信息安全产品技术丛书

安全 SECURITY

隔离与信息交换产品原理及应用

丛书主编 顾健

主编 陆臻 沈亮 宋好好

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息安全产品技术丛书

安全 SECURITY

隔离与信息交换产品原理及应用

丛书主编 顾健

主编 陆臻 沈亮 宋好好

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书从理论和实践相结合的角度，介绍了安全隔离与信息交换产品的产生背景、实现原理、相关标准、应用场景和知名产品等内容。

本书内容共分 5 章，对近几年发展迅速的安全隔离与信息交换产品进行了系统而全面的介绍，具有内容新颖、实用性强、点面结合等特点。

本书可作为安全隔离与信息交换产品使用方（系统集成商、系统管理员）、产品开发人员与测试评价人员的技术参考，也可供信息安全专业的学生及其他科研人员作参考读物。

图书在版编目（CIP）数据

安全隔离与信息交换产品原理及应用 /陆臻，沈亮，宋好好主编. —北京：电子工业出版社，2011.6
（信息安全产品技术丛书）
ISBN 978-7-121- 13873-7
I. ①安… II. ①陆… ②沈… ③宋… III. ①信息系统－安全技术－工业产品－研究 IV. ①TP309

中国版本图书馆 CIP 数据核字（2011）第 118337 号

策划编辑：李 洁 （lijie@phei.com.cn）
责任编辑：李 洁 特约编辑：钟永刚
印 刷：
装 订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编：100036
开 本：787×980 1/16 印张： 15 字数：333 千字
印 次：2011 年 6 月第 1 次印刷
印 数：3 000 册 定价：42.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着以电子计算机为主要载体的信息技术和以 Internet 为主要形式的网络技术的发展，信息网络的应用已经渗透到社会生活的各个角落。电子商务、电子政务等网络应用的发展和普及不仅给人们的生活带来了很大的便利，而且正在创造着巨大的财富，同时也在改变着整个社会的运行模式。

与此同时，各种利用信息系统安全弱点（不管是无意存在还是有意而设）的新型攻击正大量地被入侵者所利用，各类攻击群体在规模上迅速扩大，技能水平快速增强，攻击所造成的影响不断加重，信息系统以及信息资产所面临的安全风险和威胁也日趋提高，信息安全问题越来越成为人们关注的焦点。

在这样的背景之下，网络的边界安全显得尤为重要。在某些重要的场合，传统的网络边界防护产品已经不能满足我们的要求。于是安全隔离与信息交换技术应运而生，并在这几年中得到了飞速地发展。

本书是信息安全产品技术系列丛书之一，与以往的书籍或论文不同，该书将对网络隔离产品做出前所未有的全面而深度地剖析。内容力争全面，技术分析力争深刻。从产品原理、标准、应用几大方面均有详实的介绍与分析。与此同时，本书力求实用，收集了许多实际数据与案例，期望能够给读者在安全隔离与信息交换技术上以一定的帮助。

本书的主要编写成员均来自公安部信息安全产品检测中心，常年从事端设备隔离部件产品的检测，对网络隔离产品有着深入的研究。国家标准 GB/T 20277－2006（信息安全技术网络端设备隔离部件测试评价方法）与 GB/T 20279－2006（信息安全技术 网络和终端设备隔离部件安全技术要求）均由本书作者参与编制，因此，本书具有一定的权威性。

本书第 1、第 3 章主要由陆臻撰写，第 2 章主要由沈亮、张艳撰写，第 4、5 章主要由宋好好撰写。顾健负责把握全书技术方向，并对各章节的具体编写提供了指导性意见，最后由陆臻完成全书修改和统稿工作。此外，赵婷、俞优、张笑笑、韦湘等人也参与了本书资料收集和部分章节的编写工作。由于编写人员水平有限和时间紧迫，本书不足之处在所难免，恳请各位专家和读者不吝批评指正。

在本书的编写过程中，得到了珠海经济特区伟思有限公司、上海金电网安科技有限公司和联想（北京）有限公司的大力协助，在此表示衷心的感谢！

编者

目　录

Chapter 1

第1章 综 述

本章首先对网络安全隔离进行了必要性的分析，简要介绍网络隔离实施的基本原理，并按照协议隔离和网闸两种产品介绍网络隔离产品的发展历程。从宏观上使读者对网络隔离与网络隔离产品有充分的认识，为后续章节学习具体的技术细节打下基础。

1.1 为什么要实施网络安全隔离

1.1.1 信息安全问题的产生及重要性

随着以电子计算机为主要载体的信息技术和以互联网为主要形式的网络技术的发展，信息网络的应用已经渗透到社会生活的各个角落。电子商务、电子政务等网络应用的发展和普及不仅给人们的生活带来了很大的便利，而且正在创造着巨大的财富，同时也在改变着整个社会的运行模式。其次，以互联网为代表的全球性信息化浪潮席卷而来，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展。信息技术对业务系统的影响程度，正逐渐由可以不完全依赖的辅助作用，转变为只能完全依赖的支撑作用。

【辅助阅读】信息技术角色的转变

以电来做比方，在电被发现和利用之前，整个社会的运行虽然低效，却有序。随着电的发现和应用，电对人们生活的影响程度也日渐增强，最终彻底改变了整个人类的生活方式。不知不觉中，我们已经无法摆脱对电的依赖。如果说哪天电突然没了，那整个社会必然无法保持有序的运行，哪怕是想回到古代的生活方式，短期内也已经是不可能的事情了。这是因为一方面我们已经习惯了现代的生活方式，另一方面整个社会生产体系也没有办法转变为古代的模式。

信息技术对整个社会的影响轨迹，就如同电，以及其他历史上其他伟大的发明（发现）一样，不知不觉中，整个社会都只能依赖于这些新发明，才能有序、平稳地继续运行下去。

与此同时，各种利用信息系统安全弱点（不管是无意而存还是有意而设）的新型攻击正大量地被入侵者所利用，各类攻击群体（见表 1-1）出于多种目的在规模上正迅速扩大，技能水平日渐增强，攻击所造成的影响不断严重，信息系统以及信息资产所面临的安全风险和威胁也日趋严重，信息安全问题正越来越成为人们关注的焦点。

表 1-1 不同的威胁源

威胁的来源	动 机	对不同对象的危害程度		
		个 人	组织/社会	国 家
普通黑客	五花八门，不过越来越倾向于经济性	★★★	★★	★
有组织犯罪	视组织性质而定，一般经济多于政治	★★★★★	★★★★	★★
高层次深度打击	一般为政治	（不直接受打击，但间接影响巨大）	★★★★★	★★★★★

注：★表示危害程度。

计算机联网技术的发展过程中，最初的网络技术更多的是考虑信息交互的便利性，即，如何实现各种平台的互连和信息的交互。现在正在广泛使用的 TCP/IP 协议也是被设计成了一个几乎没有安全措施的网络协议，本身并不提供任何安全机制，其安全性的不足，使得现在的网络也正面临着日益剧增的安全威胁。在各领域的计算机犯罪和网络侵权方面，无论是数量、手段，还是性质、规模，都已经到了令人咋舌的地步。例如，大家所知的黑客行为，现在的安全威胁几乎涉及了所有的操作系统，包括 UNIX 与 Windows 系列，黑客以及黑客犯罪集团在网上的攻击活动也正以每年 10 倍的速度增长，他们会利用系统的漏洞篡改发布的信息、非法进入银行等金融机构的服务器或用户终端盗取和转移资金、窃取敏感信息、发送假

冒的电子邮件进行诈骗等，给用户造成损失。另一个很大的威胁是计算机病毒，被发现十多年以来，其种类正呈几何级数增长。目前，活体病毒和木马已超过数千万种，病毒机理和变种不断演变，为检测与清除带来了很大的难度，已经成为计算机及其网络发展的一个很大的危害。除此之外，拒绝服务攻击、电子商务入侵和盗窃以及网上钓鱼和僵尸网络等，都给社会造成了巨大的危害，如机密数据被篡改和窃取、网络应用瘫痪、账户资金被窃甚至利用信息系统产生物理破坏等，都令网络用户损失惨重。

网络安全的概念，正是在这样的背景下产生的。这可以从不同角度对网络安全做出不同的解释。一般意义上，网络安全包括信息安全和控制安全两部分。国际标准化组织把信息安全定义为“信息的完整性、可用性、保密性和可靠性”；控制安全则指身份认证、不可否认性、授权和访问控制。研究和发展网络安全的目的，就是为了抵御网络攻击，在这方面，各个国家都做了巨大的努力，包括美国、欧盟、日本、俄罗斯等，当然也包括我们中国。

作为全球信息化程度最高的国家，美国拥有世界上最先进和最庞大的信息系统，对信息网络的依赖性也最大。一旦受到攻击，其后果非常严重。例如，2000 年 2 月初，美国多家著名网站遭到黑客攻击，造成的直接和间接损失超过 10 亿美元；2005 年 6 月，美国信用卡公司之一的万事达公司众多用户的银行资料被黑客窃取，酿成美国最大规模信用卡用户信息泄密案；2006 年 5 月，美国退伍军人事务部发生失窃事件，窃贼将存有 2000 多万名退伍军人个人资料的计算机硬盘偷走，造成美国前所未有的军人资料数据大规模失窃，对美国武装部队的安全构成了潜在威胁。

因此，美国一直高度重视信息安全问题，把确保信息系统安全列为国家安全战略最重要的组成部分之一，采取了一系列旨在加强网络基础设施保密安全方面的政策措施。例如，美国是世界上第一个引入网络战概念的国家，也是第一个将其应用于战争的国家。美国还建立和发展了新的军种——网军。为防止“网络 9.11”事件的发生，美国组建了网络黑客部队，严防网络恐怖袭击。美国媒体推测，奥巴马今后将采取更多措施推进美国的信息安全工作。

美国总统奥巴马 2010 年 2 月 9 日要求对美国的网络安全状况展开为期 60 天的全面评估，以检查联邦政府部门采取保护机密信息和数据的措施。负责反恐和国土安全的总统高级顾问约翰·布伦南表示，美国的国家安全和经济健康有赖于公、私部门网络空间的安全、稳定和完整。

其实，奥巴马的上述举措只是其竞选期间政策的延续，也凸显了信息安全对美国的重要性。可以说，奥巴马重视信息安全与美国多年来对信息安全的重视一脉相承。

信息技术发展和网络社会的到来，在给人类社会带来巨大进步的同时，也在深刻改变着人类的安全观念，并使国家安全面临诸多新的挑战。一方面，信息领域的争夺日益激烈，控制信息权成为新的战略制高点；另一方面，计算机病毒和黑客攻击等大量信息时代的“怪胎”应运而生，对信息化程度较高的银行、交通、商业、医疗、通信、电力等重要国家基础设施

造成严重破坏，成为影响国家安全的新威胁。为了应对这一新形势，美国、俄罗斯、日本等国已将信息安全提高到前所未有的高度。

不仅美国，俄罗斯近年来对国家信息安全的重视程度也日益提高，已将信息网络安全纳入国家安全战略，并采取不断完善网络信息安全立法、建立网络信息安全保障体系等措施维护国家的信息安全；日本政府也强调“信息安全保障是日本综合安全保障体系的核心”，采取了多种措施维护国家信息安全。

【辅助阅读】克林顿总统咨文（节选）

美国前总统克林顿在签发《保护信息系统国家计划》的总统咨文中陈述道：“在不到一代人的时间里，信息革命以及计算机进入了社会的每一领域，这一现象改变了国家的经济运行和安全运作乃至人们的日常生活方式，然而，这种美好的改变也带有它自身的风险。所有电脑驱动的系统都很容易受到侵犯和破坏。对重要的经济部门或政府机构的计算机进行任何有计划的攻击都可能产生灾难性的后果，这种危险是客观存在的。过去敌对力量和恐怖主义分子毫无例外地使用炸弹和子弹，现在他们可以把手提电脑变成有效武器，造成非常巨大的危害。如果人们想要继续享受信息时代的种种好处，继续使国家安全和经济繁荣得到保障，就必须保护计算机控制系统，使它们免受攻击。”

1.1.2 我国的网络安全问题现状

1. 计算机病毒感染情况相当严重

根据国家计算机病毒应急处理中心病毒样本库的统计，2009 年新增病毒样本 299 万个，是 2008 年新增病毒数的 3.2 倍，其中木马程序巨量增加。截至 2009 年年底，木马样本共 330 万多个，占病毒木马样本总数的 72.9%，而 2008 年这一比例只有 54%；2009 年发现新增木马 246 万多个，是 2008 年新增木马的 5.5 倍。

跟踪监测和研究分析表明，当前，计算机病毒木马本土化趋势加剧，变种速度更快、变化更多，潜伏性和隐蔽性增强、识别更难，与防病毒软件的对抗能力更强，攻击目标明确，趋利目的明显。因此，计算机用户账号密码被盗现象日益增多。病毒木马传播的主要渠道是网页挂马和移动存储介质，其中网页挂马出现复合化趋势。

【辅助阅读】金山 2009 年病毒报告

2010 年 1 月 28 日，国内知名的信息网络安全厂商金山安全正式发布《2009 年中国电脑病毒疫情及互联网安全报告》。报告显示，2009 年，金山毒霸共截获新增病毒和木马 20684223

个，与5年前新增病毒数量相比，增长了近400倍。其中IE主页篡改类病毒第一次登上十大病毒之首，成为2009年的毒王。

伴随着用户对网络安全问题的日益关注，黑客、病毒木马制作者的“生存方式”也在发生变化。病毒的“发展”已经呈现多元化的趋势，类似熊猫烧香、灰鸽子等大张旗鼓进行攻击、售卖的病毒已经越来越少，而以猫癣下载器、宝马下载器、文件夹伪装者为代表的“隐蔽性”顽固病毒频繁出现，同时小范围、针对性的木马、病毒也已经成为新增病毒的主流。

报告显示，在新增病毒中，木马仍然首当其冲，新增数量多达15223588个，占所有病毒总量的73.6%。黑客后门和风险程序紧随其后，这三类病毒构成了黑色产业链的重要部分。而且网站挂马的现象也显著增加。从2009年开始，金山网盾对互联网网页挂马进行全面监控。据不完全统计，全年共检测到8393781个挂马网站。此外，欺诈类钓鱼网站的数量也在2009年下半年迅猛增长，仅12月，金山网盾共拦截钓鱼网站达1万多个。

此外报告也显示，2009年，金山毒霸共拦截病毒攻击8440631705次（约84亿次），全国共有76409010台（约7600万台）计算机感染病毒。其中广东、江苏、山东三地的病毒感染量位列全国前三位，总感染量占到全国感染量的25%。

2. 黑客活动已形成重要威胁

网络信息系统具有致命的脆弱性、易受攻击性和开放性，从国内情况来看，目前我国95%与互联网相联的网络管理中心都遭受过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点。

据有关抽样数据显示，仅2009年我国被境外控制的计算机IP地址就达100多万个，被黑客组织篡改的网站多达4.2万个；在受网络病毒威胁方面，2009年我国仅被“飞客”蠕虫一种网络病毒感染的计算机数量每月就达1800万台，占全球感染主机总量的30%，位列全球第一。在上述受攻击的计算机中，不仅涉及大量网民，而且涉及金融、交通、能源等多个部门，对我国经济发展和人民正常生产生活造成严重危害。

3. 信息基础设施面临网络安全的挑战

面对信息安全的严峻形势，我国的网络安全系统在预测、反应、防范和恢复能力方面存在许多薄弱环节。据英国《简氏战略报告》和其他网络组织对各国信息防护能力的评估，我国被列入防护能力最低的国家之一，不仅大大低于美国、俄罗斯和以色列等信息安全强国，而且排在印度、韩国之后。近年来，国内与网络有关的各类违法行为以每年30%的速度递增。

2009年7月中旬，公安机关对全国政府网站进行了为期一个月的网站安全漏洞和被攻击情况抽样检测，经对23000多家抽取的政府网站检测发现，154家政府网站遭网络攻击；

经对 6000 余家政府网站检测显示，37%的政府网站存在网页安全漏洞，极易遭到网页篡改和网页挂马等攻击破坏。政府网站安全状况亟待改进，亟须采取措施消除安全隐患，加强安全保护。

4. 利用网络进行政治颠覆活动频繁

近年来，国内外反动势力利用互联网组党结社，进行针对我国党和政府的非法组织和串联活动，猖獗频繁，屡禁不止。尤其是一些非法组织有计划地通过网络渠道，宣传异教邪说，妄图扰乱人心，扰乱社会秩序。例如，据媒体报道，“法轮功”非法组织就是在美国设网站，利用无国界的信息空间进行反政府活动。

信息安全问题日益突出，已经成为影响我国国家安全、社会稳定和人民生活的大事。

不想面对这些网络安全问题的方法就是不联网，或者是将自己的内部办公网络与其他任何网络特别是互联网断开，这样的结果可以一定程度上保证自己的数据安全。事实上长期以来我国对于关键网络的保护正是这样做的。但是，随着如今电子商务与电子政务的开展，对于很多业务应用而言，不联网已经成为不可能。

网络安全隔离技术及其产品，正是在这一背景之下被提出和发展起来的。

1.1.3 网络安全隔离的必要性

网络安全问题的根源在于，一个完整的网络，是基于网络可识别的网络协议基础之上的各种网络应用的完整组合，包括协议本身和应用本身都有可能存在问题。

【辅助阅读】“飞地”（enclave）的概念

“飞地”是在单一统辖权控制之下的物理环境，具有人事和物理安全措施。它通常包括多个带有用户平台、网络/应用程序/通信服务器、打印机与本地交换/路由设备等计算资源组件的局域网。这些有单一安全策略进行管理并无须考虑其物理位置的局域计算设备构成了一个“飞地”。

飞地边界保护关注的是如何对进出该飞地的数据流进行有效的控制与监视。常用的飞地边界保护设备包括防火墙、虚拟专用网（VPN）及远程用户的标识与鉴别（I&A）/访问控制，当然也包括本书的主角——网络隔离与信息交换产品。

因此，网络安全问题就包括了网络所使用的协议的设计问题，也包括了协议和应用的软件实现问题，当然还包括了人为的因素以及系统管理失误等网络安全问题，这些方面的网络安全问题，如表 1-2 所示。

表 1-2 常见安全问题

问题类型	问题点	问题描述
协议设计	安全问题常被忽视	一般设计人员制定协议之时，通常首先强调功能性，而安全性问题则是到最后一刻、甚至不列入考虑范围。在网络应用环境下，安全问题必须更加注意
	架构在其他问题之上	选用其他基础协议时，必须要注意该协议是否易于了解、易于操作。就算费尽心思制作完善的协议，若架构在不固的基础上，其结果可想而知
	流程问题	设计协议时，可能考虑不够周全，导致发生状况时，系统处理方式不当。
	设计错误	协议设计错误，导致系统服务容易失效或容易遭受到攻击
软件实现	实现错误	就算协议制定正确，实现协议时若发生错误，或实现人员对协议的认知错误，同样会导致安全漏洞
	程序错误	安全漏洞也常因程序撰写习惯不良引起，其中包括常见的未检测资料长度内容、输入资料容错能力不足、未检测可能发生的错误、应用环境的假设错误、引用不当模块、未检测资源不足等
人员操作	作业疏失	最严格的规定，若操作人员未受过良好训练、或未按手册操作，同样会导致安全的漏洞
系统维护	配置不安全	许多软件或操作系统在安装完成后，是处于极度不安全的配置状况下。而这些预设环境背后的理由竟是为了方便用户，诚然，用户是方便了，不过此处所指的用户，范围也同时包含了病毒、蠕虫、特洛伊木马等不速之客
	未修补系统	一般软件多多少少都会有些错误，勤于修补才能让系统免遭破坏
	萧墙祸起	对系统发起攻击的，通常是你信任的系统。在你信任的领域里若存在不够安全的系统，这些不够安全的系统很快就会成为下次攻击的跳板。一个领域的安全强度，等同于该领域中最不安全系统的安全强度

为了解决目前面对的众多计算机和网络安全问题，针对表 1-2 中所讨论的各类问题，人们开发了各种安全技术来解决计算机网络安全问题。这些技术包括访问控制技术、识别和鉴别技术、密码技术、完整性鉴别技术、审计和恢复技术、防火墙系统、计算机病毒防护、安全操作系统、安全数据库和抗抵赖协议等，也相继推出了包括防火墙、入侵检测、防病毒软件、CA 系统等在内的各类网络安全产品，这些技术和安全产品在一定程度上对网络系统提供了一定的安全防范。但是，因为这些技术和产品都是针对网络安全的一个方面实现的网络安全防范措施，因此无法对整个网络系统提供有效的保护。

下面以最常见的网络边界防护产品防火墙为例来说明。

1. 产品安全功能缺陷

普通防火墙的安全功能很难解决的问题：恶意代码流入；敏感信息流出。

由于包过滤防火墙只在网络协议的第二层、第三层和第四层对数据包进行过滤，而应用级防火墙虽然在第七层对数据有过滤，但一般只针对协议的命令进行过滤，而不会对数据包内容进行判断，所以对待如上所列的两个问题，防火墙都无法解决。

虽然从理论上说，深度包检测功能的发展，使得防火墙对上述问题的解决有了希望，但是，由于技术上的限制、性能上的制约，防火墙的深度包检测很难做到对数据的彻底剥离与检查。

厂商或者专家也许可以把饼画得很圆很大，设计出一款深度包检测能力很强的“超级”防火墙。然而事实上，由于防火墙所部署的应用环境非常复杂，厂商出于产品通用性的考虑，必须最大限度地提升防火墙的性能，以使其尽可能多的适应不同的应用环境。因此，防火墙不可能也没有必要对数据内容进行完全地、高强度地深度检测。

2. 产品自身安全缺陷

原始的包过滤防火墙容易受到如下攻击：IP 欺骗攻击；DOS 拒绝服务攻击；分片攻击；木马攻击。

基于状态检测的包过滤防火墙则比普通包过滤防火墙要安全很多，但是一样容易受到如下攻击：协议隧道攻击；利用 FTP-pasv 绕过防火墙认证的攻击；反弹木马攻击。

同时，产品本身在底层所存在的，有意或无意放置/配置的种种漏洞，也使得防火墙很难真正起到隔离内外安全域的作用。

3. 产品脆弱性后果

防火墙产品的脆弱性后果是一旦防火墙被非授权用户所控制，整个内部网络都将彻底暴露在入侵者面前，这样的脆弱性后果是十分严重的。在一些安全性要求较高的重要部门，存在这样的脆弱性后果显然是不能被允许的。

目前，在没有更为有效的安全防范产品之前，更多的用户选择防火墙这样的产品来保障自己的网络安全。然而相对应的是，新的 OS 漏洞和网络攻击层出不穷，防火墙并不能满足高安全需求的安全域的要求。因此，发展和完善隔离部件技术，已成为当务之急。

1.2 怎样实施网络安全隔离

安全隔离概念最早出现在国外，美国和以色列等国都存在此方面的技术应用和相关法规，例如，美国早在 1999 年年底就强制规定军方涉密网络必须与互联网断开。由于此类信息涉及

国家安全问题，所以国外鲜有报道。

在网闸隔离技术提出之前，协议隔离技术已经较早的在国外进行了研究，1997年，信息安全专家Mark Joseph Edwards在他编写的《Understanding Network Security》一书中就对协议隔离进行了归类。在书中他明确地指出协议隔离和防火墙不属于同类产品。再如瑞士的数据处理咨询专家E. Nyoni在2000年出版的专著《Technical Options of Computerzed World》里的“互联网Security”章节对协议隔离做了更为明确的定义和说明。

一般认为，所谓的协议隔离，是指处于不同安全域的网络在物理上是有连线的，通过协议转换（在所属某一安全域的隔离部件一端，把基于网络的公共协议中的应用数据剥离出来，封装为系统专用协议传递至所属其他安全域的隔离部件另一端，再将专用协议剥离，并封装成需要的格式）的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。

【辅助阅读】“隔离”用词的变化

从不同时期的用词可以看出，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”。这种情况是完全可以理解的，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出现之前，先断开再说。后来有“Physical Separation”，“Separation”有“分开、分离、间隔和距离”的意思，直译为“物理分开”。后期发现完全断开也不是办法，互联网总还是要用的，采取的策略多为该连的连、不该连的不连。这样的该连的部分与不该连的部分要分开。也有“Physical Isolation”，“Isolation”有“孤立、隔离、封闭、绝缘”的意思，直译为“物理封闭”。事实上，没有与互联网相连的系统不多，互联网的用途还是很大，因此，希望能将一部分高安全性的网络隔离封闭起来。再后来出现了“Physical Gap”，“Gap”有“豁口、裂口、缺口和差异”的意思，直译为“网闸”，意为“通过制造物理的豁口”，也就是“闸”，来达到隔离的目的。到这个时候，“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。现在，一般称“Gap Technology”，意为“网闸隔离技术”，成为互联网上一个专用名词。

GAP是指在不连接的网络之间提供数据传输，同时不允许这些网络间运行交互式协议的技术。在这之后，以Whale Communications公司和Spearhead公司为代表的一些美国和以色列公司借鉴了GAP的基本思想，先后提出和开发了各自的安全隔离方案和产品。该类产品利用专用网络硬件设备，使两个网络在不连通的情况下仍能实现数据安全传输和资源共享。由于GAP技术采用独特的硬件设计，能够提高内部用户网络的安全强度，现已在美国、以色列

等国家的军队、航天、金融等要害部门以及其电子政务网络中广泛采用。

在应用了 GAP 技术的网闸隔离产品中，信息以“摆渡”模式进行交换。所谓的信息摆渡是信息交换的一种方式，其物理传输信道只在传输进行时存在。信息传输时，信息先由信息源所在安全域一端传输至中间缓存区域，同时物理断开中间缓存区域与信息目的所在安全域的连接；随后接通中间缓存区域与信息目的所在安全域的传输信道，将信息传输至信息目的所在安全域，同时在信道上物理断开信息源所在安全域与中间缓存区域的连接。在任一时刻，中间缓存区域只与一端安全域相连。

该种技术对于依附于被传输信息本身进行的攻击而言，没有什么大作用，但是却防范了大部分跳跃式、渐进式攻击，因此它的存在，对飞地边界保护设备而言，还是具有重要作用的。

整个信息交换的过程有点像船闸，先连通这一头，断开那一头，把信息由左侧安全域传输到中间缓存部件，如图 1-1 所示；再断开这一头，连通那一头，把信息传输给右侧安全域，如图 1-2 所示。这就是所谓的“2+1”结构，两头是 2，中间是 1。

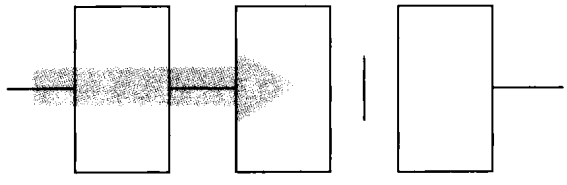

图 1-1 摆渡前

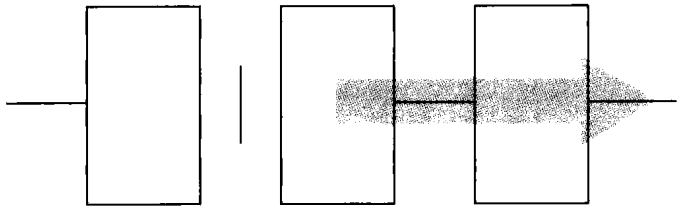

图 1-2 摆渡后

当然这只是一个示意图，硬件在真正实现的时候，并非直接做成这个样子，但是信息摆渡的原则是不变的。

由此可知，网络安全隔离的两个重要技术分别是：协议隔离技术；基于数据摆渡的 GAP 技术。

一般来说，作为一个成熟的网闸产品，也要求它具有协议隔离的功能。因此，有些标准对网络安全隔离进行了细分，有些则没有。