信息安全技术

全国信息技术人才培养工程指定培训教材

网络安全设备与技术

信息产业部电子教育中心　组编
祝晓光　编著

清华大学出版社

全国信息技术人才培养工程指定培训教材

网络安全设备与技术

信息产业部电子教育中心　组编

祝晓光　编著

清华大学出版社

北　京

内 容 简 介

本书全面系统地介绍了作为信息安全主要内容之一的网络安全的核心技术和典型网络安全设备。全书内容分为7章，第1章简要描述了目前流行的一些网络安全设备以及利用这些设备可以构建的典型应用和未来的发展趋势；第2章详细阐述了密码学基础，各种不同的加密算法，以及密钥管理和密码学的一些不同场合的应用；第3章主要阐述了PKI(Public Key Infrastructure)公钥基础架构的内容，以及两个最常见的安全协议SSL和SET；第4章详细描述了几种不同类型防火墙的工作原理及典型的防火墙部署结构；第5章详细介绍了入侵检测技术和IDS产品常见的部署方式以及IDS技术的发展趋势；第6章主要描述了安全扫描技术的工作原理和发展历程，以及漏洞扫描器的类别与特点；第7章主要针对主流路由和交换产品的安全优化和配置进行了详细描述，并深入地阐述了VPN的核心技术和目前主流的一些VPN组网方式。

本书内容实用，可操作性强，可作为计算机、通信、信息安全等领域研究人员和专业技术人员的参考书，也可作为高等院校计算机、通信、信息安全等专业的教材。

图书在版编目(CIP)数据

网络安全设备与技术/祝晓光编著. —北京：清华大学出版社，2004.11
(全国信息技术人才培养工程指定培训教材)
ISBN 7-302-09666-X
Ⅰ. 网… Ⅱ. 祝… Ⅲ. 计算机网络—安全技术—技术培训—教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字(2004)第101595号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　**邮　　编**：100084
社 总 机：010-62770175　**客户服务**：010-62776969
组稿编辑：胡伟卷
文稿编辑：刘金喜
封面设计：王　永
版式设计：康　博
印 刷 者：北京市昌平环球印刷厂
装 订 者：三河市化甲屯小学装订二厂
发 行 者：新华书店总店北京发行所
开　　本：185×230　**印张**：23.25　**字数**：493千字
版　　次：2004年11月第1版　2004年11月第1次印刷
书　　号：ISBN 7-302-09666-X/TP·6695
印　　数：1～5000
定　　价：35.00元

全国信息技术人才培养工程教材编委会

通讯地址：北京 4356 信箱教育中心

http://www.ceiaec.org/

丛书序

当今世界，随着信息技术在经济社会各领域不断深化的应用，信息技术对生产力以至于人类文明发展的巨大作用越来越明显。党的“十六大”提出要“坚持以信息化带动工业化，以工业化促进信息化”，“优先发展信息产业，在经济和社会领域广泛应用信息技术”。明确了我国经济发展的道路，赋予了信息产业新的历史使命。近年来，日新月异的信息技术呈现出新的发展趋势，各类信息技术加快了相互融合和渗透的步伐，信息技术与其他技术的结合更加紧密，信息技术应用的深度、广度和专业化程度不断提高。

我国的信息产业作为国民经济的支柱产业正面临着有利的国际、国内形势．电子信息产业的规模总量已进入世界大国行列。但是我们也清楚地认识到，与国际先进水平相比，我们在产业结构、核心技术、管理水平、综合效益、普及程度等方面，还存在较大差距，缺乏创新能力与核心竞争力，“大”而不强。国际国内形势的发展，要求信息产业不仅要做大，而且要做强，要从制造大国向制造强国转变，这是信息产业今后的重点工作。要实现这一转变，人才是基础。机遇难得，人才更难得，要抓住本世纪头二十年的重要战略机遇期，加快信息产业发展，关键在于培养和使用好人才资源。《中共中央、国务院关于进一步加强人才工作的决定》指出，人才问题是关系党和国家事业发展的关键问题，人才资源已成为最重要的战略资源，人才在综合国力竞争中越来越具有决定性意义。

为抓住机遇，迎接挑战，实施人才强业战略，信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导，充分发挥全行业和全社会教育培训资源的作用，建立规范的信息技术教育培训体系、科学的培训课程体系、严谨的信息技术人才评测服务体系，培养造就大批行业急需的、结构合理的高素质信息技术应用型人才，以促进信息产业持续快速协调健康发展。

由各方专家依据信息产业对技术人才素质与能力的需求，在充分吸取国内外先进信息技术培训课程优点的基础上，信息产业部电子教育中心精心组织编写了信息技术系列培训教材。这些教材注重提升信息技术人才分析问题和解决问题的能力，对各层次信息技术人才的培养工作具有现实的指导意义。我谨向参与本系列教材规划、组织、编写的同志们致以诚挚的感谢，并希望该系列教材在全国信息技术人才培养工作中发挥有益的作用。

王耀光

二〇〇四年四月十三日

前　言

通过多年的建设，大部分企业的信息化都已经取得了显著成绩，并且随着网络规模的不断扩大，网络体系结构的日趋复杂，应用系统数量的迅速增加，尤其是网上交易业务(如电子商务、网上银行、网上证券)的逐步展开，使得很多企业的业务、办公和管理越来越依赖于网络系统。网络系统的安全可靠正在逐步成为企业正常运行的核心基础。

然而，随着网络技术的迅速发展，网络攻击行为的破坏性越来越大，网络中严重程度中等或较高的漏洞也急剧增加，新漏洞越来越容易被利用；将病毒、蠕虫、特洛伊木马和恶意代码的特性与服务器和 Internet 漏洞结合起来而发起、传播和扩散的混合型攻击已成为趋势，并且由于此种攻击采用加密、变换、插入等技术手段巧妙地伪装自身，穿透防火墙非法获取系统权限，躲避、防御甚至攻击检测软件，而造成大部分企业现有安全防护系统无法有效防治的局面越来越严重，并且开始对整个企业的办公和业务网络的安全形成巨大威胁。因此，如何保障企业的办公网和各应用系统网络的安全，已经成为目前急待解决的问题之一。

纵观安全行业的发展历程，从大量的统计规律来看，会发现用户的思想认识发展可以分为 3 个阶段：

第 1 个阶段是受主流信息安全产品厂商的引导，坚信单一安全产品能够很好地保护自己的业务应用，典型思想表现为“安全就是防火墙”，把规模化的单一产品采购作为信息安全的惟一保障。

第 2 个阶段是在经历了一些信息安全事件之后，用户总结了一定的经验和教训，意识到单一信息安全产品并不能真正有效地维护安全的网络，开始注意各种安全产品的搭配使用、联动和协调分析。一些基于对不同安全产品进行统一管理的应用平台进入市场，但此时用户还是把信息安全当做纯粹技术产品的堆砌，把相关工作看成是纯粹技术人员的工作。这具体体现在不能很好地在企业内部贯彻安全管理思想，不能有效地控制和防范内部员工的一些不良操作习惯和由此导致的安全隐患。

第 3 个阶段是部分对信息安全有更高需求的用户开始意识到企业组织体系、管理体系在整体信息安全建设中的重要意义，也意识到制定安全规范、安全制度的必要性，但是限于在安全理解、安全观念上的局限性，很难获得真正有效的提升，从而无法有效地组织企业信息

安全管理体系的建设和实施。

本书并未涉及安全管理方面的内容，仅仅是从技术层面上，针对目前主流的一些网络安全设备，从概念、工作原理、部署方式以及发展趋势等方面进行了描述，使得读者能了解目前在安全防护方面的一些技术手段。如果要构建一个完整的安全防御体系，则必须在充分了解自身安全风险的情况下，根据安全管理策略的指导，来进行安全设备的选择和配置；单纯地为部署产品而购买产品，则很难达到购买产品所希望达到的目标，甚至会因盲目投资而造成损失。

本书在编写的过程中得到了瑞索讯杰公司的鼎力支持，在此表示感谢，同时也参阅了大量的国内外资料，包括一些网上公开的资料。另外，由于作者本身水平有限，错误和疏漏在所难免，望多多指正和批评。

作　者

目　录

第 1 章

概　述

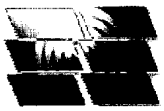
Internet 的发展在对社会、经济、文化和科技带来巨大推动和冲击的同时，作为一个提供开放性和共享性的空间，所带来的一系列安全问题是有目共睹的。通过专业的网络安全设备(诸如防火墙、入侵检测、漏洞扫描等)来保障企业的信息安全是非常重要和有效的措施之一，它们可以简化管理员的工作，实时检测和阻挡来自黑客的攻击行为。了解当前的网络中具有哪些网络安全设备，它们各自的工作原理、优缺点以及典型应用，对于指导如何构筑一个完整、有效的信息安全体系是非常有意义的。

教学目标

本章内容主要是对目前常用的网络安全设备进行描述，并根据其不同作用介绍所应用到的不同场所。学习完本章后，读者应能初步了解不同网络安全设备的概念、作用、应用场所，并对网络安全设备的发展趋势有初步的认识。

教学重点与难点

- 网络安全设备的概念和作用
- 网络安全设备的发展趋势
- 网络安全设备的典型应用



1.1 网络安全设备的划分

1.1.1 加密系统

密码技术是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。 如果用硬件设备来完成加密过程，则该设备通常称做加密机，如果采用软件来完成加密过程，则通常称为加密软件。

一般的数据加密可以在通信的三个层次来实现：链路加密、节点加密和端到端加密。 相应的也就会有三种加密设备或加密软件。

1. 链路加密

对于在两个网络节点间的某一次通信链路，链路加密能为网上传输的数据提供安全保障。对于链路加密(又称在线加密)，所有消息在被传输之前进行加密，在每一个节点对接收到的消息进行解密，然后先使用下一个链路的密钥对消息进行加密，再进行传输。在到达目的地之前，一条消息可能要经过许多通信链路的传输。

由于在每一个中间传输节点，消息均被解密后重新进行加密，因此，包括路由信息在内的链路上的所有数据均以密文形式出现。这样，链路加密就掩盖了被传输消息的源点与终点。填充技术的使用以及填充字符在不需要传输数据的情况下就可以进行加密，使得消息的频率和长度特性得以掩盖，从而可以防止对通信业务进行分析。

尽管链路加密在计算机网络环境中使用得相当普遍，但它并非没有问题。链路加密通常用在点对点的同步或异步线路上，它要求先对在链路两端的加密设备进行同步，然后使用一种链模式对链路上传输的数据进行加密。这就给网络的性能和可管理性带来了副作用。

在线路/信号经常不通的海外或卫星网络中，链路上的加密设备需要频繁地进行同步，带来的后果是数据丢失或重传。另一方面，即使仅一小部分数据需要进行加密，也会使得所有传输数据被加密。

在一个网络节点，链路加密仅在通信链路上提供安全性，消息以明文形式存在，因此所有节点在物理上必须是安全的，否则就会泄漏明文内容。然而保证每一个节点的安全性需要较高的费用，为每一个节点提供加密硬件设备和一个安全的物理环境所需要的费用由以下几

部分组成：保护节点物理安全的雇员开销，为确保安全策略和程序的正确执行而进行审计的费用，以及为防止安全性被破坏时带来损失而参加保险的费用。

在传统的加密算法中，用于解密消息的密钥与用于加密的密钥是相同的，该密钥必须秘密保存，并按一定规则进行变化。这样，密钥分配在链路加密系统中就成了一个问题，因为每一个节点必须存储与其相连接的所有链路的加密密钥，这就需要对密钥进行物理传送或者建立专用网络设施。而网络节点地理分布的广阔性使得这一过程变得复杂，同时增加了密钥连续分配时的费用。

2. 节点加密

尽管节点加密能给网络数据提供较高的安全性，但它在操作方式上与链路加密是类似的：两者均在通信链路上为传输的消息提供安全性；都在中间节点先对消息进行解密，然后进行加密。因为要对所有传输的数据进行加密，所以加密过程对用户是透明的。

然而，与链路加密不同，节点加密不允许消息在网络节点以明文形式存在，它先把收到的消息进行解密，然后采用另一个不同的密钥进行加密，这一过程在节点上的一个安全模块中进行。

节点加密要求报头和路由信息以明文形式传输，以便中间节点能得到如何处理消息的信息。因此，这种方法对于防止攻击者分析通信业务是脆弱的。

3. 端到端加密

端到端加密允许数据在从源点到终点的传输过程中始终以密文形式存在。采用端到端加密(又称脱线加密或包加密)，消息在被传输时到达终点之前不进行解密，因为消息在整个传输过程中均受到保护，所以即使有节点被损坏也不会使消息泄露。

端到端加密系统通常不允许对消息的目的地址进行加密，这是因为每一个消息所经过的节点都要用此地址来确定如何传输消息。由于这种加密方法不能掩盖被传输消息的源点与终点，因此它对于防止攻击者分析通信业务是脆弱的。

4. 加密传输方式的比较

数据保密变换使数据通信更安全，但不能保证在传输过程中绝对不会泄密。因为在传输过程中，还有泄密的隐患。

采用链路加密或者节点加密方式，从起点到终点，要经过许多中间节点，在每个节点均要暴露明文(节点加密方法除外)。如果链路上的某一节点安全防护比较薄弱，那么按照木桶

原理(木桶水量由最低一块木板决定)，虽然采取了加密措施，但整个链路的安全只相当于最薄弱的节点处的安全状况。

采用端到端加密方式，只是发送方加密报文，接收方解密报文，中间节点不必加密、解密，也就不需要密码装置。此外，加密可采用软件实现，使用起来很方便。在端到端加密方式下，每对用户之间都存在一条虚拟的保密信道，每对用户应共享密钥(传统密码保密体制，非公钥体制下)，所需的密钥总数等于用户对的数目。对于几个用户，若两两通信，共需密钥 $n(n-1)/2$ 种，每个用户需 $n-1$ 种。这个数目将随网上通信用户的增加而增加。为安全起见，每隔一段时间还要更换密钥，有时甚至只能使用一次密钥，密钥的用量很大。

采用链路加密，每条物理链路上，不管用户多少，可使用一种密钥。在节点加密情况下，每经过一个节点，都需要更换密钥，则密钥的数目是 $n(n-1)/2$ 种。这里，n 是节点数而非用户数，一个节点一般有多个用户。

从身份认证的角度看，链路加密和节点加密都是只能认证节点，而不是用户。使用节点A密钥的报文仅保证它来自节点A。报文可能来自A的任何用户，也可能来自另一个路过节点A的用户。因此链路加密不能提供用户鉴别。端到端加密对用户是可见的，可以看到加密后的结果，起点、终点很明确，可以进行用户认证。

另外，端到端加密系统的价格便宜些，并且与链路加密和节点加密相比更可靠，更容易设计、实现和维护。端到端加密还避免了其他加密系统所固有的同步问题，因为每个报文包均是独立被加密的，所以一个报文包所发生的传输错误不会影响后续的报文包。此外，从用户对安全需求的直觉上讲，端到端加密更自然些。单个用户可能会选用这种加密方法，以便不影响网络上的其他用户，此方法只需要源和目的节点是保密的即可。

总之，链路加密和节点加密对用户来说比较容易，使用的密钥较少，而端到端加密比较灵活，用户可见。对链路加密或者节点加密中各节点安全状况不放心的用户也可使用端到端加密方式。

具体的加密技术请参阅第2章密码学技术。

1.1.2 防火墙

防火墙是网络安全领域首要的、基础的设施，它对维护内部网络的安全起着重要的作用。利用防火墙可以有效地划分网络不同安全级别区域间的边界，并在边界上对不同区域间的访问实施访问控制、身份鉴别和审计等安全功能。按实现方式的不同，防火墙的基本类型有包过滤型、应用网关级防火墙、代理服务型和状态检测型。

数据包过滤(Packet Filtering)技术是在网络层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，被称为访问控制表(Access Control Table)。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或它们的组合来确定是否允许该数据包通过。

数据包过滤防火墙逻辑简单，价格便宜，易于安装和使用，网络性能和透明性好，它通常安装在路由器上。路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。

数据包过滤防火墙的缺点有二：一是非法访问一旦突破防火墙，即可对主机上的软件和配置漏洞进行攻击；二是数据包的源地址、目的地址以及 IP 的端口号都在数据包的头部，很有可能被窃听或假冒。

分组过滤或包过滤是一种通用、廉价、有效的安全手段。之所以通用，因为它不针对各个具体的网络服务采取特殊的处理方式；之所以廉价，因为大多数路由器都提供分组过滤功能；之所以有效，因为它能很大程度地满足企业的安全要求。所根据的信息来源于 IP、TCP 或 UDP 包头。

包过滤的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其弱点也是明显的：包过滤判别的只有网络层和传输层数据的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大地影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC 一类的协议。另外，大多数过滤器中缺少审计和报警机制，且管理方式和用户界面较差；若对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常和应用网关配合使用，共同组成防火墙系统。

任何类型的防火墙在某种程度上均会影响网络的性能，包过滤防火墙通常速度最快，因为它只检测每个数据包中最基本的包头信息。但包过滤策略的规则越多，就会发生越多的冲突。因此，包过滤防火墙最适合于禁止多地址往来访问的相对封闭环境。

应用级网关(Application Level Gateways)是在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时，对数据包进行必要的分析、登记和统计，形成报告。实际中的应用网关通常安装在专用工作站系统上。

数据包过滤和应用网关防火墙有一个共同的特点，就是它们仅仅依靠特定的逻辑判定是否允许数据包通过。一旦满足逻辑，则防火墙内外的计算机系统建立直接联系，防火墙外部

的用户便有可能直接了解防火墙内部的网络结构和运行状态，这有利于实施非法访问和攻击。

代理服务(Proxy Service)也称链路级网关或 TCP 通道(Circuit Level Gateways or TCP Tunnels)，也有将它归于应用级网关一类。它是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，其特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”，由两个终止代理服务器上的“链接”来实现，外部计算机的网络链路只能到达代理服务器，从而起到了隔离防火墙内外计算机系统的作用。

此外，代理服务也对过往的数据包进行分析、注册登记，形成报告，同时当发现被攻击迹象时会向网络管理员发出警报，并保留攻击痕迹。

应用代理型防火墙是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用。同时也常结合过滤器的功能。它工作在 OSI 模型的最高层，掌握着应用系统中可用做安全决策的全部信息。

为了克服包过滤模式明显的安全性不足的问题，一些包过滤防火墙厂商，如 CheckPoint 推出了状态包过滤的概念。在包过滤技术的基础上，通过基于上下文的动态包过滤模块检查，增强了安全性检查。它不再只是分别对每个进来的包简单地就地址进行检查，动态包过滤防火墙在网络层截获进来的包，直到足够的数量，以便能够确定此试图连接的有关“状态”。然后用防火墙系统内核中“专用的检查模块”对这些包进行检查。安全决策所需的相关状态信息经过这个“专用的检查模块”检查之后，记录在动态状态表中，以便对其后的数据包通信进行安全评估。经过检查的包穿过防火墙，在内部与外部系统之间建立直接的联系。

防火墙的优点主要有：保护脆弱的服务，控制对系统的访问，集中的安全管理，增强的保密性，记录和统计网络，可制定和执行网络安全策略等。

防火墙的缺点主要有：防火墙不能防止通向站点的后门；防火墙一般不提供对内部的保护；防火墙无法防范数据驱动型的攻击；防火墙本身的防攻击能力不够，容易成为被攻击的首要目标；防火墙不能根据网络被恶意使用和攻击的情况动态调整自己的策略。

综合考虑 Internet 的发展势头和防火墙产品的更新步伐，从产品及功能上，可以看到防火墙的主流动向和趋势，主要有以下几点：

- 防火墙将从目前对子网或内部网管理的方式向远程上网集中管理的方式发展；
- 过滤深度不断加强，从目前的地址、服务过滤，发展到 URL(页面)过滤、关键字过滤和对 Active X、Java 等的过滤，并逐渐有病毒扫除功能；
- 利用防火墙建立专用网(VPN)是较长一段时间用户使用的主流，IP 的加密需求越来越