# <<信息安全产品配置与应用>>

## 图书基本信息

书名：<<信息安全产品配置与应用>>

13位ISBN编号：9787121118685

10位ISBN编号：7121118688

出版时间：2010-10

出版时间：电子工业出版社

作者：武春岭 编

页数：275

## 前言

随着互联网在中国的快速发展与普及，人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化。
互联网在促进经济结构调整、经济发展方式转变等方面发挥着越来越重要的作用，目前中国已成为世界上互联网使用人口最多的国家。
然而，互联网安全问题日益突出，成为各国普遍关切的问题，中国也面临着严重的网络安全威胁。
近几年来，随着网络技术的迅速发展，网络环境也更加复杂化。
计算机网络安全威胁的日益严重，如病毒和蠕虫不断扩散、黑客活动频繁、垃圾邮件猛增都成为了目前困扰网络信息安全的较大网络威胁。
譬如，2009年新的安全威胁Conficker（飞客）的出现，打破了全球500万台电脑的感染记录，这些都迫使计算机用户不断地提高防范意识，并对信息安全产品提出了更高需求。
目前，信息安全最基本的防护手段是构建完善的信息安全防御平台，以防火墙、入侵检测产品为代表的信息安全产品构建综合防御体系，构建保障信息安全的基础屏障。
信息安全产品已经成为政府、金融和其他企事业单位信息化推进的基本硬件保障，市场对信息安全产品的需求日益增长。
与此同时，信息安全厂商、信息系统集成商和信息系统运营商对信息安全产品技术支持和技术服务的专业人员需求也与日俱增、日趋迫切。
重庆电子工程职业学院信息安全技术专业，是国家示范院校建设中唯一一个信息安全类国家级重点建设专业，该专业自2003年开办以来，就开设了“信息安全产品配置与应用”课程，目前该课程已经获得重庆市市级精品课称号。
我们根据多年的教学实践，与天融信公司合作，编写了该专业的核心技术教材，旨在更有效地培养信息安全产品工程师（产品销售工程师、产品维护工程师和产品技术支持工程师）。
作为一本专注于信息安全产品的教材，本书详细介绍了信息安全领域常用产品的配置及应用和产品部署方案。
本书共分8章，第1章讲述防火墙产品配置与应用；第2章讲述VPN产品配置与应用；第3章讲述入侵检测产品配置与应用；第4章讲述网络隔离产品配置与应用；第5章讲述安全审计及上网行为管理产品配置与应用；第6章讲述网络存储设备配置及应用；第7章讲述数据备份软件配置及应用；第8章讲述防病毒过滤网关系统配置及应用。
本书的写作融入了作者丰富的教学和企业实践经验，内容安排合理，每个章节都专注于特定主题，讲解通俗，案例丰富，力争让读者能够在最短的时间内掌握核心安全设备的基本操作与应用技巧、快速入门与提高。
本书第1章、第5章和第8章由武春岭编写，第2章由路亚编写，第3章、第4章由鲁先志编写，第6章、第7章由李贺华编写。
为了方便教师教学，本书配有电子教学课件，有此需要的教师可登录华信教育资源网免费注册后进行下载，有问题时可在网站留言板留言或与电子工业出版社联系。
本书在编写过程中，得到了电子工业出版社及天融信公司成都分公司周非副总经理和魏振国工程师的大力支持和帮助。
在此一并致以衷心的感谢！
由于编者水平有限，加上时间仓促，书中难免有不当之处，敬请各位同行与读者批评指正，以便在今后的修订中不断改进。

# <<信息安全产品配置与应用>>

## 内容概要

本书是一本专注于信息安全产品的教材，内容涵盖了防火墙、VPN、入侵检测、网络隔离、网络存储、数据备份、防病毒和安全审计及上网行为管理等常用信息安全设备，详细介绍了它们各自的功能、工作原理、配置，以及应用部署方案。

本书的写作融入了作者丰富的教学和工程实践经验，采用项目导向、任务驱动，基于典型工作任务组织教学内容，每个章节都专注于特定的主题，讲解通俗，案例丰富，力争让读者能够在最短的时间内掌握核心安全设备的基本操作与应用技能、快速入门与提高。

本书不仅可以作为高职、高专计算机信息类专业学生的教材，也可作为企事业单位网络信息系统管理人员的技术参考手册，尤其适合想在短期内快速掌握安全产品应用与部署的用户。

# <<信息安全产品配置与应用>>

## 书籍目录

## 章节摘录

插图：（3）无法控制局域网用户对互联网及对服务器的访问，网络访问均不在受控范围内。
根据上述情况，该企业的网络管理员找到了一家专业的网络安全公司寻求帮助，并提出以下要求：（1）设计一个针对本企业目前网络及应用适用的网络安全方案；（2）方案可以实现对互联网边界的访问控制与保护，可以抵御来自互联网的攻击；（3）方案可以对内部服务器进行独立的保护；（4）根据需要应该可以进一步实现对内网用户访问互联网的控制；（5）配备的产品应具备高扩展能力，可以在适当时候增加其他需要的功能模块，如VPN等；（6）配备的产品应采用最新技术，产品应具有延续性，至少保证5年的产品升级延续。
根据上述情况，该专业公司（为方便说明问题，以下以第一人称角度进行描述）计划为此客户设计一个切实可行并具备一定扩展能力的网络安全方案。
1.5.2 任务2：方案设计我们在接到客户的需求并进行分析后，首先发现客户网络的安全区域（SSN）划分不够明确，为此，在方案中首先对客户的网络安全区域进行了设计。
区域划分是网络安全规划的首要任务，安全区域划分除了可以实现对重点区域的重点保护外，还可以进一步对网络及应用的安全边界进行明确。
根据对网络及应用的了解，我们在方案中将这个客户的网络划分为3个逻辑区域，区域情况分别如下：服务器区域：该规划区域部署的是该单位重要的ERP、数据库、OA等业务系统，对中心的日常办公有着极其重要的意义，为此作为一个独立的安全区域进行独立的安全保护。
内网办公区域：该区域为日常办公计算机的一个区域，该区域下大约有100台计算机，其中30台计算机可以访问互联网，其他计算机不运行访问互联网，但可以访问服务器区域的部分应用。
该区域计算机均为接入终端，安全性要求较低，但该区域计算机因为数量大，分布不如服务器区域那么集中，维护和管理相对烦琐，故该区域计算机出现故障、中病毒的概率较大，为避免影响到其他区域，所以也作为一个独立的安全区域进行接入控制。
互联网区域：该区域是公众区域，基本上大部分的安全威胁均是来自这个区域。
同时，以后可能涉及的移动办公及可能需要的和集团的互连，均需要通过互联网区域。
在进行上述区域划分后，我们为客户提供了进一步的网络规划建议如下：虽然目前客户内部计算机数量只有百台左右，但若网络规划不合理，即使内部网络采用千兆网络，也可能出现网速慢，以及病毒极易传播的问题，为此我们建议如下：（1）在核心交换机上进行VI,AN划分，将服务器单独作为一个VLAN；（2）将接入计算机按照重要性或部门分为多个VLAN；（3）各个VLAN间的路由及基本的ACL由核心交换机完成，如果核心交换机功能有限，可以使用部署在边界的防火墙实现VLAN间的路由和访问控制，但这样需要选择性能相对较高的防火墙设备。
网络IP地址规划，不建议使用公网地址，建议根据今后一段时间的扩展需要，最好将VLAN内地址分在一个C类私有网段，并且建议均使用固定IP，对于网络维护及故障查找较DHCP方式方便。

# <<信息安全产品配置与应用>>

## 编辑推荐

《信息安全产品配置与应用》：以防火墙、入侵检测等核心信息安全产品应用为载体，培养学生信息安全综合防御能力，采用项目导向、任务驱动，基于典型工作任务组织教学内容。

# <<信息安全产品配置与应用>>

## 版权说明