<<网络设备安全与防火墙>>

图书基本信息

书名：<<网络设备安全与防火墙>>

13位ISBN编号：9787810823562

10位ISBN编号：7810823566

出版时间：2005-3

出版时间：清华大学出版社/北京交通大学出版社

作者：杨富国 编

页数：341

前言

最近几年，网络逐渐渗透到社会生活的方方面面。
人们在网上查洵信息，企业在网上发布信息，而政府则在网上公开信息。
这一切的一切，都预示着在不远的将来，网络的使用将同电话一样普遍。
随着网络技术的发展，出现厂越来越多的网络设备。
与此同时，也出现了越来越多的网络安全问题。
这些安全威胁极大地损害丁人们对互联网的信心，从而影响了Intcmct更大作用的发挥。
因为没有有效的安全保护，很多企事业单位放缓了将部分业务或服务转移到网上的步伐，极大地降低了工作效率。
因此，如何能够为奉组织的网络提供尽可能强大的安全防护就成为各企事业单位的关注焦点。
为了解决网络安全问题，需要使用一种被称为“ 防火墙 ”的安全设备。
防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。
它是不同网络或网络安全域之间们息的惟一出入口，能根据企业的安全策略控制（允许、拒绝、监测）山入网络的信息流，日本身具有较强的抗攻占能力。
它是提供信息安全服务、实现网络和信息安全的基础设施。
除了防火墙之外，本书也对其他一些网络安全设备进行了介绍。
因为最近几年是政府和企业仁网的重要时期，内外网的安全管理是一个很重要的问题，所以网络的物理隔离技术也是本书的一个重点。
当然，一些网络设备自身也设计了相应的安全模块。
但无论从功能上还是从作用上，都不能和防火墙相比。
因此，本书从防火墙的基本概念、没汁与实现、使用与维护等各方面对防火墙知识进行了详尽的阐述。
最后，本书还对当前一些著名的防火墙产品做了具体的介绍。
本书的组织结构　本书在逻辑上分为两个部分，前半部分主要介绍网络设备的安全问题，而后一部分则主要介绍防火墙的相关知识。
读者可以根据自己的需要，选择阅读相关的章节，如果对前面的内容很熟悉，可以跳过这些内容进行选择学习。
第1章主要概述了计算机网络的发展和安全缺陷，同时还探讨了网络系统结构的复杂性.最后给出了对网络复杂性的控制办法。
第2章是对网络设备和系统的安全性分析。
本章首先介绍了国际、国内的一些安全事件，然后具体描述了设备、系统漏洞及黑客的攻击方法，最后给出了网络设备的安全管理方法和策略。
第3章主要介绍了网络设备安全的物质基础，分别介绍了网络传输媒介、局域网物理设备和拓扑结构，以及广域网结构。
第4章主要讨论网络协议的安全性，分别介绍了网络基本协议、地址转换协议、路由协议、应用协议及它们的安全性。
第5章主要介绍了物理网络隔离技术及其设备。
本章首先给出了物理隔离的定义和现实意义，接着分别讨论了几种物理隔离技术，然后探讨了物理隔离技术的解决方案，最后是对物理隔离技术的展望。

<<网络设备安全与防火墙>>

内容概要

本书从介绍因特网的安全问题入手，讨论了网络中各种设备的安全问题和黑客攻击方法，随后介绍了网络协议的安全性。
针对政府和企业上网问题，详细讨论对内部网络和外部网络进行安全控制的物理/逻辑隔离技术，并提供了多种解决方案。
本书还对常用的网络设备及防火墙产品的安全特性进行了全面而系统的介绍。
通过阅读本书，不仅可以深刻理解网络设备的防火墙的安全机制，还可以掌握对常用网络设备（例如Cisco路由器、交换机——的安全配置方法，并了解当前流行的防火墙系统的安全特性和功能。
这是一本理想的进行网络设备安全配置和防火墙安全管理的实用参考书。

<<网络设备安全与防火墙>>

书籍目录

第1章 概述　1.1 计算机网络的发展　1.2 计算机网络的安全缺陷　1.3 计算机网络的复杂性　1.4 对网络复杂性的控制第2章 网络设备和系统安全分析　2.1 网络安全事件　2.2 设备安全分析　2.3 系统安全分析　2.4 黑客攻击方法　2.5 网络系统安全策略第3章 网络设备安全技术基础　3.1 网络传输媒介　3.2 网络物理设备　3.3 广域网设备第4章 网络协议的安全性　4.1 网络基本协议和安全性　4.2 地址转换协议和安全性　4.3 路由协议　4.4 应用协议第5章 物理网络安全隔离技术及设备　5.1 什么是物理隔离　5.2 实现物理隔离中的问题　5.3 单机物理隔离技术　5.4 其他物理隔离技术　5.5 远程安全传输方式　5.6 安全网闸　5.7 内外网信息安全转发系统　5.8 物理隔离解决方案　5.9 物理隔离技术的展望第6章 接入服务器的安全管理　6.1 接入服务器　6.2 接入服务器的功能模块　6.3 设备的功能要求　6.4 接入服务器的业务　6.5 常见的接入服务器的产品——Quidway系列以太网接入服务器　6.6 接入服务器的安全第7章 交换机的安全管理　7.1 多层交换技术　7.2 VLAN及其安全性　7.3 典型交换机的安全管理　7.4 生产交换机的厂商　7.5 第三层交换机的选择第8章 路由器　8.1 路由器的发展　8.2 路由器的原理　8.3 路由器的管理　8.4 路由器的安全　8.5 路由协议设置　8.6 服务质量及访问控制　8.7 虚拟局域网（VLAN）路由第9章 防火墙概述　9.1 背景　9.2 什么是防火墙　9.3 防火墙的职责和局限性　9.4 防火墙技术的发展　9.5 防火墙的分类　9.6 专用术语第10章 防火墙的设计与实现　10.1 相关标准　10.2 防火墙的需求　10.3 防火墙的体系结构　10.4 防火墙中使用的安全技术　10.5 其他相关技术　10.6 高速防火墙技术　10.7 防火墙开发　10.8 防火墙的测试与评估第11章 防火墙的使用与维护　11.1 网络环境及风险分析　11.2 防火墙的选择　11.3 防火墙的部署　11.4 防火墙安全策略的制定　11.5 防火墙的运行维护　11.6 典型应用案例第12章 防火墙产品介绍　12.1 Firewall-1防火墙　12.2 NetScreen系列防火墙　12.3 FortiGate系列防火墙　12.4 Cisco PIX系列防火墙　12.5 WatchGuard防火墙　12.6 3Com的嵌入式防火墙系统　12.7 CyberwallPLUS防火墙　12.8 诺基亚硬件防火墙参考文献

章节摘录

2.2.2 交换机的安全问题 无论是在企业内部还是超越企业的边界，因特网都显著地扩充了对信息传输的需求。
目前，业界对Intrfmet的主要信息部件即服务器的关注往往很多。
在过去几年里，服务器的数量显著地增加了，但网络的基础设施却没有足够的变化，不足以支持这种增长以及随之而来的对控制能力的需求。
Intranet所具有的“任意到任意”的数据流量打破了传统的工作组子网流量模式。
局域网交换机对提高网络性能产生了很大的帮助，但是有些机构往往出于政治或者经济原因而无法自由地将网络限制在第二层，从而利用交换的好处。
路由提供了必要的控制方面的隔离，但它也成为最主要的也是代价最高的瓶颈。
结果。
服务器的采用与网络的层次结构有关，限制了Intranet初衷所想提供的自由。
其他问题也开始出现。
所有的用户都被赋于相同的网络访问权限，而不考虑他们的重要程度或桌面计算机的速度。
网络不能为特殊的用户或服务器分配更高的优先级。
高优先级的事务和应用必须给予更大的网络访问权限。
网络管理员要求在不损害性能和安全的前提下提供流量的优先化处理及服务质量的保证。
由此，逐渐提出了二层交换机和三层交换机，并提供了vuN等既可以满足用户快速通信的需要，又具有一定的安全性的技术方法。
2.2.3 路由器的安全问题 路由器作为内外网之间数据通信的核心设备，其本身的安全性能的重要性不言而喻，由于作为网络转接设备的路由器，需要不断接收与发送路由信息及IP数据报，而路由信息与敏感IP数据报的安全正是网络安全防护的核心。
因此，强化路由器本身的安全防范往往可以收到事半功倍的作用。
基于这一理念而出现的新型网络设备——安全路由器已经成为网络安全产业中的一支尖兵。
针对网络潜在的各种安全威胁，安全路由器在实现常规路由功能的基础上，在设计时强化了数据传输加密这一关键技术问题，增强了信息保护与数据加密性能，能够有效检测及防范各类攻击事件的发生。
L安全路由器 实际上，安全路由器只是一个松散的产品概念，并没有严格的范围界定，它通常是指集常规路由与网络安全防范功能于一身的网络安全设备，有一部分安全路由器产品甚至完全是通过在现有常规路由乎台之上加装安全加密卡，或相应的软件安全系统而来的。
一般说来，具备IP Set（IP Security）协议支持、能够有效利用IPSec保证数据传输机密性与完整性或能够借助其他途径强化本身安全性能的路由器都可以称之为安全路由器。

<<网络设备安全与防火墙>>

版权说明