防火墙和入侵检测系统在电力企业信息网络中的应用

王先培[1]，熊 平[1]，李文武[2]
(1. 武汉大学电子信息学院，湖北省武汉市 430072；2. 三峡大学现代教育技术中心，湖北省宜昌市 443002)

摘要：如何保障电力企业信息网络的安全是当前电力企业信息建设的研究热点。文中通过分析电力企业信息网络的结构和对网络安全的要求，在归纳了防火墙和入侵检测系统在网络中的防御功能的基础上，提出了将防火墙和入侵检测系统运用到电力企业信息网络的具体方案，并对相关技术和网络安全体系的建设进行了讨论。

关键词：电力企业；防火墙；入侵检测系统；企业信息网

中图分类号：TP393.08

0 引言

当前，电力系统已基本形成了自己的生产过程自动化和管理现代化信息网络，并在实际生产和管理中发挥着巨大的作用。随着全球信息化的迅猛发展，电力系统必将加强与外部世界的信息交流，以提高生产和管理效率，开拓更广阔的发展空间。然而，网络开放也增加了网络受攻击的可能性。与外部网络的连接必然面临外来攻击的威胁。对于关系到国计民生的电力系统而言，网络安全必须作为一个重大战略问题来解决。目前，防火墙技术作为防范网络攻击最基本的手段已经相当成熟，是抵御攻击的第一道防线，入侵检测系统(intrusion detective system，缩写为 IDS)作为新型的网络安全技术，有效地补充了防火墙的某些性能上的缺陷，两者从不同的角度以不同的方式确保网络系统的安全。

本文首先分析电力企业信息网络的结构，并结合其特点和对网络安全的特殊要求，就如何有效地将防火墙和入侵检测技术运用到电力企业信息网络中进行探讨。

1 电力系统的信息网络

电力系统的信息网络[1]分为两大模块：监控信息系统(supervisory information system，缩写为 SIS)和管理信息系统(management information system，缩写为 MIS)。

SIS 对生产现场进行实时监控，从分布在生产现场的许多点采集数据，再由系统中的计算单元进行性能计算、故障诊断等，将结果存放到实时数据服务器，为生产现场实时提供科学、准确的数据，以控制整个生产过程。SIS 包括 CRT 监控系统、DCS(数据通信系统)、FCS(现场总线控制系统)等子系统。

MIS 的功能是实现企业自动化管理，包括若干子系统，分别实现生产经营管理、财务和人事管理、设备和维修管理、物资管理、行政管理等功能。较完善的 MIS 还包括辅助决策子系统，为管理人员提供智能支持，是企业管理规范化、科学化的基础。

目前电力系统的信息网络一般将 SIS 和 MIS 分做同一网络中的两个子网，并分别配置服务器，两子网之间用网关连接，如图 1 所示。

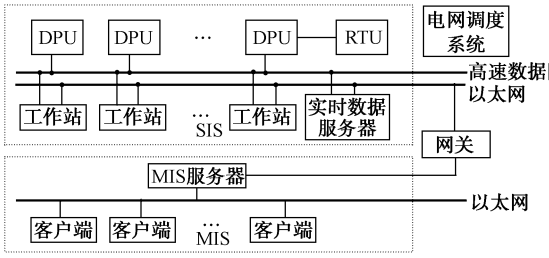

图 1 企业内部局域网
Fig. 1 Structure of LAN in electric enterprise

DPU(分散过程控制单元)从生产现场采集数据并发送到高速数据网供 DCS 各工作站分析处理，同时为了保证 SIS 的网络安全，SIS 以太网通过网关与 MIS 服务器连接，作为 MIS 到 SIS 的入口并管理 MIS 对 SIS 的访问。

SIS 和 MIS 功能各异，对安全的要求也有所不同。SIS 由于与现场生产息息相关，一旦遭到入侵，势必影响生产甚至造成恶性事故，所以其安全性要求更高。现行的网络结构也充分体现了这一特点，对 SIS 实施更高级别的保护。

当局域网与外部网络连接后，MIS 要向外界提供服务，网络面临的威胁将空前广泛、尖锐，这时原有的安全系统显然过于单薄，必须在原有基础上制定更严密、可靠的防御体系。

收稿日期：2001-09-16；修回日期：2001-10-29。

在安全的操作系统基础上,防火墙结合 IDS 是一种较为理想的解决方案。

2 防火墙

防火墙[2]是防范网络攻击最常用的手段,是构造安全网络环境的基础工程。它通常被安置在内部网络与外部网络的连接点上,将内部网络与外部网络隔离,强制所有内部与外部之间的相互通信都通过这一节点,并按照设定的安全策略分析,限制这些通信,以达到保护内部网络的目的。

2.1 防火墙的体系结构[3]

构造防火墙时通常根据所要提供的服务、技术人员的技术、工程的性价比等因素采用多种技术的组合,以达到最佳效果。

目前常见的防火墙体系结构有以下几种:

a. 双重宿主主机体系结构。在内部网络与外部网络之间配置至少有两个网络接口的双重宿主主机,接口分别与内部、外部网络相连,而主机则充当网络之间的路由器。这样,内部、外部网络的计算机之间的 IP 通信完全被阻隔,只能通过双重宿主主机彼此联系。

b. 屏蔽主机体系结构。这种结构的防火墙由路由器和堡垒主机构成,路由器设置在内部、外部网络之间,实现数据包过滤。堡垒主机设置在内部网络中,外部网络的计算机必须连接到堡垒主机才能访问内部网络。

c. 屏蔽子网体系结构。利用两个路由器(内部路由器和外部路由器)将内部网络保护到更深一层,而在两个路由器之间形成一个虚拟网络,称之为周边网络,堡垒主机连接在周边网络上,通过外部路由器与外部网络相连。这样,如果入侵者突破了外层的防火墙,甚至侵入堡垒主机,内部网络依然安全。

2.2 电力企业信息网防火墙的结构设计

电力系统对安全性的高度要求,企业信息网络的安全问题应该予以格外关注。必须组建科学、严密的防火墙体系,为企业内部网络尤其是内部网络中的 SIS 子网提供高度的网络安全。

电力企业内部网络由两个安全级别不同的子网 MIS 和 SIS 构成,其中 SIS 对安全要求更高,因此它仅向 MIS 提供服务而不直接与外部网络相连,由 MIS 向外界提供服务。基于这个特点,防火墙宜采用屏蔽子网的体系结构,如图 2 所示。

MIS 作为体系中的周边网,SIS 作为内部网。设置两台屏蔽路由器,其中外部路由器设在 MIS 与外部网络之间,内部路由器设在 SIS 与 MIS 之间,对进出的数据包进行过滤。另外,堡垒主机连接在

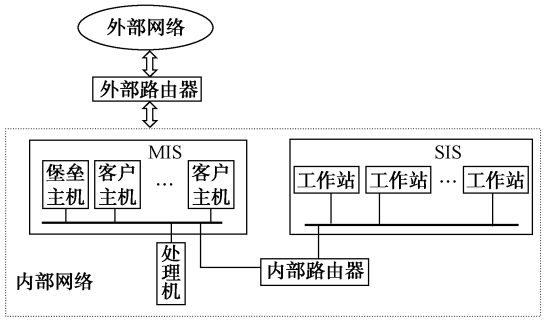

图 2 防火墙体系结构
Fig. 2 Structure of firewall system

MIS 中,对外作为访问的入口,对内则作为代理服务器,使内部用户间接地访问外部服务器。

应该强调的是,MIS 的堡垒主机极有可能受到袭击,因为所有对内部网络的访问都要经过它,因此,在条件允许的情况下,可以在 MIS 中配置两台堡垒主机,当一台堡垒主机被攻击而导致系统崩溃时,可以由另一台主机提供服务,以保证服务的连续性。同时,在 MIS 中配置一台处理机,与内部路由器组成安全网关,可以作为整个防火墙体系的一部分,控制 MIS 向 SIS 的访问以及对数据传输进行限制,提供协议、链路和应用级保护。网关还应考虑安全操作系统问题,Win2000[4]是一个可行的选择。尽管可能还存在一些潜在的漏洞,Win2000 依然是目前业界最安全的操作系统之一。由于 SIS 仅对 MIS 的固定用户提供服务,同时考虑到 SIS 的安全要求,对网关的管理可以采取 Client/Server 方式,这样虽然在实现上较 Browser/Server 方式复杂一些,但却具有更强的数据操纵和事务处理能力,以及对数据的安全性和完整性的约束能力。

2.3 防火墙的缺陷

尽管防火墙在很大程度上实现了内部网络的安全,但它的以下几个致命的缺陷使得单一采用防火墙技术仍然是不可靠的。

a. 无法防范病毒。虽然防火墙对流动的数据包进行严格的过滤,但针对的是数据包的源地址、目的地址和端口号,对数据的内容并不扫描,因此对病毒的侵入无能为力。

b. 无法防范内部攻击。从防火墙的设计思想来看,防范内部攻击从来就不是它的任务,它在这方面是一片空白。

c. 性能上的限制。防火墙只是按照固定的工作模式来防范已知的威胁,从这一点来说,防火墙虽然“勤恳”,但是过于“死板”。

所以,安装了防火墙的系统还需要其他防御手段来加以充实。

3 IDS

IDS(入侵检测系统)是一种主动防御攻击的新型网络安全系统,在功能上弥补了防火墙的缺陷,使整个安全防御体系更趋完善、可靠。

3.1 入侵检测原理与实践

IDS 以检测及控制[5]为基本思想,为网络提供实时的入侵检测,并采取相应的保护措施。它的设计原理一般是根据用户历史行为建立历史库,或者根据已知的入侵方法建立入侵模式,运行时从网络系统的诸多关键点收集信息,并根据用户行为历史库和入侵模式加以模式匹配、统计分析和完整性扫描,以检测入侵迹象,寻找系统漏洞。

IDS 一般分为基于主机的 IDS 和基于网络的 IDS 两种。基于主机的 IDS 其输入数据来源于系统的审计日志,用于保护关键应用的服务器;基于网络的 IDS 输入数据来源于网络的信息流,用于实时监控网络关键路径的信息。目前的入侵检测产品通常都包括这两个部件。

在实践中,IDS 一般分为监测器和控制台两大部分。为了便于集中管理,一般采用分布式结构,用户在控制台管理整个检测系统、设置监测器的属性、添加新的检测方案、处理警报等。监测器部署在网络中的关键点,如内部网络与外部网络的连接点、需重点保护的工作站等,根据入侵模式检测异常行为,当发现入侵时保存现场,并生成警报上传控制台。

3.2 在电力企业信息网中运用 IDS

电力企业的安全涉及国家安全和社会稳定,建议尽可能使用国产检测系统,如北京中科网威"天眼"入侵检测系统[6]、清华紫光 Unis 入侵检测系统等,这些产品在技术上已相当成熟,且在不断升级。

安装 IDS 的关键步骤是部署检测器与控制台。针对电力企业网络的特点,首先,可以在外部路由器与外部网络的连接处部署监测器(如图 3 所示),以监测异常的入侵企图。在防火墙与 MIS 之间部署监测器,以监视和分析 MIS 与外部网络的通信流。然后,分别在 MIS 和 SIS 中部署一台监测器,监视各子网的内部情况;控制台设置在 MIS 中。最后,根据实际情况为个别需重点保护的服务器、工作站安装基于主机的入侵检测软件,保护重要设备。

安装 IDS 后,更具挑战性的工作就是有效地运行 IDS。防火墙在测试和设置后便开始工作了,而 IDS 则不同。IDS 提供实时检测需要管理员"实时"地配合,管理员要做好处理各种警报的准备工作;在系统发出警报时要判断是否误报,正确处理警报,决定是否关闭系统或是继续监视入侵者以收集证据等,都需要管理员就地解决。只有管理员及时采取恰当的处理方法,才能真正发挥 IDS 的功效。

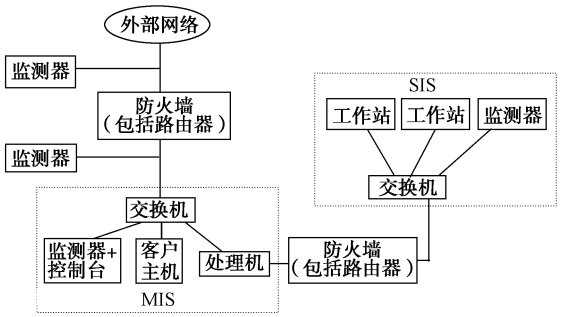

图 3 IDS 分布式布置

Fig. 3 Distributive disposal of IDS

4 安全体系的运作与后期扩充

虽然防火墙的防护是被动的,而 IDS 是实时的,但安全体系(包括各单一主机自身的安全体系)是作为一个整体协同运作的。目前的主机和网络设备都具有完备的安全审计功能,IDS 可以充分利用系统的网络日志文件作为必要的数据来源,而当 IDS 发现可疑行为时又需要其他主机或防火墙采取相应的保护措施,例如通知防火墙对可疑 IP 地址发来的数据包进行过滤等。

当然,从技术方面来说,网络安全所涉及的范围是相当广泛的,包括安全的操作系统、防火墙、安全审计、入侵检测、身份认证、信息加密、安全扫描、灾难恢复等。防火墙结合 IDS 只是形成了安全体系基本内容,还需要在系统运行中运用多种技术不断充实安全体系的功能,例如在系统中配置扫描器,定期进行风险评估和查找漏洞,升级防火墙或者向 IDS 中添加新的攻击方式等。同时,任何防御体系都不可能保证系统的绝对安全,必须不断提高系统管理人员的技术水平,密切关注网络安全的发展动态,及时升级网络防御系统,提高系统的防御能力。

5 结语

当前,电力企业正以原有设施为基础,构建企业与电力公司、企业与企业间的信息网络,网络安全是一个不可忽视的问题。防火墙与入侵检测技术相结合,为网络安全体系提供了一个良好的基础,对保障系统安全发挥不可忽视的作用。当然,完备的安全体系还需要其他多种安全技术从功能上进一步完善,同时,安全问题不仅是一个技术问题,也是一个系统工程,需从组织管理、法律规范等多方面予以支持。

参 考 文 献

1 侯子良(Hou Ziliang). 中国火电厂自动化发展趋势及对策(Developmental Trendency and Strategy for Automation of Thermal Power Plant in China). 中国电力(Electric Power), 1999, 32(10): 41～45

2 聂元铭(Nie Yuanming). 网络信息安全技术(Security Techniques of Network Information). 北京:科学出版社(Beijing: Science Press), 2001
3 杨守君(Yang Shoujun). 黑客技术与网络安全(Hacker & Internet). 北京:中国对外翻译出版公司(Beijing: China Translation and Publishing Corporation), 2000
4 Internet Security Systems: Windows 2K Support. http://documents.iss.net/whitepapers/windows2000security.pdf
5 金 波,林家骏,王行愚,等(Jin Bo, Lin Jiajun, Wang Xingyu, et al). 入侵检测技术评述(Commentary of Intrusion Detective Techniques). 华东理工大学学报(Journal of East China University of Science and Technology), 2000, 26(2): 191~197
6 中科网威"天眼"网络入侵侦测系统(Netpower NIDS). http://www.netpower.com.cn/jiejue/chanpin/4.htm

王先培(1963—),男,博士,副教授,研究方向为计算机网络及系统工程。E-mail: xpwang@wuhee.edu.cn
熊 平(1974—),男,硕士研究生,研究方向为网络安全。E-mail: pingxiong01@163.net
李文武(1975—),男,硕士研究生,主要研究网络安全。

APPLICATION OF FIREWALL AND IDS IN THE INFORMATION NETWORK FOR POWER ENTERPRISES

Wang Xianpei[1], *Xiong Ping*[1], *Li Wenwu*[2]
(1. Wuhan University, Wuhan 430072, China)
(2. Three Gorges University, Yichang 443002, China)

Abstract: How to guarantee the security of information network is a hot spot in the study of information network construction for power enterprises. The information network structure in a power enterprise and its requirements on the network safety are expounded. On the basis of what has been found about the functions of the firewall and the intrusion detective system (IDS) and according to the characteristics of the network, a detailed project for the application of firewall and IDS in the information network is proposed. Associated techniques and the development of the network security system are discussed.

Key words: power enterprise; firewall; intrusion detective system; information network for enterprises