DOI:10.13954/j.cnki.hdu.2005.05.011

网络安全体系结构的设计与实现

王秋华,章坚武,骆 懿
(杭州电子科技大学通信工程学院,浙江 杭州 310018)

摘要:随着计算机网络的发展,网络安全也已成为网络建设的重大对策问题。该文首先说明网络安全的必要性,并在所提出的一种网络安全系统设计框架的基础上,对其中的网络安全体系结构设计与实现进行了详细的分析,给出了体系结构模型和策略管理执行模型,详述了其设计过程,把安全体系结构、安全策略管理的实现和网络安全的实现机制有机地结合在一起,保证从高级安全策略向网络安全实现机制的平滑过渡。

关键词:网络安全;体系结构;安全策略;安全设计
中图分类号:TP393.08 文献标识码:A 文章编号:1001-9146(2005)05-0041-04

0 引 言

随着计算机网络的不断发展,全球信息化已成为人类发展的大趋势,但由于计算机网络具有联结形式的多样性,终端分布的不均匀性和网络本身的开放性、互连性等特征,致使计算机网络易受黑客、恶意软件和其它不法行为的攻击,网络入侵和网路攻击层出不穷,网络安全已成为网络建设的重大对策问题,如何确保网络系统的安全,如何构建一个坚实的网络安全体系已成为网络系统设计人员和管理人员的重要任务和职责。

1 网络安全体系框架的介绍

通常网络安全系统设计的过程分4步,如图1所示。

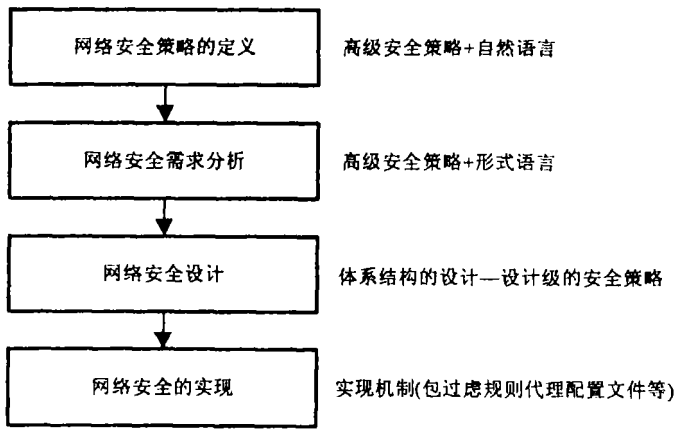

图1 网络安全系统设计框架

首先是基于方针手册如ISO/IEC 17799标准[1]的文档化的高级安全策略和控制的基础上,对安全需

收稿日期:2005-05-08
作者简介:王秋华(1978-),男,山东聊城人,硕士,网络安全技术.

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

求规范进行形式化，然后再对组成系统的几个执行机制进行具体的设计与实现。但是从高级安全需求到实现它们的执行机制之间却有差距：安全设计者从一个高级策略描述直接到复杂系统的实现，有些组件有时在它们的配置中有完全不同的特性。这将会导致不正确执行所需的安全策略，从而造成安全漏洞和非常危险的安全失误。

1.1 网络安全策略的定义

第一步是网络安全策略的定义，它是对网络安全策略进行详细描述。目的在于为网络安全提供管理和支持，网络安全系统必须与其它领域一起考虑，如物理安全、人员安全、操作安全、通信安全和社会机制。这个通常根据向导手册 ISO/IEC 对企业进行风险分析来完成。这一步最后的结果是由自然语言描述的网络安全策略和控制的文档，称其所产生的安全策略为高级的安全策略。

1.2 网络安全需求分析

第二步是网络安全需求分析，它是对上一步高级安全策略的形式描述，从而获得高级形式安全策略。对高级安全策略的形式化描述有几个优点，如通过分析可以检查策略之间的冲突，同时还可以消除自然语言中高级策略比较含糊的描述。Leiwo 和 Zheng[2] 曾经提出用形式化的方法处理高级安全策略的框架，在该层中允许冲突监测和协调分析。

2 网络安全设计

第三步网络安全设计，其主要目标就是把网络安全系统模型中高级形式安全策略转换为系统设计级的执行机制。这一步分为体系结构的设计和安全策略的设计与实现，是本文的重点。

2.1 网络安全体系结构的设计

根据上一步的安全需求有针对性地构建适合自己的安全体系结构，从而有效地保证网络系统的安全。体系结构设计的目的是建立网络安全系统的全面结构，它是通过提出几个组件以及构建这些组件的技术来完成的。根据OSI参考模型中各层之间的相互依赖性，以及安全的需求的全面性，把安全在逻辑上分配到体系结构的各个层，如图2所示。

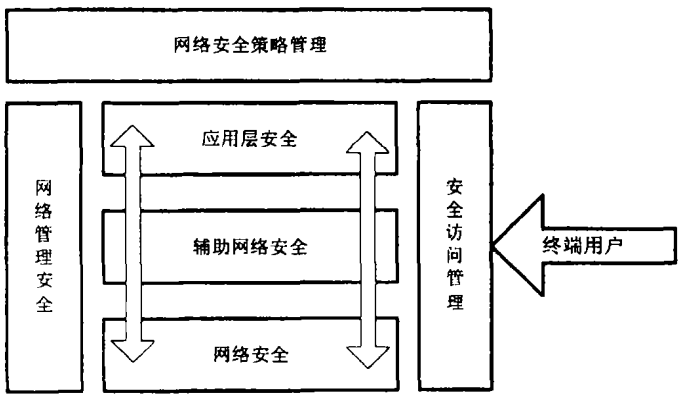

图2 网络安全体系结构

网络安全层：它提供 OSI 模型中一到三层的安全功能（物理、数据链路和传输层）。

辅助网络安全层：它提供 OSI 模型中四到七层的安全功能（网络层到应用层），在网络安全层上增加安全。

安全应用层：它提供 OSI 模型中第七层（应用层）的安全，包括服务器和存储平台上的安全。

访问列表和 VLANs，只在网络安全层操作。防火墙既在网络安全层，也在辅助网络安全层操作。SSL 可以在网络辅助层或应用安全层实现。如表1所示，普通的安全技术怎样映射到图2的安全体系结构中。

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 1　安全技术在安全体系结构中的映射

安全功能	网络安全层	辅助网络安全层	应用安全层
L2 第二层的 VPN，EAP，端口安全	Yes		
NAT 网络地址解析	Yes		
ACL 访问控制列表	Yes		
Ipsec Ipsec 加密	Yes		
SRT 安全动态路由	Yes		
FW 防火墙	Yes	Yes	
IDS 入侵监测系统		Yes	Yes
SSL SSL 加密		Yes	Yes
CF 内容路由		Yes	Yes
VS 病毒扫描		Yes	Yes

2.2　网络安全策略的设计与实现

网络安全体系结构设计中的第二步是安全策略的设计与实现, 其目的是对一套设计级安全策略的定义, 这些策略是框架底层的抽象策略, 它的特性更接近于技术执行。, 由于组织和部门的计算机网络的配置可能经常变化, 它们对安全的需求也会发生变化, 因此网络安全是一个动态的过程, 组织的安全策略也需要经常进行相应的调整。一个适当的设计和执行安全策略是所有企业的需求, 它应是一个现存的文档和过程。它被执行、实现和升级, 来反映企业的基础组织和服务需求中的最新变化。安全策略必须在企业中清楚地识别有风险的资源, 并给出缓解威胁的方法。这个策略定义用户中哪个用户或组可以访问哪种资源, 它必须定义审计跟踪的用户, 以帮助识别和发现侵害并给出适当的响应。

安全策略管理包括安全组件的全部领域, 如防火墙、IDS、访问列表和路由器、认证技术等。安全体系结构中策略管理实现的参考模型如图 3 所示。它是基于 IETF 安全体系框架中的 RFC2753 策略管理[3]。在这个模型中策略管理在整个网络中执行, 包括所有的安全级(应用安全层, 辅助网络安全层和网络安全层), 它对所有用户和应用都适合。

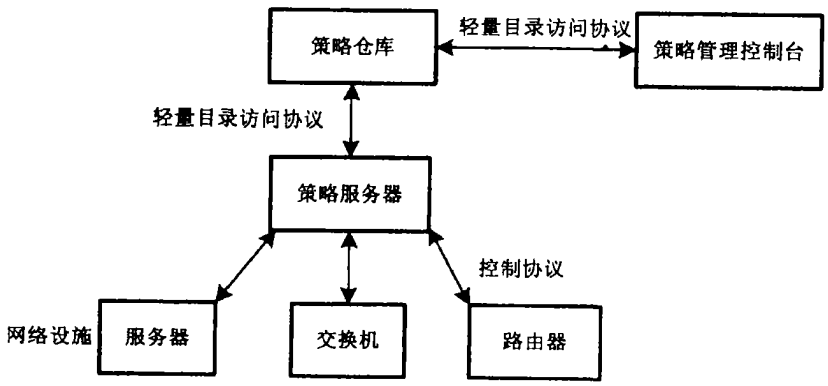

图 3　网络安全策略管理实现模型

策略管理功能主要包括策略仓库, 策略决定点和策略实现点。

策略仓库存储一个网络目录中的所有策略信息。它描述网络用户、应用、计算机和服务, 以及这些实体之间的关系。这个策略仓库通常在运行于 Unix 或 WindowsNT/2000 上的专用数据库上执行, 它通过策略服务器由轻量目录访问协议访问。

策略决定点或策略服务器把网络策略抽象成详细的策略控制信息, 然后再传给策略执行点。这些策略服务器经常运行于 Unix 或 WindowsNT/2000, 在一个管理域中控制交换和路由, 它们用控制协议(如: COPS, SNMP, 或 CLI)与这些设备通信。

策略实现点是一个网络或安全设备, 它从 PAPs 接受策略(配置规则)。

公共开放策略服务是一个简单的请求－应答基于 TCP 的协议, 它在 PDP 和它的客户——PEPs 之间交换策略信息。这在 RFC2748[4] 中有详细的说明。COPS 依赖 PEP 与主要的 PDP(当主要的 PDP 不可达时, 用第二个 PDP)一直建立连接。一个 COPS 代理装置可把来源于策略服务器的 COPS 信息翻译成 SN-

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

MP 或 CLI 命令。

策略管理控制台通常运行在个人计算机或工作站上,它对策略管理系统提供人机接口。

3 网络安全的实现

第四步网络安全的实现就是通过一些实现机制来实现网络安全。在图 2 的安全体系结构中,网络安全管理运行在服务器和工作站上,利用网络级和网络辅助级上的安全,由应用级的安全来实现。网络操作者是一些特殊的用户,他们是有更严格的认证和授权程序的主体。由于网络管理人员有更大的访问授权和功能权限,他们的访问和行为必须确保安全,以保护网络的配置、性能和存活能力。越开放的企业和越集中的网络管理系统,对网络管理的过程就有更迫切的安全需求。

安全的网络管理需要一个整体的方法,在安全体系结构中网络安全的实现机制包括以下几个主要的领域:安全行为记录,网络操作认证,网络操作授权,加密,安全远程访问,隔离网络的防火墙和 VLANs,入侵监测,主机加固和反病毒保护。

安全行为记录对用户或管理员的行为以及由网络设备产生的事件提供可作证的审计跟踪。网络操作者认证基于集中管理和口令的执行,从而确保只有授权的操作者获得系统管理的访问权限。网络操作者的授权用认证的身份来确定用户的访问权限——他们可以访问什么系统,可以实现什么功能。网络管理事务的加密保护网络管理数据的机密性和完整性,加密对内部和外部的威胁提供高度的保护。操作者的安全远程访问:应用 IPsec 提供一个安全的 VPN 是强制的解决方案,因为这将对所有的远程操作者提供有力的加密和认证。防火墙和 VLANs 把网络分开进行隔离管理。入侵检测系统组成的管理服务器通过提示管理员潜在的不安全因素(如服务器妥协和拒绝服务的袭击)来保护网络。

4 结束语

文中在所提出的网络安全系统设计框架的基础上,细化了网络安全的设计过程,给出了安全体系结构模型和策略管理执行模型的设计与实现,把安全体系结构、安全策略管理的实现和网络安全的实现机制有机地结合在一起,从而实现了从高级安全策略向网络安全实现机制的平滑过渡。

参考文献

[1] ISO/ IEC 17799:2000. Information technology—code of practice for information security management[S]. International Organization for Standardization, 2000.

[2] Leiwo J, Zheng Y. A Framework for the Management of Information Security[A]. Ishikawa. Information Security — Proceedings of the 1997 Information Security Workshop (ISW'97)[C]. Japan: Springer — Verlag, 1998, 232 — 245.

[3] RFC 2753, A Framework for Policy — based Admission Control[S]. 2000.

[4] RFC 2748, . The COPS (Common Open Policy Service) Protocol[S]. 2000.

[5] Porto J, Geus P L D. A Framework for Network Security System Design[A]. Rio de Janeiro, Brazil. 2002 WSEAS International Conference on Information Security, Hardware/ Software Code sign, E—Commerce and Computer Networks[C]. 2002.

The Design and Implementation of Network Security Architecture

WANG Qiu-hua, ZHANG Jian-wu, LUO Yi

(*School of Communication Engineering, Hangzhou dianzi University, HangZhou Zhejiang* 310018, *China*)

Abstract: With the development of computer network, network security has also become an important issue. The necessary of network security was first developed and based on a framework for network security system design put forwarded, detailed analysis of the phase of network security design is made in this paper, and architecture model and policy management implemented model and process of design are given, which hangs security architecture, security policy implement and the enforced mechanism of network security together, and insures the transition between high—level ecurity requirement analysis and the low—level system implementation smoothly.

Key words: network security; architecture; security policy; security design

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net