万平国　编著

网络隔离与网闸

国家信息化安全教育认证(ISEC)系列教材

机械工业出版社
CHINA MACHINE PRESS

国家信息化安全教育认证(ISEC)系列教材

网络隔离与网闸

万平国　编著

机械工业出版社

本书详尽阐述了网络隔离技术的原理，网闸技术的实现，应用协议的隔离和数据交换原理，网闸的测试原理与方法和基于网闸的安全解决方案。为帮助读者理解网络隔离技术的概念，本书简要介绍了网络的安全威胁和目前流行的网络安全技术。为帮助读者了解网闸产品，本书简要介绍了网闸产品的基本特征和功能，以及国内外网闸产品的概况，并以一个网闸产品为实例，介绍了网闸产品的部署和配置管理。本书最后的网闸常见问题解答，有助于读者对基本概念和原理的掌握。

本书主要面向参加国家信息化安全教育认证(ISEC)考试的人员，也可供网络安全的从业人员和大专院校计算机及相关专业师生参考使用。

图书在版编目(CIP)数据

网络隔离与网闸/万平国编著. —北京：机械工业出版社，2004.4
(国家信息化安全教育认证(ISEC)系列教材)
ISBN 7-111-14169-5

Ⅰ.网… Ⅱ.万… Ⅲ.计算机网络—安全技术—资格考核—教材
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2004)第 019296 号

机械工业出版社(北京市百万庄大街 22 号　邮政编码 100037)
责任编辑：孙　业
责任印制：洪汉军

三河市宏达印刷有限公司印刷 ·新华书店北京发行所发行

2004 年 4 月第 1 版·第 1 次印刷
787mm×1092mm 1/16·8 印张·192 千字
0 001—5 000 册
定价：15.00 元

国家信息化安全教育认证(ISEC)专家组

卿斯汉　中国科学院信息安全技术工程研究中心主任　研究员
曲成义　中国航天科技集团公司第710研究所总工　研究员
许榕生　中国科学院高能物理研究所计算中心研究员
贾颖禾　国务院信息化工作办公室网络与信息安全组研究员
曹元大　北京理工大学软件学院院长　博士生导师
杨义先　北京邮电大学信息安全中心主任　博士生导师
林　鹏　国家计算机网络应急技术处理协调中心广东分中心副主任
　　教授级高级工程师
祁　金　公安部公共网络信息安全监察局管理监察处副处长
景乾元　公安部公共网络信息安全监察局安全对策处副处长
万平国　国际信息战略研究中心理事　中网通讯网络有限公司董事长
刘宝旭　中国科学院高能物理研究所计算中心副研究员

教材编委会

主　任：宋　玲
副主任：赵小凡　张会生　欧阳满　蔡金荣　沈志工
成　员：洪京一　张宝泰　王　宏　孙论强　彭　澎　张晓伟
　　刘树安　刘　旸　马志谦　胡　铮　宁宇鹏　阎　慧
　　王　伟　薛静锋　辛　阳

出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前　言

由于网络隔离与网闸技术还很新，了解并熟悉网络隔离与网闸技术的人还不多，容易出现这样或那样的误解。所以本书把重点放在网络隔离与网闸技术的概念、原理和应用上，特别是行业应用对网络隔离与网闸的特殊要求和解决方案上。如果你是一位网络安全方面的专家，经常参加安全方案的制订和评审；如果你是一个单位的信息安全主管，正准备使用网络隔离与网闸；如果你是网络安全的从业人员，需要了解网络隔离与网闸技术和产品；如果你是一个系统集成商，准备将网络隔离与网闸集成到方案中去，那么这本书对你了解网络隔离与网闸技术会有所帮助。

本书详细地阐述了网络隔离技术的原理，网闸技术的实现，应用协议的隔离和数据交换原理，网闸的测试原理与方法和基于网闸的安全解决方案。为帮助读者理解网络隔离技术的概念，本书简要介绍了网络的安全威胁和目前流行的网络安全技术。为帮助读者了解网闸产品，本书简要介绍了网闸产品的基本特征和功能，以及国内外网闸产品的概况，并以一个网闸产品为实例，介绍了网闸产品的部署和配置管理。本书最后的网闸常见问题解答，有助于读者掌握网闸的基本概念和原理。

阅读本书的读者应具有计算机软、硬件基础知识，掌握 Internet 基础知识，TCP/IP 协议，了解有关网络安全、防火墙和网络应用等方面知识。

在本书出版之际，我要感谢何德全院士的指导，国家信息安全产品测评认证中心的吴世忠主任的帮助，国家保密局及其保密技术研究所、公安部十一局和公安部计算机信息系统安全产品质量监督检验中心的大力支持；感谢我的同事王骏、谢经荣、黄慧明、王小东、胡炳强、阎峰和宋永柱，以及本书审校和图片制作人员柴晓松、杨宏伟、彭静、李媛媛和高科的帮助。最后感谢我的妻子黄艳和我的家人，在写作本书的过程中正好赶上春节，是他们的鼓励和帮助，才使本书顺利完成。因作者水平有限，书中错误和不妥之处在所难免，诚请读者提出宝贵意见。

万平国

目　录

第 1 章　网络隔离技术的起源和现状

本章导读：

本章简要地介绍了网络隔离的概念来源和变迁，介绍了网络隔离技术在美国、以色列、俄罗斯和我国的发展，对比了简单隔离技术与网闸技术，归纳了国内目前流行的网络隔离技术的产品和方案。

网络隔离，是指两个或两个以上的计算机或网络，不相连，不相通，相互断开。不需要信息交换的网络隔离很容易实现，只需要完全断开，既不通信也不联网就可以。但需要交换信息的网络隔离技术却不容易，甚至很复杂。以下讨论的所有的网络隔离技术，都是指在需要信息交换的情况下，实现网络隔离。

1.1　网络隔离技术的概念

1.1.1　网络隔离技术的概念来源

网络隔离是一个复杂的系统概念，而且与人们的常识表面上看是矛盾的。既要隔离又要交换数据，这怎么可能？人们的印象是要交换数据就要联网，要隔离就不能交换数据。但实际上是不矛盾的。要回答这个问题，我们需要了解网络隔离的概念来源。网络隔离的概念部分源于人工拷盘、Sneakernet 和轮渡。

1. **人工拷盘**

人工拷盘是已知的最早的网络隔离技术。最早的计算机是单机的，不同的计算机还没有联网。没有联网的两台计算机之间要交换数据，最简单的办法是人工拷盘。计算机操作人员将需要交换的数据，先从源计算机复制到一个磁盘里，再将数据复制到目的计算机里。要特别强调，在人工拷盘的任何时刻，两台计算机之间是完全断开没有联网的。当计算机操作人员在一台计算机里拷盘时，与另外一台计算机是完全断开的；当计算机操作人员把磁盘拿出的时候，与两台计算机都是完全断开的；当计算机操作人员把文件数据复制到目的计算机时，与原来的计算机是完全断开的。在任何时候，两台交换文件数据的计算机，总是断开的。

人工拷盘并不是天生的安全技术，而是数据交换技术。到今天为止，人工拷盘依然是最广泛使用的数据交换技术之一。人工拷盘技术也有局限性，存在潜在的内容安全问题，交换的数据本身可能带有病毒，从而感染另外一台计算机。但它不是网络安全问题，不存在攻击和入侵之类的威胁。

一个典型的人工拷盘的交换过程如图 1-1 所示。

在互联网广泛应用的今天，经常会碰到网络故障或网络断了，用户因此无法通过网络得到信息或交换数据。时间长了，用户的印象是网络断开就无法交换数据。这个印象对理解网络隔离是一个非常大的障碍。之所有要强调人工拷盘，就是要让用户知道，在网络隔离的情况

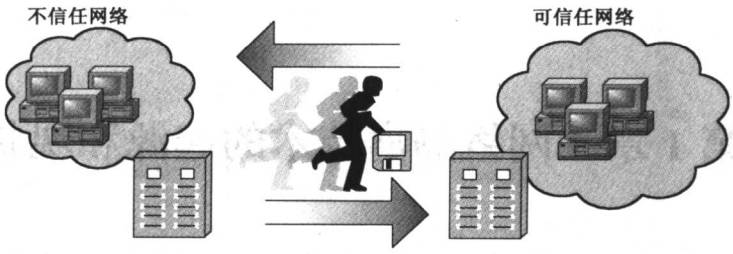

图 1-1 人工拷盘示意图

下,两个主机之间是可以通过非网络方式如拷盘来交换静态可携带的文件数据。

2. Sneakernet

人工拷盘利用软盘来实现文件数据交换,但并不是只有软盘才能交换文件数据。除软盘外,磁带、热插拔硬盘、可擦写光盘以及今天流行的 USB 存储盘,都可以实现文件数据交换。人在两台计算机或两个网络之间使用软盘、磁带等可移动的存储介质来交换文件或数据,这样两个隔离的计算机或网络与人一起构成了一个逻辑上的虚拟网络,如图 1-1 所示,用人工拷盘不足以全面、正确地描述这种逻辑关系。于是出现了 Sneakernet(人力网)这个词。

很多用户不理解为什么叫 Sneakernet? 因为 Sneaker 是个贬意词,具有讽刺的意思,意为悄悄地走动,鬼鬼祟祟做事的人,暗指秘密地行为,有点偷跑的意思。这是有原因的。Sneakernet 这个词出现在 20 世纪 80 年代末。那个时候网络是一个高级而又时尚的新东西,很多人比较喜欢往网络上靠,沾上网络的边就是好东西。利用移动介质人工手动地交换数据,把两个没有联网的网络在逻辑上联系起来,说它是一个网络,总有点底气不足,所以用了这么一个调侃的名词。虽然 Sneakernet 不是一个真正的网络,但实现了网络所实现的数据交换,因此与网络也沾得上边。

在研究网络隔离的时候人们发现,如果网络隔离就不能真地联网,但又需要交换数据。而 Sneakernet 是一个很好的原型,所以在一些网络隔离的资料中,常常提到 Sneakernet 这个词。Sneakernet 在技术字典中的定义是,悄悄地将文件或数据复制到软盘或磁带等可移动介质上,然后将移动介质带到另外一台计算机上,再将文件或数据复制给这台计算机。

迄今为止,Sneakernet 还是一次性携带大数据最有效的方法。因为这两个网络是隔离的,只能人为地交换合法数据,所以它具有很高的安全性。这种方式现在还是要害部门在两个隔离网络之间交换数据的主要方法。但其主要缺点是不能实时交换数据,在需要频繁交换数据时效率太低,不能满足现在实时交换数据的应用需要。

3. 轮渡

网络隔离有多种方式,其中最重要的一种方式是网闸。网闸的概念主要是源于轮渡。

河流在古代战争中经常被作为屏障,因此被赋予安全的含义。在电影里常见的镜头是甲方追杀乙方,到达一条人不借助工具就无法渡过的河流,这时会出现两种常见但绝然相反的结果。如果没有轮渡的工具,对乙方来讲,就是绝地。如果乙方有轮渡的工具,甲方则往往只能在岸边兴叹。

轮渡是指河流断开了传统的交通工具如汽车的路线,人被迫从汽车上下来,改乘轮船,渡过河流,到达对岸后,从轮船上下来,再改乘汽车或其他的交通工具。轮船在河流里开动时,与

两岸是完全断开的。两岸在任何时候都是完全断开的。

对轮渡的工作机理的借鉴，大大地推动了网络隔离的研究发展，直接导致网闸技术的出现。“下车改乘轮船”的现象启发我们研究协议的剥离技术，“下船改乘汽车”的现象启发我们研究协议的重建技术，“轮船载人渡河”启发我们研究文件“摆渡”，最后实现了在两网断开的情况下可以进行数据交换。从两台主机在断开的情况下可以实现数据交换，到两个网络之间在断开的情况下也可以实现数据交换，是一次质的飞跃。

1.1.2　网络隔离技术的概念变迁

到目前为止，并没有完整的关于网络隔离技术的定义和标准。从不同时期的用词也可以看出，网络隔离技术一直在演变和发展。较早的用词为 Physical Disconnection，Disconnection 有使断开、切断、不连接的意思，直译为物理断开。这种情况完全可以理解，当保密网与互联网连接后，出现很多问题，在没有解决安全问题或没有解决问题的技术手段之前，先断开再说。后来有的用词为 Physical Separation，Separation 有分开、分离、间隔和距离的意思，直译为物理分开。因为发现完全断开也不是办法，互联网总还是要用的，所以采取的策略多为该连的连，不该连的不连。该连的部分与不该连的部分要分开。也有的用 Physical Isolation，Isolation 有孤立、隔离、封闭、绝缘的意思，直译为物理封闭。因此，希望能将一部分高安全性的网络隔离封闭起来。再后来多使用 Physical Gap，Gap 有豁口、裂口、缺口和差异的意思，直译为物理隔离，意为通过制造物理的豁口，来达到隔离的目的。Physical 这个词显得非常僵硬，于是有人用 Air Gap 来代替 Physical Gap。Air Gap 意为空气豁口，很明显在物理上是隔开的。但有人不同意，理由是空气豁口就“物理隔离”了吗？没有。电磁辐射、无线网络、卫星等都是空气豁口，却没有物理隔离，甚至连逻辑上都没有隔离。于是，现在大家不太强调 Physical 这个词，不主张过分强调物理上断开，认为物理隔离本身无法准确从技术上来定义。现在，一般称 Gap Technology，意为网络隔离，成为互联网上的一个专用名词。

网络隔离在我国也经历了一个概念澄清的过程。我国最早对网络隔离的表述为“不得直接或间接地与国际互联网或者其他公共信息网络相连接，必须实行物理隔离”，意思是不准进行网络连接。人们早期并不知道网络隔离的技术架构是什么，但人们对网络安全的要求是明确的，要消除一切潜在的网络安全威胁。第一个阶段采取的策略是从严，“物理隔离”这个词就诞生了。在“物理隔离”的技术定义上出现了一些歧义。有一种观点认为，任何有物理接触的都不是物理隔离。后来发现这种理解不行，两台计算机放在桌子上，在物理上桌面与两台计算机是连接的，你能说它进行了网络连接，显然没有，它是断开的。隔离卡现在被定义为物理隔离卡。按照上述观点，隔离卡的两个网口可是在同一块电路板上，也应该不是物理隔离的，但实际上隔离卡已经被认定是物理隔离的。反过来，没有物理连接就是物理隔离的？也不是，现在已经开始发展太空中的互联网。无线联网可以在真空中进行。因此，没有现实中的物理连接也可能是联网的。要给出“物理隔离”在技术名词上的定义是困难的，甚至不可行。

第二个阶段采取的策略是从宽，“安全隔离”这个词就诞生了，“安全隔离”是我国对网络隔离的另外一种提法。这种观点主张，从物理隔离走向安全隔离，主张以安全隔离来代替物理隔离。放宽要求之后，一下出现了大量的产品。为了减少从宽的策略带来的风险，“安全隔离”被限制在一定的场合下使用，在另外一些场合下被禁止使用。安全隔离多采用直接连接的办法，

在机箱内部,用以太线将两个主机连接起来,通过协议转换的方式,进行联网。协议转换增加了一些安全性,但没有发现与虚拟专用网(VPN)有什么本质的不同。另外,安全隔离还是一种网络直接连接的方式,两个网络还是联网的,这与不准进行网络连接,不准联网,是矛盾的。

国外国内的趋势都是用网络隔离这个名词。用网络隔离来代替物理隔离或安全隔离等名词的理由很多。首先,隔离的概念是基于网络来谈隔离的。没有联网就没有隔离的必要,离开网络来谈隔离是没有意义的。其次,没有信息交换或资源共享的概念,也谈不上隔离。两个完全独立的网络,一不需要信息交换,二不需要共享资源,本身就是完全不相关的,既不需要联网也不需要隔离。因此,隔离的本质是在需要交换信息甚至是共享资源的情况下才出现,既要信息交换或共享资源,又要隔离。三是物理隔离和安全隔离无法给出一个技术上的精确定义,而网络隔离可以给出一个完整准确的技术定义。

1.2 网络隔离技术的发展与现状

1.2.1 网络隔离技术的发展

美国是最早研究网络隔离技术的国家,主要应用在军方。计算机本来是独立的,因为要信息共享和交换才发展联网技术。联网技术的发展直接导致大规模的联网。联网出现了安全问题,所以要研究网络隔离。下面首先简单地回顾一下联网,特别是互联网的发展历程:

- 20 世纪 60 年代末,美国国防部高级研究计划署(DOD Advanced Research Project Agency,ARPA)建立了著名的 ARPANET。它是由四个节点组成的分组交换网,是最早出现的计算机网络之一。
- 20 世纪 70 年代,ARPANET 从一个实验性网络变成一个可运行网络。在 ARPANET 不断增长的同时,ARPA 开发研制了卫星通信网与无线分组通信网,并想将它们联入 ARPANET,由此导致网络互连协议 TCP/IP 的出现。对该网的基本要求之一是,即使它的基本结构中的很大一部分消失,它也能继续工作。
- 20 世纪 80 年代初,TCP/IP 协议成为军用标准,1983 年 1 月 1 日美国国防部通信局正式将 TCP/IP 作为 ARPANET 的网络协议,与此同时,在当时流行的 BSD UNIX 内核集成了 TCP/IP,推动了 TCP/IP 协议的进一步研究和应用。同年,ARPANET 分为独立的两部分,一部分仍叫作 ARPANET,用于研究工作,另一部分是 MILNET,用于军方非机密通信。ARPANET 的一个副产品是网络互联的概念——将独立的网络联接成为一个整体。在 ARPANET 的 TCP/IP 协议制定之后,这种互联开始实现,于是形成了一个"由网络组成的网络",技术术语称为网间连接(Internetworking)。这个网际网络称为 Internet,就是今天的互联网。
- 20 世纪 80 年代中后期,美国国家科学基金会(National Science Foundation NSF)围绕其六个超级计算机中心建立了 NSFNET 并与 ARPANET 相连。NSFNET 代替 ARPANET 成为 Internet 的新主干。
- 20 世纪 90 年代,Internet 以惊人的速度继续商业化发展,成为全球连接范围最广、用户最多的互联网络。

美国军方在 20 世纪 80 年代和 1999 年 11 月，两次明确要求把军方的网络与互联网断开一段时间。尽管互联网的前身实际是美国军方的一个实验网，即 APPANET，后来转移给美国国家科学基金 NSF，让大量的高校和研究机构介入。到 20 世纪 80 年代，大量的商业公司开始介入互联网，开始了互联网的商业化。美国军方此时发现了大量的攻击，这些攻击正是来自学校和商业公司的网络，因此大规模地断开了一段时间。于是提出了对网络隔离技术的研究。这时用得最多的是 Sneakernet 技术。

以色列也是最早研究网络隔离技术的国家。以色列是一个非常特殊的国家，以色列与周边国家的关系紧张，因此以色列非常重视安全，在网络安全上也不例外。早期的应用也是在军方。后来一些军方的研究人员退休后，纷纷开起商业公司，专门研究网络隔离技术和产品，因此是商业化最早的国家。后来这些公司纷纷搬到美国。这些公司包括鲸鱼通信公司，矛头安全公司等。无论是隔离卡，还是网闸，以色列在这些技术上都是领先的。

俄罗斯人 Ry Jones，也是最早研究网络隔离技术的研究人员。Ry Jones 采用 OPENBSD 操作系统，基于 SCSI 技术来实现网络隔离，在当时是比较先进的。

我国提出物理隔离是在 20 世纪 90 年代的中后期。同其他国家的情况不同，率先提出的不是军方，而是国家保密局。这一点对我国的网络隔离技术的研究有很大的影响，后来的技术路线较多地强调防泄密，就与此有关。1997 年中央提出了涉密网络要同步建设保密措施，在经过主管部门审批后才能投入使用。根据国家保密部门公开的文献资料，当时国内大部分涉密网络的安全保密防护措施非常薄弱，有的甚至处于空白状态，同时涉密网络的使用管理没有明确要求，缺少规范化，存在很多泄密的隐患和漏洞。这样的系统或网络如果再与互联网相连，将很难保证存储在网络中的国家秘密信息的安全。因此，针对我国安全保密技术手段尚不完备、对操作系统和网络设备的关键技术尚未掌握，不足以抵御高技术窃密的客观情况，国家保密局在 1998 年发布的《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》中，最早提出了“物理隔离”要求。文中明确规定：涉密系统不得直接或间接与国际联网，必须实行物理隔离；2000 年 1 月 1 日正式实施的《计算机信息系统国际联网保密管理规定》中也明确规定：“凡涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或者其他公共信息网络相连接，必须实行物理隔离。”在这样一个大背景下，我国开始了对网络隔离技术的研究。

1.2.2　网络隔离技术的研究现状

1. 国外网络隔离技术的现状研究

美国、以色列、俄罗斯等国家都实行内部网与公共网的网络隔离，在网络隔离方面的技术和产品也比较多。从总体上来看，大致可以分为简单隔离技术和网闸技术。

(1) 简单隔离技术

隔离技术在理论上可分为终端级和网络级两个层次。终端级是通过存储器的隔离实现的，在单硬盘上划分安全区、非安全区以及交换区，通过使用特制的隔离卡，使安全区和非安全区的控制逻辑具有排他性，以达到信息隔离的效果；网络级的隔离通过在终端上使用特制的网络隔离卡，与安全集线器相配合，通过网络隔离卡上电信号的高低选择相应的网络进行连接，做到不能同时连接安全和非安全网络，与终端存储器的隔离相配合达到信息隔离的效果。

(2) 网闸技术

网闸的主要原理是由两套各自独立的系统分别连接安全和非安全的网络,两套系统之间是一个类似"网闸"的装置,保证存储介质与安全的网络连通时,断开与非安全网络的连接;当与非安全网络连通时,断开与安全网络的连接,分时地使用两套系统中的数据通路进行数据交换,以达到隔离与交换的目的。在数据交换过程中要进行防病毒、防恶意代码等信息过滤,以保证信息的安全。

2. 国内网络隔离技术的研究现状

根据国家保密局公开的文献资料,我国目前流行的网络隔离技术的产品和方案,主要分为五类。

方案一:建设两个独立的网络,一个是内部网络,用于存储、处理、传输涉密信息;一个是外部网络,与 Internet 相连。两个网络之间如果有数据交换需要,则采用人工操作(如通过软盘、磁带等)的方式。

方案二:采用安全隔离计算机(终端级解决方案),用户使用一台客户端设备联接内部网络和外部网络。主要类型可分为:

(1) 双主板,双硬盘型:在一个机箱内设置两套计算机设备,相当于两台计算机共用一台显示器,通过客户端开关分别选择两套计算机系统。

(2) 单主板,双硬盘型:客户端通过增加一块隔离卡、一块硬盘,将硬盘接口通过添加的隔离卡转接到主板,网卡也通过该卡引出两个网络接口。通过该卡控制客户端存储设备,同时选择相应的网络接口,达到物理隔离的效果;另外一种方案是在主板 BIOS 等更底层的技术方面进行设计,做到不同的网络选择不同的硬盘,达到物理隔离的目的。

(3) 单主板,单硬盘型:客户端需要增加一块隔离卡,但不需要额外增加硬盘,将存储器通过隔离卡连接到主板,网卡也通过隔离卡引出两个网络接口。在原有硬盘上划分安全区、非安全区,通过该卡控制客户端存储设备分时使用安全区和非安全区,同时选择相应的网络接口,达到物理隔离的效果。

方案三:采用安全隔离集线器(集线器解决方案),主要解决房间和楼层单网布线的问题。这种集线器需要和专用的安全隔离计算机相配合,只采用一个网络接口,通过网线将不同的网络选择信号传递到网络选择器,根据不同的选择信号,选择不同的网络连接。

方案四:属于物理隔离的远程安全传输方式,包括使用独立铺设线路和交换设备方式;在具备相应的认证和链路加密措施的前提下,使用面向连接的电路交换方式(如 PSTN、ISDN、ADSL 等);使用永久虚电路(PVC)交换方式(如在 DDN、X.25、帧中继和 ATM 中使用永久虚电路构建的专线)。

方案五:采用网闸的网络隔离方案。网闸的外部主机连接外部网络,网闸的内部主机连接内部网络,网闸的外部主机和内部主机是完全网络隔离的,支持文件、数据或信息的交换。

1.3 练习题

一、单项选择题

1. 下列关于人工拷盘的陈述中,正确的是(　　)。

A. 人工拷盘导致两个断开的主机相连接
B. 人工拷盘导致两个连接的主机断开
C. 人工拷盘使两个断开的主机交换信息
D. 人工拷盘使两个断开的主机实现网络通信

2. 下列关于人工拷盘的陈述中，正确的是(　　)。
A. 人工拷盘可能传播病毒或恶意代码
B. 人工拷盘存在攻击和入侵之类的威胁
C. 人工拷盘能够彻底阻止病毒传播
D. 人工拷盘确保主机之间交换信息绝对安全

3. 人工拷盘(　　)的攻击。
A. 不存在基于网络　　B. 存在基于网络层
C. 存在基于 TCP/IP 协议　　D. 存在基于应用协议

4. 网闸源于(　　)的概念。
A. 轮渡　　B. 水闸
C. 拉闸限电　　D. 单个开关

5. 拷盘是(　　)。
A. Sneakernet　　B. 网络通信
C. 不是 Sneakernet　　D. 网络数据处理

6. 研究隔离技术的国家主要有(　　)。
A. 美国、以色列、俄罗斯和中国等　　B. 不是中国。
C. 不是美国　　D. 不是以色列

7. 两个主机之间没有有线连接，(　　)。
A. 一定是物理隔离　　B. 可以无线通信
C. 一定是安全的　　D. 不能网络通信

8. 两个主机之间有有线连接，(　　)。
A. 也可能不能交换数据　　B. 一定能够交换数据
C. 不能实现网络层断开　　D. 不能实现应用层断开

9. 下列关于网闸的陈述，正确的是(　　)。
A. 网闸不是网络隔离技术　　B. 网闸是网络隔离技术
C. 网闸不是网络安全产品　　D. 网闸是隔离卡

10. 网闸技术的英文术语是(　　)。
A. GAP Technology　　B. Sneakernet
C. DISCONNECTION　　D. SEPARATION

二、简答题

1. 简述网络隔离的起源。
2. 简述常见的网络隔离技术。
3. 简述常见的网络隔离产品和方案。

第2章　网络安全概述

本章导读：

本章归纳了网络攻击的类型，介绍了TCP/IP原理及其OSI通信模型，讨论了各种网络攻击在TCP/IP模型各层的定位。介绍了目前安全技术的手段及其局限性。详细讨论了防火墙的架构，并提出了网络隔离的新思路。

在深入地讨论网络隔离技术之前，有必要先讨论来自网络的安全威胁。如果没有来自网络的安全威胁和风险，可能就没有人去研究网络隔离技术了。只有全面地了解这些来自网络的安全威胁后，才能准确、全面地从技术标准和规范上，定义什么是网络隔离技术。

要详细地说明来自网络的安全威胁，可能写一本书甚至是几本书，也不一定能把这个问题说全面、说清楚。本书不打算写一本包罗万象的关于网络的安全威胁的书，而是把主要的来自网络的威胁进行归类，尽可能全面地从技术类型上涵盖目前存在的主要的安全威胁。本章先从人们常见的攻击类型上进行总结，然后从技术上给它们进行归类。

对网络攻击的归类，有助于我们寻求解决这些攻击的解决方案。本章的后半部分详细地检查目前已有的解决方案解决了哪些问题，没有解决哪些问题，为什么没有解决这些问题，并提出新的网络隔离的解决方案。

2.1　网络攻击的类型

业界已经知道有很多种攻击，对网络的攻击，对系统的攻击，对服务的攻击，对用户的攻击。有很多种不同的方式对其进行归类研究。在本节对攻击的总结上，还是以大家熟知的方式来进行描述和总结。

(1) 入侵

对系统最常见的攻击就是入侵。一个黑客，通过入侵你的计算机或网络，可以使用你的计算机或网络的资源，甚至是完全掌控你的计算机或网络。这是一件让用户感觉非常不安全的事情。用户最担心的事情，莫过于黑客破坏、删除和修改用户的数据。造成的损失也是不可估量的。

黑客有很多办法来入侵你的系统或网络。从猜测用户的密码，到冒充内部人员诈骗管理员，要求立即修改他声称的那个用户的密码，甚至采用黑客软件来搞到密码，如利用监听工具来收集密码，或利用字典攻击法来自动强制破解系统的密码等。这一类入侵属于“搞到密码，合法地进入系统”，就像窃贼搞到了钥匙开锁入门一样。

还有一种可能，黑客没有那么文雅，而是直接破门而入。这种情况下，黑客一般是通过扫描系统来发现漏洞或缺陷，利用漏洞或缺陷来入侵系统的。事实上，这种情况在现实生活中发生得更多。

(2) 拒绝服务攻击