<<网络安全原理与应用>>

图书基本信息

书名：<<网络安全原理与应用>>

13位ISBN编号：9787517006077

10位ISBN编号：751700607X

出版时间：2013-2

出版时间：水利水电出版社

<<网络安全原理与应用>>

书籍目录

章节摘录

版权页： 插图： 防火墙并不能确保内部用户之间的安全访问。
内部网络中每一个用户的安全要求是不一样的，一些机密信息（如财务、人事档案等）就要求较高的安全等级，否则一旦遭到攻击就会造成巨大损失。
这种攻击可能来自外网，也可能来自内网，据统计，80%的攻击来自内部。
对于来自内部的攻击，边界防火墙是无能为力的。
为了机密信息的安全，还需要对内网的部分主机再加以保护，使之免受内部用户的侵袭。
可以将内部网络的一部分与其余部分隔离，在内部网络的两个部分之间再建立防火墙，称之为内部防火墙。
建立内部防火墙，可以使用分布式防火墙、嵌入式防火墙等新的产品。
5.4.1 分布式防火墙（Distributed Firewall） 1.分布式防火墙简介 分布式防火墙是一种全新的防火墙概念，是比较完善的一种防火墙技术，它是在边界防火墙的基础上开发的，目前主要以软件形式出现。
分布式防火墙是一种主机驻留式的安全系统，用以保护内部网络免受非法入侵的破坏。
分布式防火墙把Internet和内部网络均视为“不友好的”，对所有的信息流进行过滤与限制，无论是来自Internet，还是来自内部网络。
它们对个人计算机进行保护的方式如同边界防火墙对整个网络进行保护一样。
分布式防火墙克服了操作系统具有的安全漏洞，如DoS（拒绝服务），从而使操作系统得到强化。
分布式防火墙对每个主机都能进行专门的保护。
2.分布式防火墙的体系结构 分布式防火墙包含以下三个部分：（1）网络防火墙（Network Firewall）：这一部分有的公司采用的是纯软件方式，有的公司可以提供相应的硬件支持。
它用于内部网与外部网之间，以及内部网络各子网之间。
与边界防火墙相比，它多了一种用于内部子网之间的安全防护层，这样整个网络的安全防护体系就显得更加全面，更加可靠。
其功能与传统的边界式防火墙类似。
（2）主机防火墙（Host Firewall）：同样也有纯软件和硬件两种产品，用于对网络中的服务器和工作站进行防护。
这是边界防火墙所不具有的功能，是对边界防火墙在安全体系方面的一个完善。
它作用在同一内部子网之间的各工作站与服务器之间，以确保内部网络的安全。
（3）中心管理（Central Management）：这是一种服务器软件，负责总体安全策略的策划、管理、分发及日志的汇总。
这样防火墙就可以进行智能管理，提高了防火墙的安全防护灵活性，具备可管理性。
3.分布式防火墙的主要特点 综合起来这种新的防火墙技术具有以下几个主要特点：（1）主机驻留。
分布式防火墙最主要的特点就是采用主机驻留方式，所以称之为“主机防火墙”。
它驻留在被保护的主机上，该主机以外的网络不管是处在网络内部还是网络外部都认为是不可信任的，因此可以针对该主机设定针对性很强的安全策略。
主机防火墙使安全策略不仅停留在内网与外网之间，而是把安全策略延伸到网络中的每台主机。

编辑推荐

戚文静、刘学主编《21世纪高等院校规划教材:网络安全原理与应用(第2版)》的目的是帮助读者了解网络所面临的各种安全威胁，掌握网络安全的基本原理，掌握保障网络安全的主要技术和方法，学会在开放的网络环境中保护信息和数据。

《21世纪高等院校规划教材:网络安全原理与应用(第2版)》注重理论与实践相结合，每章都配有应用实例，一方面有助于读者对理论知识的理解和掌握；另一方面，学以致用可以提高读者的学习兴趣、增加学习动力，也有助于提高读者的实践能力。

<<网络安全原理与应用>>

版权说明