Digital Library Forum 数字图书馆论坛
http: // www.dlf.net.cn

NSTL网络安全管理系统的设计与实现

□ 张婧 毕军荣 孙钦山/ 中国科学技术信息研究所 北京 100038
胡铁军 / 国家科技图书文献中心 北京 100038

摘要：文章基于国家科技图书文献中心（简称NSTL）网络服务系统的业务模式，针对网络和应用系统的安全管理提出了层次化分级防护的安全模型和配套的安全管理办法，并在此基础上设计、构建了NSTL网络安全管理系统。

关键词：网络安全，计算机网络，风险评估，网络服务系统
DOI：10.3772/j.issn.1673—2286.2010.10.011

1 引言

NSTL的千兆城域骨干网平台建设自2002年开始启动，利用位于中国科学技术信息研究所的NSTL网络管理中心至中科院文献情报中心、冶金工业信息标准研究院、机械工业信息研究院、中国化工信息中心、中国农科院科技文献信息中心、中国医科院医学信息研究所、中国标准化院标准馆、中国计量科学研究院文献馆的点对点裸光纤互联，建立了1000Mbps宽带光纤网络系统，实现了中心“统一网络，统一业务平台”，为实现文献信息资源共建共享的目标奠定了坚实的基础。同时，还建立了NSTL到国家图书馆、中国教育网（CERNET）、中国科技网（CSTNET）、中国工程技术信息网的点对点100Mbps裸光纤互联，以方便向全国的科技人员提供文献信息服务。

建设初期，NSTL千兆城域骨干网的安全防护单一，中心网络平台与成员单位本地网之间边界模糊，已有网络硬件设备和管理措施无法有效应对NSTL网络系统和其服务系统所面临的网络安全威胁，不能满足国家计算机等级保护二级安全防护等级的要求。

为此，中心提出要对现有网络基础架构和网络安全进行适应性改造。经过有关专家论证，2008年12月科学技术部批准了NSTL网络安全管理集成项目启动实施。实施安全管理项目后的网络见图1。

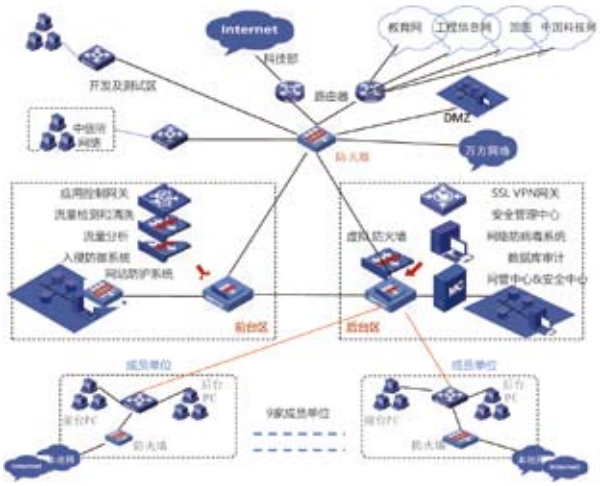

图1 NSTL网络结构示意图

2 加强安全管理的必要性

2.1 适应国家信息安全规范的需要

根据国家《信息系统安全等级保护定级指南》的规定，NSTL应用系统的业务信息和系统服务的安全等级均被定为二级。按照国家“信息安全技术-信息系统安全等级保护基本要求”，NSTL网络系统必须在结构安全、边界防护、访问控制、安全审计、入侵防范和

网络设备防护等方面满足二级等级保护所规定的基本要求。

2.2 建设国家科技文献信息战略保障平台的需要

提供方便快捷的网络信息服务，逐步建设成为一个在国内具有权威性，在国际上具有一定影响力的现代科技文献信息服务中心是NSTL的目标。NSTL网络文献信息服务系统及丰富的科技文献信息资源，已成为国家科技创新体系的重要支撑环境和基本保障条件。加强NSTL网络系统的安全管理对于充分发挥科技文献信息资源这一国家的战略资源的效益，确保满足当前和长远科技创新发展的需要，构建国家科技文献信息战略保障平台，具有重要意义。

2.3 应对国内外网络共同威胁的需要

网络安全形势日益严峻，威胁无处不在，网络攻击手段日新月异。孤立地解决特定安全问题的防范措施已无法应对目前NSTL所面临的网络安全威胁，迫切需要建立一个以应用为导向、以管理为基本手段、以技术作为重要支撑的新型网络安全防护体系。

3 网络安全技术和遵循的标准规范

3.1 网络安全技术的最新进展

经典网络安全技术的基本特点是从网络安全威胁出发，有针对性地解决网络安全问题。大致归为以下几类：防火墙技术；检测、扫描技术；密码和认证技术；虚拟专用网技术；监控、审计和信息过滤。这些网络安全技术对于威胁的多样性和不断变化的特性有明显的局限性。从网络系统业务出发、以管理和监控作为核心手段、经典网络安全技术为重要补充的网络安全技术和方案已经成为现实。

下一代网络安全技术既吸纳了传统网络技术中最精华的部分，也发展了大部分有价值的方法，同时又创新了许多新的问题解决思路。从网络系统的业务和结构特点出发，以综合增强网络系统的安全性能为目标是下一代网络安全技术解决网络安全问题的基本思路。下一代网络安全技术体系包括图2所示的几个不同

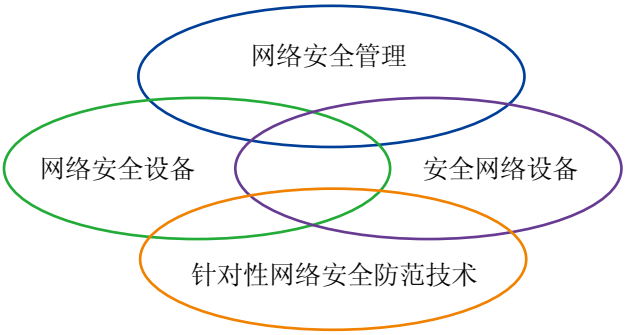

图2 网络安全技术体系

的基本方法。

这四类不同解决网络安全的技术代表了四类相辅相成的不同思路，即网络安全设备技术、安全网络设备、针对性网络安全防范技术、网络安全管理，而网络安全管理是下一代网络安全技术的核心。

3.2 网络安全标准

目前，国际上通行的网络和信息安全有关的标准可分为三类，如图3所示。

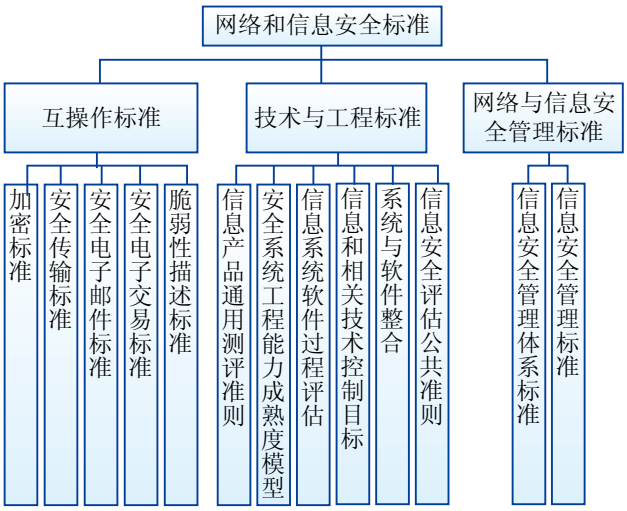

图3 网络和信息安全相关标准

网络与信息安全管理标准主要包括两个：信息安全管理体系标准（BS 7799，其中第一部分称为ISO/IEC 17799）和信息安全管理标准（ISO 13335）。

国内标准主要是《信息安全技术信息系统安全等级保护基本要求》。信息安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法。开展信息

安全等级保护工作是保护信息化发展、维护国家信息安全的根本保障。实施信息安全等级保护制度，使各单位、各部门能够按照标准进行安全建设、整改，使信息系统安全与否有了衡量标准。

4 NSTL网络安全管理的技术路线和实施方案

4.1 加强NSTL网络安全管理的目的和任务

根据公安部《信息系统安全等级保护定级指南》的规定和“信息安全技术信息系统安全等级保护基本要求”，在充分了解NSTL网络系统应用现状，进一步明确存在的主要问题的基础上，结合国内外网络安全发展趋势，采用目前最新成熟的网络安全管理技术，本着基于标准、依托风险评估、整体规划设计理念，贯彻集中管理、重点保护、规范可控、投资保护、注重效益的基本原则，在网络管理、入侵检测、病毒防治和对接入设备可实施严格监控等多层次上，实现NSTL网络系统安全控制和规范管理，努力将NSTL网络服务系统及其应用系统打造成为更加安全可靠的网络运行平台。

4.2 加强NSTL网络安全管理的技术路线

加强NSTL网络安全管理，实现NSTL网络系统安全和规范控制，必须在厘清NSTL网络系统边界、建立前后台系统有别层次化安全防护体系、实现集中防护、因特网出口严格限控、发挥现有设施功能等方面着手，因此，NSTL网络系统安全管理解决方案的技术路线是：

1）按照前后台有别的思路，将NSTL网络系统划分为外网、前台和后台三个垂直的、不同安全等级的安全平面。

2）NSTL网络系统与外网用防火墙实施隔离，实现安全的网络访问和应用传输，以及高级的应用控制。

3）通过VPN技术构建异地业务平台网络，使外网工作用户利用SSL VPN经过NSTL网络系统Internet入口访问后台资源。

4）将NSTL网络系统内所有的桌面机和服务系统分为前后台两个安全平面，前台桌面限制对NSTL网络系统的访问范围，严格控制后台桌面对NSTL网络系统的接入和安全威胁。

5）前台、后台安全平面分别部署在两台经过安全加强的核心交换机上。在后台安全平面实现内部业务系统逻辑隔离，并且保证在策略允许的情况下实现可控的互访，利用防火墙模块与后台核心交换机的集成实现后台核心交换机的功能扩展，充分利用二层VLAN隔离、三层ACL控制/策略路由、虚拟防火墙应用隔离等技术手段，实现不同安全区域业务之间的可控互访。

6）后台终端安全和桌面管理：利用网络准入解决方案，保证接入NSTL网络系统后台网络的终端符合NSTL网络系统的入网健康检查、集中防病毒要求和用户身份认证条件，利用终端控制软件对终端进行安全加固、病毒零天保护、限制非法应用等操作，与网络安全威胁主动应对技术进行横向联动，自动拦截来自体系内的网络威胁和攻击。

7）部署集中管理的防病毒服务器，提高前、后台桌面机防病毒能力。

8）对后台服务系统的业务主机进行内核加固。

9）前台增加传统的安全设施，入侵防护、流量分析、DDoS检测和防护过滤，用于统计和过滤访问前台业务服务系统的网络流量。

10）主动安全响应系统可随时获取全网范围内的所有报告，进行智能的关联和分析，指出当前正在发生的攻击路径，给出响应方案，对攻击进行拦截和阻断。

4.3 建立前、后台有别的网络模型，实现层次化的安全保护体系

按照前后台区分的原则，NSTL网络系统划分为三个安全平面：外部安全平面、前台安全平面和后台安全平面。三个安全平面利用防火墙技术进行有效的逻辑隔离。三个安全平面和内部安全域的逻辑关系如图4所示。

外部安全平面是指NSTL网络系统以外的网络，其相对于NSTL网络系统而言，是不可信任的区域，网络安全威胁非常大，其对NSTL网络系统的访问设定为个别IP地址和固定服务端口。

位于外部安全平面的工作用户在经过用户身份认证通过后利用SSL VPN访问受控的后台服务器资源。

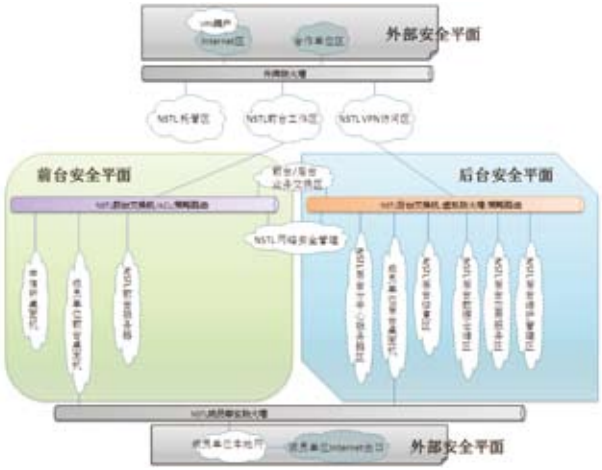

图4 NSTL网络系统三个安全平面和内部安全域的逻辑关系

后台安全平面主要是NSTL进行文献加工服务的桌面机和服务器，其在NSTL网络系统内被严格管理，受控于集中的网络安全策略。后台服务器被安全加固和禁止主动访问因特网，后台桌面机在终端安全控制之下可以通过本地网络因特网出口访问Internet和限制性访问前台安全平面内的服务器。

其余的桌面机和服务器都被放置在前台安全平面内。前台服务器被禁止主动访问因特网，其与后台服务器的通信和业务交换受到严格限制。前台桌面机只能限制访问本安全平面内的服务器，可以通过本地网络因特网出口访问Internet。

各成员单位本地网络可以利用NSTL网络系统访问NSTL前台服务器的指定资源。

4.4 加强NSTL网络安全管理的关键技术

4.4.1 DDoS的检测与过滤技术

随着DDoS攻击的危害性越来越大，而传统的防护方法不可避免的局限性，目前的DDoS攻击防护技术主要有以下两类：基于传统识别的防护技术和基于MVP技术的数学模型技术。

1) 基于传统识别的防护技术

主要是从防火墙技术和内容交换机技术演变而来。它主要采用串行模式，所有流量通过该设备，对通过流量的分析来判断攻击流量，并将攻击流量直接丢弃。

2) 基于MVP技术的数学模型技术

在DDoS攻击防御中，最关键的技术是如何分辨合法业务流量和恶意业务流量。Multi-Verification Process architecture技术是专门针对DDoS攻击的独特的、申请专利的多验证过程技术，就是将各种验证、分析和实施技术结合在一起，用来从合法业务中识别和分离恶意业务。

NSTL城域网构建了从网络层到应用层多种DDoS攻击方式的防御体系，可以有效应对IP碎片攻击、TCP半连接攻击、HTTP空连接攻击等攻击方式。同时，为应对未知的DDoS攻击方式，通过对NSTL网络日常流量进行学习、统计和阈值调整，生成网络基线流量。在DDoS攻击检测时，通过实时流量统计与基线流量进行比较，对异常流量进行识别、标识，并作进一步分析和防御。图5是NSTL所采用的网络流量清洗系统记录，图中蓝色为正常流量。

图5 网络流量实时记录

4.4.2 网络安全运行趋势的分析和响应技术

为对网络中的异常流量进行检测，首先需要对网络中不同类型业务的正常通信进行基线分析，包括测量和统计不同业务日常的流量和流向数据并计算基线的合理范围。为了识别、管理和应对安全威胁，必须集中汇聚来自多种不同的常见网络设备的日志和事件（如路由器、交换机）、安全设施的日志和时间（如防火墙、入侵检测、漏洞扫描和防病毒系统）、操作系统的系统日志、应用的日志以及Netflow的数据。这个数据收集就是网络安全监控、分析和响应系统的功能之一。

所有设施的日志都表示了网络中的流量，由于网络安全监控、分析和响应系统在较高的颗粒度水平上来描述网络简况，它提供了网络安全方面所需要的全部智能，可以轻松提供某个安全事件的全部上下文——被感染的来源、目的地端口等。它可以发现攻击的来源，最重要的是，可以找到制止攻击的位置和方法。

NSTL部署的安全管理中心对收集到的事件可进行高度聚合存储及分析，实现实时安全状况监视信息、安全事件关联分析、实时告警等实时信息显示等功能。通过它网络安全管理人员能够迅速地获得正在进行的大规模攻击的有力证据，及时制止攻击并防止进一步的破坏，从而提升攻击防护能力。

5 网络安全组织与管理

管理制度是网络和信息安全的保障，为了保证NSTL城域网和应用系统的安全，统一协调各成员单位间的业务工作流程，提升服务质量，必须具备完善的管理规章制度。为此，中心成立了管理办法起草工作组负责该项工作，工作组对办法的体例和内容进行了深入调研并广泛征求成员单位的意见，最终确定了《国家科技图书文献中心网络服务平台安全管理办法》，其内容涵盖了物理设备、网络、主机、应用系统、人员、工作流程和术语等多个方面，使NSTL各项工作开展有章可循，业务分工明确，管理办法具有可操作性。

6 实施NSTL网络安全管理后的效果

安全管理项目的实施使NSTL城域网、业务系统和应用服务系统防护能力比过去有了质的提升，实现了多层次的安全控制和规范管理。

安全评估的结果认为：NSTL网络安全管理系统根据自身的业务逻辑进行安全分区，针对每个区域设定了不同的安全策略，实现了各区域不同级别、不同层次的安全保障，初步建立起边界清晰、前后台系统有别的层次化的NSTL网络系统安全防护体系，提升了整体安全防护能力，实现了后台工作系统的集中管控，确保了后台工作系统服务器的安全加固，建立了可实现智能检测、主动防范 、集中有效的一体化网络安全管理中心，完善并加强了NSTL网络系统安全管理制度、流程和运行机制，能够保障核心业务系统和应用服务系统的安全、稳定运行，也符合 “信息安全技术-信息系统安全等级保护基本要求”规定的二级安全防护等级规范。

参考文献

[1] 思科系统网络技术有限公司. 下一代网络安全[M]. 北京:北京邮电大学出版社,2006.
[2] 吴亚非,李新友,禄凯. 信息安全风险评估[M]. 北京:清华大学出版社,2007.
[3] 陈道泉. 建设发展中的国家科技图书文献中心——新系统、新功能、新服务[C]// 全国网络环境下信息资源共享学术研讨会. 情报学报,2003,22.
[4] 张志平. 国家科技图书文献中心网上共建共享系统的建设实践[C]// 全国网络环境下信息资源共享学术研讨会,2003.

作者简介

张婧，毕业于北京大学图书馆学系。NSTL网管中心高级工程师。通讯地址：北京市复兴路15号 100038。E-mail: zhangj@istic.ac.cn
胡铁军，国家科技图书文献中心研究员，通讯地址同上。Email:hutj@nstl.gov.cn
毕军荣，中国科学技术信息研究所。NSTL网络管理中心高级工程师。通讯地址同上。E-mail: bjr@istic.ac.cn
孙钦山，中国科学技术信息研究所情报学专业研究生，NSTL网管中心工程师。通讯地址同上。E-mail: sunqs@istic.ac.cn

The Design and Implementation of NSTL Network Security Management System

Zhang Jing / Institute of Scientific and Technical Information of China, Beijing, 100038
Hu Tie Jun / National Science and Technology Library, Beijing, 100038
Bi Jun Rong / Institute of Scientific and Technical Information of China, Beijing, 100038
Sun Qin Shan / Institute of Scientific and Technical Information of China, Beijing, 100038

Abstract: Based on the business model of National Science and Technology Digital Library (NSTL) network service system, multitier security protection model and management regulations are proposed which is used for network security and application security. NSTL network security management system is designed and constructed utilizing this model.

Keywords: Network security, Computer network, Risk assessment, Network service system

（收稿日期：2010-08-30）