至少包括IP地址、使用该IP地址的时间和所进行操作的内容信息：如图5A和5B所示，但不仅于此，IP日志还可以不包括时间信息，还可根据需要记录任何其信息。

步骤402，在生成的IP日志中查找IP地址：其中，查找IP地址可采用如下方式：首先进行点判断，即判断所述IP日志记录的内容中是否有至少三个点字符，其中，对于IP4，IP地址包含三个点字符“.”，若判断的结果为有“.”，则进一步判断该至少三个点字符“.”中的相邻两点字符“.”之间的信息“*”是否为数字；若判断的结果为是，则确定与至少三个点字符相邻的信息以及所述点字符，如“.*.*.*”构成IP地址，这样，就找到了IP地址。

例如，对于IPv4，例如192.168.1.15，当检查日志内容时，首先判断字符串中是否包含三个“.”，对于上述IP地址是包含三个“.”，然后判断两个相邻的“.”之间的信息是否为数字，对于上述IP地址，两个相邻“.”之间的信息“168”、“1”是数字，因此，判断与该三个“.”相邻的信息与该三个“.”构成IP地址，即192.168.1.15。

本实施例中，上述数字在0～255之间。

步骤403，查找到该IP地址后，根据IP地址、使用该IP地址的时间和ID的
对应关系，如表8所示，将IP地址替换为ID，例如，若IP地址是192.168.1.15，
时间是2007-7-20，16:30:00时，则根据表8将IP地址替换为“Wang”，如图5A
所示；并且，对于同一IP地址，在2007-7-21，9:45:35时，则根据表8，对应的
用户ID是“Gao”，因此将IP地址替换为“Gao”。同样，给小李分配IP地
址为192.168.1.17，时间是2007-7-20，10:30:05时，可将该IP地址替换为“Li”。

或者也可以进一步根据ID-姓名的对应关系，如表4所示，将IP地址替换
为姓名“小王”，从而获得ID日志，如图5B所示。

另外，在基于IP来配置策略的目录记录方法中，与基于ID来配置策略的
方式类似。

例如，当小王通过ID登录某台终端时，认证通过后，服务器根据小王的ID，
表1、表2和表3的对应关系来给小王分配IP地址，即为192.168.1.8。然后，
可将分配的IP地址和用户ID记录在IP-ID绑定表中，产生类如表9所示的绑定
关系表，同时还记录该用户登录的开始和结束时间。

<table>
<thead>
<tr>
<th>ID</th>
<th>IP</th>
<th>起始时间</th>
<th>结束时间</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wang</td>
<td>192.168.1.8</td>
<td>2007-7-20 16:30:00</td>
<td>2007-7-20 17:00:00</td>
</tr>
<tr>
<td>Gao</td>
<td>192.168.1.9</td>
<td>2007-7-20 8:00:30</td>
<td>2007-7-20 17:00:00</td>
</tr>
<tr>
<td>Li</td>
<td>192.168.1.17</td>
<td>2007-7-20 10:30:05</td>
<td>2007-7-20 12:30:00</td>
</tr>
<tr>
<td>Gao</td>
<td>192.168.1.8</td>
<td>2007-7-21 9:45:35</td>
<td>2007-7-21 11:15:00</td>
</tr>
</tbody>
</table>

在基于IP来配置策略的目录记录方法中，将IP日志转换为ID日志的方法
流程与上述基于ID的方法流程类似。在查找到IP地址后，根据IP地址、使用
该IP地址的时间和ID的对应关系，如表9所示，将IP地址替换为ID，例如，若
IP地址是192.168.1.8，则可根据表9的绑定关系，以及时间将IP地址替换为
“Wang”或“Gao”，如图5A所示；同样，给IP地址为192.168.1.17时，可将
该IP地址替换为“Li”。由上述可知，当小高想上网或访问服务器时，那么
小高通过使用小王的计算机来达到目的，这样在ID日志文件中可知道真实的用户，因此，有利于网络管理和网络安全。

同理，在上述实施例中，还可根据用户ID、表4、表5、表8的对应关系，或者表1、2、3和类似表9的对应关系，获得IP-用户组的对应关系，如IP-部门、IP-职位的对应关系；此外，用户组还可以按照用户的年龄来划分，但不限于上述方式，可根据网络的实际情况和所要获得的用户信息来绑定上述对应关系。

通过上述实施例，将IP日志转换为基于ID的ID日志，这样，通过ID日志可直接获得使用计算机的真实用户，这些日志信息可向系统管理员提供危害安全的非常有用的相关信息，对公司、企业的秘密和网络安全非常有利；

对于网站，ID日志会产生很多有价值的信息，如通过ID日志分析出很多用户的行为信息，并以此为依据帮助网站针对性的推出点击率高的内容和广告等；并且，ID日志可作为日志数据挖掘、日志分析等软、硬件的输入，用ID日志输入，可得到更准确的结果。

实施例二

本发明实施例提供一种日志记录系统，如图3所示，该日志记录系统至少包括：IP日志生成单元301，用于生成IP日志，该IP日志记录的内容至少包括IP地址、所进行操作的信息，如图5A和5B所示，此外，还可包括时间等信息，但不限于此；

查找单元302，与IP日志生成单元301连接，接收IP日志生成单元301传送的IP日志，在所述IP日志中查找所述IP地址；

ID日志生成单元303，与查找单元302连接，接收查找单元302查找到的IP地址的信息和IP日志，并将查找到的所述IP地址替换为用户信息，以获得ID日志。

本实施例中，该日志生成单元303根据IP地址、使用该IP地址的时间和ID的对应关系将IP地址替换为用户信息。但不限于此，该日志生成单元303还可
根据IP地址和ID的对应关系将IP地址替换为用户信息。

本实施例中，如图3所示，查找单元302至少包括：

接收单元302a，与IP日志生成单元301连接，接收IP日志生成单元301传送的IP日志；

判断单元302b，与接收单元302a连接，用于判断IP日志中是否有至少三个点字符；若判断的结果为有，则进一步判断该至少三个点字符中的相邻两点字符之间的信息是否为数字；若判断的结果为是，则确定与至少三个点字符相邻的信息以及所述点字符构成IP地址，并将该IP地址和IP日志传送至ID日志生成单元303。

此外，如图3所示该系统还包括存储单元304，与ID日志生成单元303连接，储存生成的ID日志。

在上述实施例中，是以生成的日志格式是由日志文件的情况为例进行说明，但不优于此，ID日志的格式除了可以为日志文件以外，还可以也可以是一条一条日志记录的格式，处理流程与处理日志文件类似，此处不再赘述。

上述系统的工作流程与方法流程一致，此处不再赘述。

通过上述实施例，将IP日志转换为ID日志，这样，通过ID日志可直接获得使用计算机的真实用户，这些日志信息可向系统管理员提供危害安全的非常有用的相关信息，对公司、企业的秘密和网络安全非常有利。

此外，对于网站，ID日志会产生很多有价值的信息，如通过ID日志分析出很多用户的行为信息，并以此为依据帮助网站针对性的推出点击率高的内容和广告等；并且，ID日志可作为日志数据挖掘、日志分析等软、硬件的输入，用ID日志输入，可得到更准确的结果。

以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。
日志文件

1. ...

2. Cisco-PIX-506 # 192.168.1.15
   2007.7.24; 9:30:05 access
   192.168.1.201 ...

3. ...

4. ...

......

图1

日志文件

192.168.1.8 2007.7.20; 9:30:05 浏览网页
192.168.1.9 2007.7.20; 9:30:05 编辑文件
192.168.1.17 2007.7.20; 10:30:05 copy报表

......

图2
图3
图4

IP日志
192.168.1.15 2007-7-20:16:30:00 浏览网页
192.168.1.17 2007-7-20:10:30:05 copy报表
192.168.1.15 2007-7-21: 9:45:35 编辑文件

ID日志
Wang 2007-7-20:16:30:00 浏览网页
Li 2007-7-20:10:30:05 copy报表
Gao 2007-7-21: 9:45:35 编辑文件

图5A
图5B

IP日志

192.168.1.15  2007-7-20:16:30:00  浏览网页
192.168.1.17  2007-7-20:10:30:05  copy报表
192.168.1.15  2007-7-21: 9:45:35  编辑文件

......

ID日志

小王  2007-7-20:16:30:00  浏览网页
小李  2007-7-20:10:30:05  copy报表
小高  2007-7-21: 9:45:35  编辑文件

......