<<网络工程师必读>>

图书基本信息

书名：<<网络工程师必读>>

13位ISBN编号：9787121083365

10位ISBN编号：7121083361

出版时间：2009-8

出版时间：电子工业出版社

作者：王达

页数：749

字数：1382400

前言

朋友，你是否正有打算朝着网络安全工程方面发展，成为一名当前国内外最热门又最紧缺、最有发展前景的IT职业人士——网络安全工程师呢？
你是否正为没有系统的网络安全系统设计方面的权威指南而发愁呢？
本书或许是您很好的选择。

本书是目前国内IT图书市场中第一本真正从设计角度系统地介绍网络安全系统设计和综合方案的图书。
本书最大的特点就是深入、系统地介绍了许多目前主流应用的网络安全技术体系架构和功能实现原理，如Kerberos、证书和证书服务、IPSec、TLS/SSL等。
可能有许多读者对深奥的理论不感兴趣，在笔者所接触的网友中，的确有许多网友是这样的，只喜欢实操型的书籍。
如果作为网络管理员，这可以理解，但是如果作为网络工程师，有这样的心态就非常不正确了。
因为网络管理员的工作基本上都是操作型的，而网络工程师的工作则主要是进行各类系统的设计，是底层的。
没有全面、深入、扎实的理论基础，不可能对相应技术有一个本质上的理解和运用，更谈不上利用这些技术来设计解决方案了。
这就是网络管理员和网络工程师的一个本质区别。

本书主要内容　　《网络工程师必读——网络安全系统设计》与笔者在本系列中写的另一部图书——《网络工程师必读——网络系统设计》一样，题目非常大（指其内涵），所涉及的技术、产品和方案非常广。
就像我们在写一篇作文一样，题目越大，文章越难写。
因为要写，或者可写的内容实在太多、太广，从主题选取，到各主题内容的选取都不是一件简单的事。
毕竟就目前来说，网络安全已自成一个庞大的系统，所涉及的技术、产品和方案渗透到了网络领域的各个角落，而无论如何，一本书的篇幅都是非常有限的。
所以，在笔者正式写这部书之前，仅写什么和怎么写这两个方面就考虑了非常长的时间。
而且在编写这部书之前，总希望能借鉴一些已有的网络安全系统设计类图书的主题选取和写作方法，总希望用有限的篇幅尽可能系统地介绍一些主流的网络安全技术和方案设计思路。
但非常遗憾，笔者在网络上查看了近20部网络安全类图书的目录，竟然没有一部是希望看到的。
所以，笔者最终还是只能靠自己，从头设计本书的主体架构，包括整部图书的章节安排（也可以算是整部图书的体系架构）、各章的主题，以及各章内部的主要内容。
综合起来是这样一个基本的写作思路：整部图书的主线是OSI/RM的7层结构，各章主要针对各主要层次的主要安全技术和方案进行展开，并在本书最后介绍了几个综合的网络安全系统设计和配置方案。

本书共11章，具体内容安排如下。

第1章 网络安全系统设计综述　　本章主要对目前主要的网络隐患、所涉及的主要网络安全技术，以及网络安全系统的设计基本思路进行综合介绍。

第2章 物理层的网络安全保护方案　　本章主要对基于OSI/RM物理层的主要网络安全保护技术和方案进行具体介绍。
其中所涉及到的网络安全技术包括计算机网络通信物理介质、线路和设备的屏蔽、网络通信线路的物理隔离、网络通信线路的冗余、数据备份和容灾，以及典型网络物理层的安全保护工具的介绍等。

第3章 数据链路层的安全保护方案　　本章主要介绍了各种主要的数据链路层可用的加密技术，以及WLAN网络中所用的各种数据链路加密、身份验证技术原理和配置方法，如WEP、WPA、WPA2、IEEE 802.1x和IEEE 802.11i等。
还介绍了主流品牌网络设备MAC地址绑定和嗅探防护等。
至于VLAN方面的详细配置在本系列的《网络工程师必读——网络设备配置与管理》（交换机分册）一书中介绍。

<<网络工程师必读>>

内容概要

本书从网络工程师的职业角度出发组织和安排内容，非常具有针对性。
本书从网络安全系统设计全局出发，以OSI/RM的7层结构为主线，层层把关，全面、系统地介绍各层的主要安全技术和方案设计思路、方法。

本书从深层次分析了网络安全隐患存在的各个主要方面，然后从这几个方面出发，全面介绍企业局域网安全防护系统的设计方法。
其中包括网络安全系统设计综述、物理层的网络安全保护方案、数据链路层的安全保护方案、网络层防火墙安全保护方案、网络层Kerberos身份认证方案、网络层证书身份认证、加密和签名方案、网络层PKI综合应用方案设计、网络层IPSec身份认证和加密方案、传输层TLS/SSL身份认证和加密方案、应用层Web服务器的综合安全系统设计与配置、WLAN网络综合安全系统设计与配置，并通过实际可用的安全防护方法来实现网络安全隐患的排除或防护。
这些不同方面的安全防护措施形成了一个系统的整体，使得企业网络从各个方面都得到足够的安全保证。
以上这些都是网络工程师所必须掌握的基础知识和技能。

本书适合网络工程师参考学习，也可作为高等院校及相关培训机构的教材。

<<网络工程师必读>>

书籍目录

第1章 网络安全系统设计综述　1.1 网络安全系统设计基础　1.2 OSI/RM各层的安全保护　1.3 系统层的安全保护　1.4 网络安全系统设计　1.5 网络安全系统设计的基本思路第2章 物理层的网络安全保护方案　2.1 物理层安全保护概述　2.2 物理层的线路窃听技术分析　2.3 计算机网络通信线路屏蔽　2.4 物理线路隔离　2.5 设备和线路冗余　2.6 机房和账户安全管理　2.7 数据安全管理　2.8 物理层安全管理工具　2.9 服务和服务账户安全规划第3章 数据链路层的安全保护方案　3.1 典型数据加密算法　3.2 数据加密　3.3 WLANSSID安全技术及配置方法　3.4 WLANMAC地址过滤　3.5 WLANWEP加密　3.6 WPA加密　3.7 WPA2加密　3.8 无线AP/路由器的WPA和WPA2设置……第4章 网络层防火墙安全保护方案第5章 网络层Kerberos身份认证方案第6章 网络层证书身份认证、加密和签名方案第7章 网络层PKI综合应用方案设计第8章 网络层IPSec身份认证和加密方案第9章 传输层TLS/SSL身份认证和加密方案第10章 应用层Web服务器的综合安全系统设计与配置第11章 WLAN网络综合安全系统设计与配置后记

章节摘录

“容灾”，简单地说就是尽量减少或避免因灾难的发生而造成的损失。
它是一个系统工程，备份与恢复就是这一系统工程的两个重要组成部分。
除此之外，还有许多具体的工作，如备份媒体的保管、存放、容灾演练等，都是容灾中要做的。
从广义上讲，任何有助于提高系统可用性的努力，都可以被称为容灾。
要实现容灾，首先要了解我们的“敌人”——灾难。
哪些事件可以定义为灾难呢？
典型的灾难事件是自然灾难，如火灾、洪水、地震、飓风、龙卷风、台风等，还有原先提供给业务运营所需的服务中断，如设备故障、软件错误、电信网络中断和电力故障等。
此外，人为的因素往往也会酿成大祸，如操作员错误、破坏、植入有害代码和恐怖袭击。
现阶段，由于我国很多行业正处在高速发展的阶段，很多生产流程和制度仍不完善，加之缺乏经验，这方面的损失屡见不鲜。
对此，我们需要做到两点：一是建立切实可行的应急机制，这主要包含一套基于充分且清楚地将风险予以分类定义的业务持续计划；二是在危机突然降临时，此计划能被有效地执行。
从广义上讲，任何有助于提高系统可用性的努力，都可称之为容灾。
本地容灾，就是主机集群，当某台主机出现故障，不能正常工作时，其他的主机可以替代该主机，继续进行正常的工作。
平时讲到的容灾，尤其是值得重视的容灾，一般都是远程容灾。
远程容灾可以这样理解：在各种企业的IT系统中，必然有一部分（尤其是核心部分）是非常重要的，我们叫它生产中心。
人们往往给生产中心配备一个备份中心，该备份中心是远程的，并且在生产中心的内部，已经实施了各种各样的数据保护。
不管怎么保护，当火灾、地震这种灾难发生时，一旦生产中心瘫痪了，备份中心会接管生产，继续提供网络服务。
比如全国铁路调度中心的网络系统，当发生火灾、地震等灾难性事件时，该系统仍要保证正常运行，不能因为调度中心出现灾难性事件，使全国的铁路处于瘫痪状态，让灾难不合理地蔓延。
除了详尽的容灾计划外，还需要合理的IT系统架构来确保企业的容灾计划得以实现。
对于IT系统而言，在技术层面上，容灾需要考虑以下几个方面。

编辑推荐

作者王达中国知名网络技术IT作家，继畅销书“网管员必读”系列之后又一力作，一本真正全局意义上的安全系统设计类图书，专业的一手技术资料，庞大的读者服务体系。

<<网络工程师必读>>

版权说明