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

2007,23(4):356~359
Vol. 23,No. 4 November 2007

广西柳工机械股份有限公司网络的准入控制管理方案
The Network Access Control Management of the Industrial Machinery Co. ltd of Liuzhou,Guangxi

邢海韬[1],孙宁青[2],吴伟琦[2]
XING Hai-tao[1],SUN Ning-qing[2],WU Wei-qi[2]

(1.广西柳工机械股份有限公司,广西柳州 545007;2.广西工业职业技术学院,广西南宁 530000)
(1. Guangxi Liugong Machinery Co. Ltd, Liuzhou, Guangxi, 545007, China; 2. Guangxi Vocational and Technical Institute of Industry,Nanning,Guangxi,530000,China)

摘要:在介绍广西柳工机械股份有限公司(简称柳工)网络概况的基础上,简述柳工网络的准入控制管理方案。该方案采用SYMANTEC公司的SYGATE解决方案,通过LAN Enforcer策略、Gateway Enforcer策略等技术实现对所有网络终端的规范化管理和策略准入控制,能够正常连接合法用户进入网络、拒绝非用户进入网络或拷贝数据。该方案是一个新的内部网络安全控制方法。

关键词:网络管理 网络安全 网络准入控制 风险分析
中图法分类号:TP393.07 **文献标识码**:A **文章编号**:1002-7378(2007)04-0356-04

Abstract: This paper presents the design of the network access control management of the Industrial Machinery Co. Ltd of Liuzhou Guangxi. With SYGATE of the SYMANTEC, all the network terminals are under standardized management and access control via the technology of LAN Enforcer and Gateway Enforcer. The system is a new security control over the network.

Key words: network management, network security, network access control, risk analysis

广西柳工机械股份有限公司(以下简称柳工)是我国工程机械行业的骨干企业,主导产品中,装载机系列产品的开发水平、制造规模和市场占有率多年来一直居全国领先地位,产销量近年跃居世界前列。作为一个以技术领先为导向的创新型企业,柳工一贯非常重视IT技术在企业中的应用。"九五"至今,公司在以"柳工CIMS(计算机集成制造系统)"两期工程为主体内容的信息化建设上已经累计投入了2800多万元。目前,柳工已经建成一个内连企业所有业务区域、外接互联网、总部和远程分部异地相通、固定和移动用户方便协同的立体、庞大、方便、安全的复合网络体系。

对于这样一个复杂的网络环境,如果没有良好的网络管理体系,容易导致安全泄密以及网络运行不稳定等情况。网络安全是一个需要柳工重点考虑的工作。为此,柳工结合自己网络的实际情况,通过与科研院所和公司合作的方式,实现了自己环境下的网络准入控制。

1 柳工网络概况

柳工网络接着南、北两个厂区以及近地子公司,位于江苏镇江、江阴等处的远地子公司则通过专线及VPN虚拟专网与总部相连。由主干网及其延伸组成的企业网络覆盖公司所有的办公、制造和仓储地点,公司在网络协同环境的支撑下,全部主体业务(包括产品开发,生产计划管理、财务管理、营销服务、采购招标平台等)都在网络环境下进行,全部管理和技术人员以及企业上、下游的主要合作伙伴都在网络上协同工作,实现了IT对企业创造价值过程的有力支撑。

柳工网络的结构拓扑如图1所示。

收稿日期:2007-09-30
作者简介:邢海韬(1975-),男,工程师,主要从事网络管理与网络安全研究。

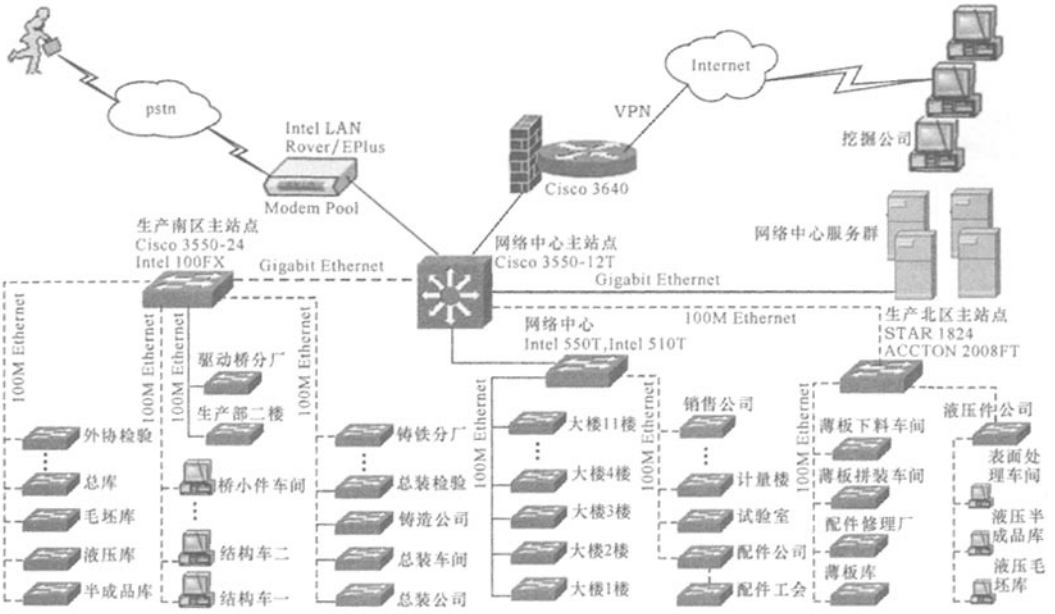

图 1 柳工网络拓扑

——:双绞线;----:光缆。

2 柳工网络准入控制管理的解决方案

2.1 网络准入控制管理的目标

柳工网络准入控制管理的目标主要有两个方面,一是将安全策略、硬件及软件等方法结合起来,构成一个统一的防御系统,有效阻止非法用户进入网络,减少网络的安全风险。二是定期进行漏洞扫描,审计跟踪,及时发现问题,解决问题。

2.2 网络准入控制的需求

网络准入控制的需求实际上是如何防止企业的计算机网络被非法连入,以及防止数据被非法拷贝。因此,网络准入控制的需求是:(1)在柳工本部的计算机网络内,所有接入网络的计算机必须被验证后才能加入网络;(2)网络内存在的非计算机连接点(如考勤机、数控机床等)可以正常连接进网络,但是要防止在这些连接点被非法连入计算机;(3)通过远程方式连入的计算机必须符合企业网络管理控制的有关要求才可接入。

2.3 网络准入控制的总体部署

通过技术对比与方案评估,柳工采用了SYMANTEC公司的SYGATE解决方案。由于柳工网络系统主要包含公司本部,远端分公司通过SDH电信链路与总部相连,同时公司还有相当数量的远程VPN移动用户,为实现对所有网络终端的规范化管理和策略准入控制,在柳工网络的所有终端(含远程VPN用户)均部署Symantec Sygate终端保护代理。

(1)在公司本部大楼2L-Switch交换机通过接入LAN Enforcer策略强制服务器满足公司本部终端的网络准入控制。

(2)在各分公司统一接入的路由器和核心层交换机中间,接入Gateway Enforcer策略强制服务器满足分公司接入公司总部网络的准入控制。

(3)对于大量的远程VPN用户,通过在公司网关防火墙和核心层交换机之间,部署Gateway Enforcer策略强制服务器满足远程VPN用户的网络准入控制和策略强制。

在柳工通过网络准入(LAN Enforcer)和网关准入(Gateway Enforcer)两种方式实现终端准接入控制。Sygate Gateway Enforcer安装于Linux平台,需要两块网卡并以透明桥方式接入,目前部署了3台,其中放置在两台防火墙之后的网关准入服务器配置为负载均衡模式(同时工作,负载均衡);网络准入LAN Enforcer安装于Linux平台,目前部署2台并配置为负载均衡模式(同时工作,负载均衡)。由于网络准入Lan Enforcer,需要交换机支持802.1x协议并在端口上配置802.1x端口认证。详见图2。

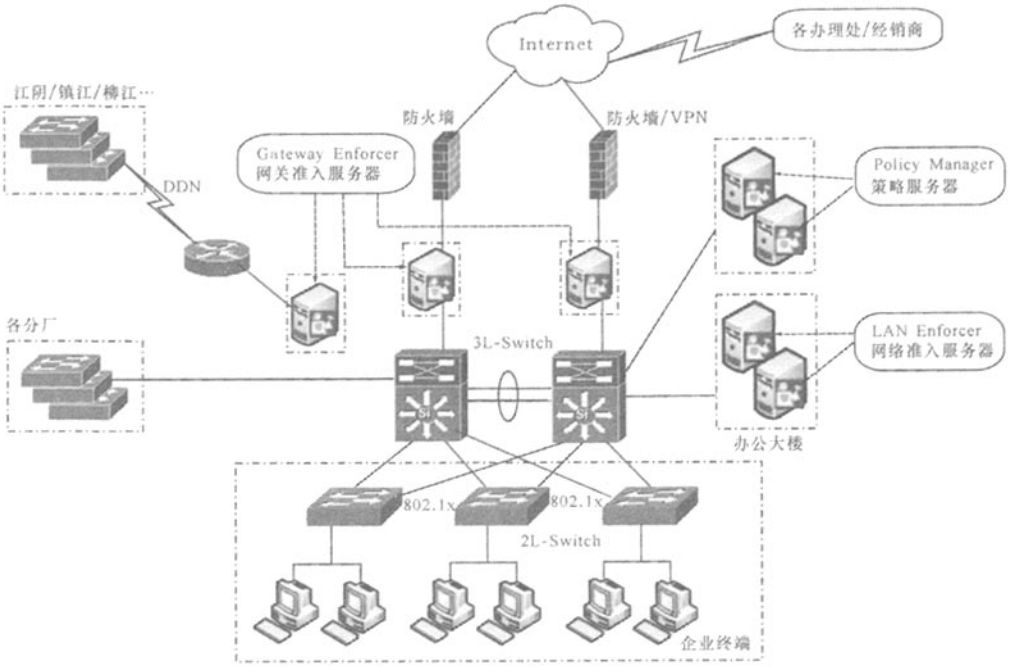

图2 柳工网络准入控制的总体部置拓扑

2.4 特殊接入点的控制方案

由于数控机床、考勤机系统等无法安装客户端，所以，在准入控制的时候，采取对数控机床、考勤机等不安装 Sygate 客户端，同时与数控机床、考勤机相连的交换机端口也不配置 802.1x 认证。为满足数控机床与外网传输数据的要求，网关准入 Gateway Enforcer 将通过例外表方式对数控机床 MAC 地址不进行认证。考虑到可能会有用户使用数控机床网口接入网络，就对所有的 Sygate 客户端均配置策略禁止与数控机床之间的访问(这样用户就算使用了数控机床的 IP/MAC 也无法访问网络中其他设备)，另一方面通过在防火墙上配置策略，只允许数控机床应用的特定端口/访问方向的外网访问(这样用户就算使用了数控机床的 IP/MAC 也无法访问外网)。

2.5 网关准入管理方式下的风险控制

网关准入控制要考虑如果出现问题该如何处理。首先 Sygate 的网关准入安装在最小化安装的 Linux 平台上，运行非常稳定，出现故障的可能性非常低。其次是配置为负载均衡模式，能够同时工作，负载均衡，两台机器同时出现故障的可能性更低。再次是提供网关跳线操作解决方案，即把网关准入服务器以透明桥方式接入核心交换机和防火墙中间，应急情况下用户可以直接将核心交换机直连防火墙，保障发生意外故障时，正常业务实现通信不中断。

2.6 LAN 准入管理方式下的风险控制

网络准入控制也要考虑如果出现问题该如何处理。首先 Sygate 的网络准入安装在最小化安装的 Linux 平台上，运行非常稳定，出现故障的可能性非常低。其次是配置为负载均衡模式能够同时工作，负载均衡，两台机器同时出现故障的可能性更低。再次是由于 802.1x 涉及到的认证环节比较多(客户端-交换机-LanEnforcer-策略服务器)，其中任一环节出问题均会导致认证失败；认证失败将有两种结果：a. 直接关闭交换机端口，b. 切换为隔离 Vlan，用户可以通过配置进行设定，隔离 Vlan 的资源受限访问完全是由路由访问控制的；所以应急情况下，网络准入控制可以通过放开隔离 Vlan 的受限访问控制，这时隔离 Vlan 和正常 Vlan 没有区别，换个意思表达即和没有实施 802.1x 之前访问方式是一样的。

2.7 日常管理方式的改变

Sygate 的策略服务器界面简洁直观，同时可以通过 Web 直接访问，平时维护和管理非常方便。尤其是在对网络计算机进行准入控制的时候，可以通过管理界面直观地看到网络内计算机的连接以及非认证连接的计算机。因此，在日常管理工作中，主要通过监控功能实时察看网络内攻击行为、违规行为

等日志,不定期升级相关 IPS 库、策略模版即可实现对网络内的管理。同时,Sygate 内置的邮件通知功能可以通过配置直接将上述日志报表发送到管理员的邮箱。

3 结束语

广西柳工机械股份有限公司使用这套网络准入控制管理方案后,可以实现合法用户正常连接进入到网络,非法用户无法连接进入网络,远程连入的用户也能够按照企业的网络管理规则签到而进入网络。这套方案为对于在网络内如何做好安全控制提供了新的思考方向。

参考文献:

[1] 雷震甲. 网络工程师教程[M]. 北京:清华大学出版社,2004.

[2] 王春森. 系统设计师[M]. 北京:清华大学出版社,2001.

[3] 郭军. 网络管理[M]. 北京:北京邮电大学出版社,2001.

[4] 张炯明. 电子商务安全使用技术[M]. 北京:清华大学出版社,2005.

[5] 劳帼龄. 网络安全与管理[M]. 北京:高等教育出版社,2003.

[6] 祁明. 网络安全与保密[M]. 北京:高等教育出版社,2005.

[7] 白以恩. 计算机网络基础及应用[M]. 哈尔宾:哈尔宾工业大学出版社,2004.

(责任编辑:邓大玉)

(上接第 349 页)

得了 USB 安全钥和用户 PIN 码,才可以登录系统。即使用户的 PIN 码被泄漏,只要用户持有的 USB 安全钥不被盗取,合法用户的身份就不会被仿冒;如果用户的 USB 安全钥遗失,拾到者由于不知道用户 PIN 码,也无法仿冒合法用户的身份。

USB 安全钥在系统中的认证流程如图 2 所示。

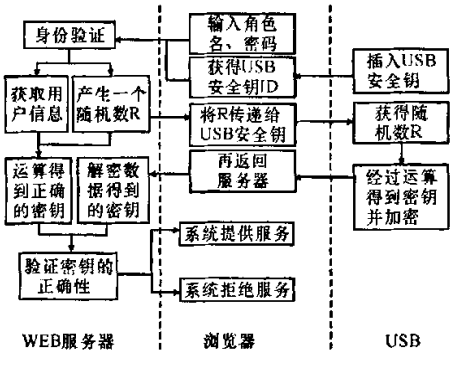

图 2 USB 安全钥在系统中的应用流程

5 结束语

本文实现的政府部门专用的办公自动化系统充分利用了 Internet/Intranet 的优势,采用成熟的网络和安全技术,保障了政务的安全传送和处理,为政府部门及时掌握和处理信息提供了一个先进、可靠、安全保密的系统。通过使用该系统,可以不断改进现有的工作环境和条件,进一步提高机关工作的效率、水平和质量,实现日常办公事务、处理事务的自动化、标准化,最终实现办公过程的"无纸"化,以适应办公信息化建设的需要。本文所介绍的系统对行政单位、企事业单位建设办公自动化系统有一定的参考价值。

参考文献:

[1] RICH HELTON, JOHENNIE HELTON. Java 安全解决方案[M]. 北京:清华大学出版社,2004.

[2] 祝晓光. 网络安全设备与技术(公钥基础设施(PKI)部分)[M]. 北京:清华大学出版社,2004.

[3] 冯世立,李鹏飞,张海峰. USB 安全钥在电子政务系统的应用[J]. 计算机安全,2006(2):31-32.

(责任编辑:韦廷宗)