广西科学院学报
Journal of Guangxi Academy of Sciences

2008,24(4):342~344
Vol. 24,No. 4 November 2008

一个内网外联监控系统的设计与实现

The Design and Build of the Monitor System on the Intranet Connecting to the Internet

雷启麟,杨辉华
LEI Qi-lin,YANG Hui-hua

(桂林电子科技大学,广西桂林 541004)
(Guilin University of Electronic Technology,Guilin, Guangxi,541004,China)

摘要:在Microsoft Windows NT系列平台下设计实现一个内网外联监控系统。该系统由报警中心、审计管理中心、发放管理平台和客户端监控程序组,能够重点解决局域网内部系统非法外联的安全问题,确保各个局域网内部安全。

关键词:网络监控 内网 非法外联
中图法分类号:TP312 **文献标识码**:A **文章编号**:1002-7378(2008)04-0342-03

Abstract: On the platform of Microsoft Windows NT, the monitor system specialized on the intranet connecting to the internet was designed and built. This system consists of alarm center, audit management center, grant management platform and the program of client monitoring. In order to ensure the safety of the intranet, the system could primarily solve the safety issue caused by the invalid connecting of the intranet.

Key words: network monitor, intranet, invalid connect

随着信息技术不断发展,各种蠕虫病毒、黑客攻击也越来越猖獗。传统的网络安全解决方法都是把目标的重点放到边界上,却往往忽略网络内部安全。在目前的网络管理工作中,工作量最大的是客户端的安全管理,对网络正常运转威胁最大的也是客户端的安全管理,网络客户端会经常暴露出一些安全隐患。内网的客户端构成了内部网络90%以上的组成,当之无愧的成为内部安全的重中之重。当前,虽然大力提倡信息公开,但是许多涉及国家秘密、客户私人信息、公司内部重要资料等的计算机还是不宜联接互联网。对这些禁止联接互联网的内部计算机,一旦使用者通过电话线拨号、VPN拨号、GPRS无线拨号等方式非法外联,就很容易被互联网上的攻击者获取内部重要信息。

我们提出一种专门针对内部网络私自外联的安全管理的体系结构,并设计实现了内网外联监控系统,通过直观有效的安全策略设置,对内网中的私自外联行为进行监控和管理,并通过完善的日志记录各种外联行为的痕迹,确实阻断内网私自外联行为。

1 内网外联监控系统的设计目标

根据网络安全的特征,结合对内网安全问题的分析,我们将内网外联监控系统的总体设计目标定为:监控内部计算机通过电话线、ISDN、ADSL、无线网卡、GPRS/CDMA、双网卡、代理服务器等多种方式导致的内部计算机连接互联网的行为。无论被监控的计算机在何时何地,一旦发现违规外联国际互联网,第一时间上报管理部门,并阻断被监控计算机的网络连接,杜绝非法外联的可能,有效保障网内信息安全。

内网外联监控系统在Microsoft Windows NT系列平台下开发实现,可以对内部网络系统中的各终端、单机、笔记本电脑的外联行为进行监控,有效阻止内部计算机非法外联,确保单位内部数据安全。

2 内网外联监控系统设计

2.1 总体设计

内网外联监控系统的关系如图1所示。

收稿日期:2008-07-25
修回日期:2008-09-18
作者简介:雷启麟(1980-)男,硕士研究生,主要从事保密技术检查工作。

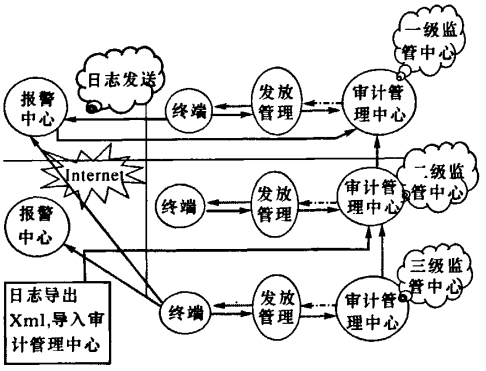

图1 内网外联监控系统的关系

------▶：提交用户信息xml文件；------▶：生成各单位发放管理平台的配置文件；……▶：生成各终端监控程序的配置文件；——▶：提交终端用户信息。

为了解决跨地区，跨部门监管的问题，本系统采用多级监控管理。以省、市、县三级监管中心为例。一级监管中心平台的运作流程是首先省级建立一级管理平台，在外网服务器安装报警中心，在1台计算机上安装审计管理中心，这样平台搭建完毕。管理员利用审计管理中心的编码分配管理功能，为各省直单位分配1个编码，然后根据分配的编码为每个单位生成一个对应此编码的配置文件（例如：服务器IP、服务名称、编码中的前四位编号等）。将配置文件和发放管理平台一同发放到各省直单位，各单位的管理人员安装之后，发放管理平台实施完毕。省直各单位的管理员，通知各部门通过发放管理平台的用户信息注册功能提交用户信息（内容如下：用户姓名、部门名称、联系电话、提供一个实际使用的物理网卡MAC地址等），然后管理员对提交的信息进行审批，审批不通过的退回重新提交。对于审批通过的可以利用发放管理平台的终端机器编码分配管理功能为每个终端机器生成监控程序安装所需要的配置文件。将配置文件和监控程序的安装程序一同发放到终端用户。终端用户将客户端安装到终端机器，则监控程序实施完毕。到此整个系统的实施阶段结束。在后续的时间里，监控程序实时监控终端主机的外联行为，一旦发现外联，立即向报警中心发送外联日志，阻断网络，给出10s的提示，然后关闭违规的主机。报警中心在接收到监控程序发送来的外联日志后，给出声音报警，同时在监控地图上显示出发生违规行为的主机所属的地理位置和编号，并且将外联的信息发送到指定的Email。而且通过网页远程登录报警中心，也可以收到声音报警和文字提示报警。管理员可以利用报警中心的日志导出功能，将外联日志导出为xml文件，然后导入到审计管理中心，则可以对外联日志进行统计、报表、打印等管理。

二级和三级监管中心（各地市）的流程跟一级监管中心（省级）相同，不同的地方就是在二级、三级（各地市）的审计管理中心，需要将用户信息导出为xml文件，上报到上一级的监管中心，然后一级监管中心（省级）的管理员通过一级（省级）审计管理中心的用户信息导入功能将下面各级中心的用户信息导入到一级（省级）的审计管理中心，从而完成各级用户信息的上报。

系统的模块框架如图2所示。

2.2 功能设计

2.2.1 报警中心

报警中心具有并发连接的性能，单服务器承受10万级别的并发连接数量，而通过服务器集群的连接可以承受多达百万或者千万级的并发客户端数量，能够保证通讯安全和数据存储安全。

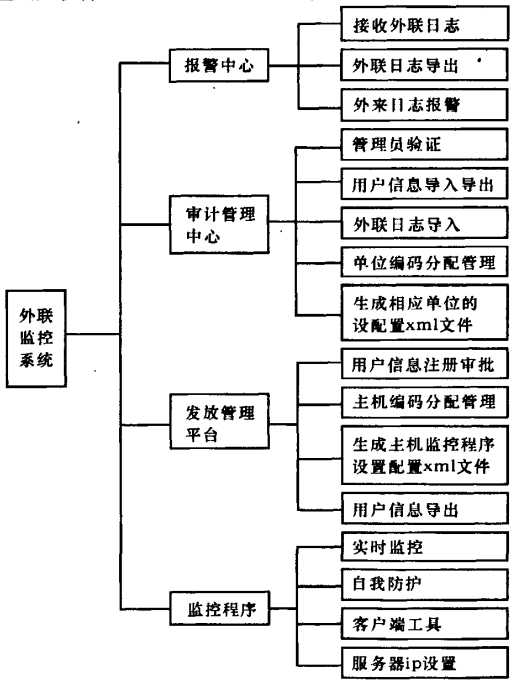

图2 系统的模块框架

报警中心具有完善的安全保密策略，只存储违规外联计算机的唯一序列号，与存放计算机具体信息的内网审计管理中心计算机物理隔离，并采用硬件加密措施确保监控程序与外网监视服务器之间数据通讯的安全性；支持多个外网监视服务器，满足多级管理需求；支持跨路由、多网段的检测；支持日志导出和存储，提供声音报警，支持邮件提醒等方式。

2.2.2 内网审计管理中心

内网审计管理中心的功能主要是对外联日志进行审计、统计以及生成发放管理平台。其采用key+密码的形式进行主页的登陆，提供违规日志导入功能；可以导入由外网监视端导出的违规日志的xml文件；日志查询；日志统计：按不同策略统计违规外联发生的次数，可以生成月报、季报和年报；提供安装信息导入功能：完成二级以上平台安装信息的汇报；提供安装信息打印功能；提供生成"主机监控程序发放管理系统"功能，监控中心的管理员可以利用这个功能，为各个部门生成相应的发放管理系统，从而各部门的管理人员可以自己分配管理各终端主机的编号以及生成监控程序安装所需的配置文件等。

2.2.3 发放管理平台

发放管理平台由内网审计管理中心生成，安装在各部门局域网内的服务器上，由各自管理员管理各自内网的主机相关的用户信息。

终端用户通过发放系统的"用户信息注册"页面，注册自己的部门、姓名、联系方式、机器的mac、硬盘序列号等。在用户信息提交后，管理员则可以根据编码规则对提交上来的信息进行编码处理，编码分配后，终端用户则可以在下载页面，下载自己机器相关的客户端（客户端安装包与本机的MAC和硬盘序列号绑定，不可交叉使用）。待终端用户的客户端安装完毕后，则可以修改对应用户的安装状态。

安装成功的注册信息可以导出成xml文件，以便上报，xml文件需要加密，防止内容被修改。

发放管理平台采用标准的web技术实现，操作简单，使用方便。发放管理平台通过key中密钥校验，确保信息安全。

2.2.4 主机监控程序

主机监控程序主要用于监控内部计算机是否通过电话线、ISDN、ADSL、无线网卡、GPRS/CDMA、双网卡、代理服务器、无线网卡等多种方式连接互联网的行为。一旦检测到主机外联，一方面，将自动阻断主机与互联网的连接，并给用户10s的时间保存其他未保存的文件，之后将会自动关机；另一方面，将通过通讯加密的方式将日志传输到报警中心，日志在传输过程、数据库中存储均为加密状态，其中密钥存储在外网服务器的key中，加密算法通过key完成，保证传输过程所传输的信息不被黑客截获破解。除此之外，监控程序还要具备自身保护、防火墙突破等功能。

3 系统运行环境及实现技术

3.1 系统运行环境

网络运行环境支持TCP/IP协议的以太网。监控服务器支持Windows 2003 Server R2操作系统，Internet信息服务，.NET Framwork3.0及以上版本，SMTP服务，SQL Server2005数据库或更高版本。监控服务器为即插即用(Plug-in)硬件设备(专用工业级机架服务器)结构，对外的连接界面为2个100/1000Base-TX接口，对于大中型网络环境，LPS-G10000可提供千兆以太网接口，提供高速大流量处理能力。内网审计管理中心和主机监控程序的软件环境支持Windows2000 /Windows XP；CPU为Pentium 4 2.0G以上，内存256MB或以上，硬盘为512MB以上空余空间。

3.2 系统实现的关键技术

系统实现主要利用了网络通讯TCP/IP数据包编程技术。在内部网络中安装终端监控软件，在Internet上安装非法外联监控服务器，一方面利用监控服务器对指定网络计算机进行多线程并发发送探测数据包，对监控的内部计算机网络进行轮循扫描，检测网络主机向外连接链路状态；另一方面，监控计算机不停尝试设在互联网上的服务器及互联网上的各大主要门户网站，一旦发现网络内用户在连接内部网络的同时连接Internet或其它不安全网络，自动断开网络、关闭主机并告警，安全管理人员可立即通过管理系统对违规机器准确定位。

4 结束语

内网外联监控系统在现有的计算机网络安全体系的基础上提供了一个内部网络安全保障的解决方案。内网外联监控系统解决了如何监管内部网络用户非法外联的问题，能够限制内部网络用户非法外联，不但可以保证内部重要数据的安全，也可有效防止内部网络用户受到外网的恶意访问和攻击。

参考文献：

[1] 李涛. 网络安全概论[M]. 北京：电子工业出版社，2004.

[2] 沈昌祥. 信息安全工程导论[M]. 北京：电子工业出版社，2003.

[3] Jim Beveridge，Robert Wiener. Win32多线程程序设计[M]. 第2版. 北京：清华大学出版社，2000.

（责任编辑：邓大玉）