用好代理日志 维护网络秩序

申 政 (烟台东方电子信息产业集团网络中心 264001)

摘要：本文为员工通过企业局域网的代理服务器到Internet上浏览、查询和下载资料的安全管理提供一种方法，方法的中心思想是通过提高上网透明度让业务部门领导能够随时了解本部门员工的网上操作，使企业有效的网络资源发挥最大的效益。

关键词：网络安全 代理服务器 方便监督

1 引言

企业计算机网络一般都设置一台WEB服务器用作企业员工上Internet的出口，为了企业内部网的安全，通常需要安装Microsoft Proxy Server代理服务器软件作为内外部交换信息的中介，它象一堵墙一样将Internet上的计算机和企业内部的计算机有效地隔离，因此它也算是一个防火墙。企业内部的计算机要到Internet上查询和下载相关信息，必须出示允许上网权限的帐号，经验证通过后代理服务器才同意给予代理并将目的地址及相关信息通过相应端口送达Internet上目的计算机，同时将目的计算机的信息取回来再送到企业内部相应的计算机上，这一过程被代理服务器的日志详细记录了下来，比如企业内部申请上网的计算机的IP地址、帐号、日期、时间、目的站点的地址、栏目以及送出和取回信息的字节数等信息。无疑这些记录信息对于维护网络安全起到了重要作用，企业网络管理人员应将这些信息充分利用好。

2 维护网络程序有关事项

代理服务器记录上网信息默认的形式是纯文本，也可采用SQL/ODBC Database的形式记录，前者很难对数据加工，后者记录的速度慢，在并发访问较多的情况下，网络性能会有显著下降。在网管的实践中，我们对这一部分信息做了一些小小的加工，以用来维持网络秩序。首先要编写一个《上网记录处理》小程序，这个可以用各种前端数据库管理系统生成，如VB、PB、VFP等，处理程序应具备以下功能，如图1所示。

(1) 转换处理：分人工干预和自动两种方式。

①所谓转换，是指将指定日期的上网记录剔除多余部分，从代理服务器的纯文本形式转换到MS SQL Server或Sybase等后端数据库内，并且进行流量统计，将统计结果一并送入后端数据库。

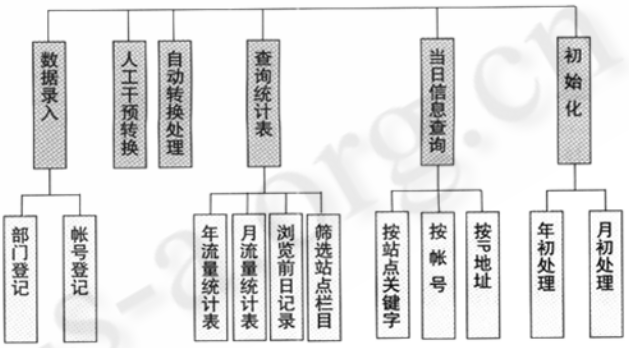

图 1 上网记录处理

②平时系统处于自动转换模式，一般安排在每天凌晨零点以后，网络负荷小的时候开始转换。

③当出现特殊情况没有进行自动转换时，可启动“人工干预转换”，这只是一种补救措施。

(2) 数据录入：主要进行部门和帐号登记，为后面的查询模块提供查询选项。

(3) 查询统计表：该模块可有4种选择。

①查询年流量统计表：该表是由月流量表汇总生成，可显示各子网或帐号每个月的流量累计及截止目前的总累计。

(下转第60页)

(上接第 76 页)

②查询月流量统计表：该表是转换处理模块汇总生成。可显示各子网或帐号每天的流量累计及截止目前的月累计结果。

③浏览当日记录：由于转换处理模块始终缓存着前一次转换的源数据，所以浏览前日记录时一般不需再转换，因而处理速度较快。

④筛选站点栏目：是通过输入一些感兴趣的站点地址或关键字或帐号或IP地址，将记录筛选出来有针对性地查询。

(4) 当日信息查询：是将当天到目前为止的上网记录按站点关键字或帐号或IP地址筛选查询。

(5) 初始化：是系统需要恢复初始状态时使用，如需要年初处理、月初处理或全部恢复初始状态等。

其次，为在网上查询方便起见，可用asp编写一个类似上述模块中“查询统计表”的小程序放在服务器端，这样各级领导和有关人员便可在自己的计算机上通过微软提供的IE浏览器进行快速查询相应的上网记录或统计表，当然，这些查询只能在权限规定的范围内。这一措施可帮助企业各级领导及时掌握本部门员工上网的情况，出现倾向性的苗头可随时给予纠正。■