信息安全产品技术丛书

下一代安全隔离与信息交换产品原理与应用

丛书主编　顾健

主编　张艳　沈亮　陆臻　顾建新

中国工信出版集团

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

下一代安全隔离与信息交换产品原理与应用

丛书主编 顾 健

主 编 张 艳 沈 亮 陆 臻 顾建新

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

内 容 简 介

本书共分为五章，从下一代互联网的技术发展背景和传统威胁防护方法的局限性入手，结合 IPv6 特性对下一代安全隔离与信息交换产品的产生需求、发展历程、实现原理、技术标准、应用场景和典型产品等内容进行了全面、翔实的介绍。

本书适合安全隔离与信息交换产品的使用者（系统集成商、系统管理员）、产品研发人员及测试评价人员作为技术参考，也可作为信息安全专业的学生及其他科研人员的参考读物。

图书在版编目（CIP）数据

下一代安全隔离与信息交换产品原理与应用 / 张艳等主编. —北京：电子工业出版社，2016.1
（信息安全产品技术丛书）

ISBN 978-7-121-28041-2

Ⅰ. ①下… Ⅱ. ①张… Ⅲ. ①信息系统－安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2016）第 007086 号

策划编辑：李 洁
责任编辑：张 京
印 刷：三河市鑫金马印装有限公司
装 订：三河市鑫金马印装有限公司
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：720×1 000 1/16 印张：16 字数：296 千字
版 次：2016 年 1 月第 1 版
印 次：2016 年 1 月第 1 次印刷
印 数：3 000 册 定价：49.00 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

<<<<< PREFACE

随着我国信息化进程的快速推进和 IPv6 下一代互联网技术的迅速发展，面向 IPv4 网络的传统安全技术无论是在网络适应性方面、安全防护功能方面，还是在性能方面，都已无法满足下一代互联网的安全技术要求；同时，IPv6 下一代互联网协议虽考虑到了 IPv4 的安全问题，但也带来了更多的安全风险。

与防火墙包过滤、状态检测等技术比较起来，物理断开、分时连接技术具有更强的逻辑隔离与访问控制能力，因此，安全隔离与信息交换产品作为安全域隔离的重要技术手段，逐步在行业内得到广泛应用。

在当前信息网络不断朝 IPv6 下一代互联网协议演进的趋势下，以及 IPv6 带来的新安全形势与威胁背景下，安全隔离与信息交换系统必须进行全新的设计以应对和适应下一代互联网的应用及安全需求。从硬件设计、协议栈处理等方面优化对 IPv6 报文的处理性能，充分发挥 IPv6 的性能优势，具备未来网络带宽高速增长情况下的数据转发能力。

本书作为信息安全产品技术丛书之一，在下一代互联网发展历程、技术特点、安全需求，以及下一代互联网安全隔离与信息交换系统产品的发展历程、关键技术、实现原理、技术标准、典型应用等几大方面均进行了翔实的描述。与此同时，本书突出了下一代互联网 IPv6 的特性，收集了许多实际数据与案例，期望能够给读者在对安全隔离与信息交换产品的安全防护技术和标准的了解上提供一定的帮助。

本书的主要编写成员均来自公安部计算机信息系统安全产品质量监督检验中心，他们常年从事安全隔离与信息交换产品等信息安全产品的测评工作，对安全隔离与信息交换产品有着深入的研究。本书作者组织和参与了下一代互联网安全隔离与信息交换产品标准从规范、行标到国标制修订的工作。因此，本书在标准介绍和描述方面具有一定的权威性。

顾健作为丛书主编，负责把握全书的技术方向，第 1 章由张艳撰写，第 2 章由沈亮、顾建新撰写，第 3 章由陆臻撰写，第 4、5 章由张艳、王志佳和李旋撰写。此外，俞优、邹春明等同志也参与了本书资料的收集和部分编写工作。由于编写人员水平有限和时间紧迫，不足之处在所难免，恳请各位专家和读者不吝批评指正。

本书的编写受到了国家发改委信息安全专项“下一代互联网信息安全专项标准研制”项目（发改高技【2012】1615 号）及上海市科委 2013 年度技术标准专项“信息安全关键产品检测技术标准研究”（课题编号：13DZ0500501）的资金支持。

在本书的编写过程中，得到了珠海经济特区伟思有限公司、北京天融信网络安全技术有限公司和华为技术服务有限公司的大力协助，在此表示衷心的感谢！

编者

目录

CONTENTS

第1章 综 述

互联网发展到现在，安全问题始终与其息息相关。目前正在广泛应用的IPv4互联网协议设计是假定用户自律，位于彼此信任的小规模、封闭网络环境中，因此没有内置相关的安全机制，也没有考虑开放环境下操作系统和应用的安全问题。互联网的脆弱性表现在设计、实现、运行管理的各个环节，中间节点对传输数据包的来源不验证、不审计，导致地址、身份被假冒，垃圾信息泛滥，大量的入侵和攻击行为无法跟踪，难以溯源；用户个人信息或关键数据在网络上存储和传输都会面临风险，互联网中的数据系统、业务系统常常遭到攻击，这种情况导致当前的互联网面临层出不穷的安全威胁。IPv4互联网中解决安全问题的方式是通过各种安全技术“打补丁”，增强数据完整性、身份鉴别、访问控制等方面的安全性。以IPv4协议为核心技术的互联网面临着日趋严峻的挑战，具体表现为网络可扩展性差、地址匮乏和路由表不断膨胀；网络不可控、不可管、没有感知和测量功能，服务质量无法得到保证等。IPv6下一代互联网协议是解决目前互联网在扩展性、高性能、实时性、移动性、安全性、易管理和经济性等方面问题的主要手段，IPv6下一代互联网协议是一种典型的协议安全增强技术。IPv6通过IPSec为网络中的每个节点提供数据源认证、完整性保护和加密机制，还可以使节点有能力抵抗重放攻击。IPsec通过两个扩展报头，即认证头（AH）和封装安全载荷（ESP）将安全机制内嵌在协议之中。其中AH实现了保护数据完整性（即不被非法篡改）、数据源发认证（即防止源地址假冒）和抗重放攻击3个功能，而ESP则在AH所实现的安全功能基础上增加了对数据保密性的支持。

现有互联网IP地址尤其是B类地址资源接近枯竭，连入因特网的子网数目急剧增长，导致因特网路由表的爆炸性增长，为了支撑物联网、移动网络等下

一代互联网应用的发展，IPv6 下一代互联网协议扩大了对 IP 地址空间的范围，同时增强了对流媒体、P2P 等应用的高网络带宽支持。

随着我国信息化进程的快速推进和 IPv6 下一代互联网技术的迅速发展，面向 IPv4 网络的传统安全技术，包括防火墙包过滤技术、入侵检测技术及网络隔离与信息交换技术等，都已经无法满足下一代互联网的技术要求。在网络适应性方面，传统的 IPv4 边界防护技术缺乏面向 IPv6 网络协议的支持能力，无法解析和处理 IPv6 报文，不支持邻居发现（ND）、ICMPv6 和扩展报头等新特性，不能适应纯 IPv6、IPv4/IPv6 混合网络的应用环境。在安全防护功能方面，传统的 IPv4 边界防护设备不能有效执行 IPv6 下一代互联网环境下的地址转换、包过滤、应用代理、内容过滤、身份认证、加解密等安全功能，面向 IPv4 的传统安全隔离与信息交换技术不具备 IPv4 与 IPv6 的过渡能力，缺乏针对 IPv6 地址、认证头（AH）、封装安全载荷（ESP）等 IPv6 报文的安全处理能力，无法实现 IPv6 与 IPv6、IPv4 与 IPv6 网络间的网络隔离与信息内容过滤。在性能方面，下一代互联网对网络带宽的要求大幅提高，骨干网络带宽从千兆位向万兆位、100Gb 发展，同时，IPv6 下一代互联协议 IPv6 基本报头被固定为 40bit，使网络设备可以加快对数据包的处理速度，提高了转发效率，从而提高网络的整体吞吐量，使信息传输更加快速，安全隔离与信息交换系统需要适应这种需要，从硬件设计、协议栈处理等方面优化对 IPv6 报文的处理性能，充分发挥 IPv6 的性能优势，适应未来网络带宽高速增长情况下的网络转发能力。

虽然 IPv6 下一代互联网协议考虑到了 IPv4 的安全问题，设计了端到端的新安全机制，但 IPv6 也带来了更多的安全风险。首先，IPv6 的新安全机制是为了让 IPSec 的实施更便利，允许 IPSec 运行得更好而已，但它也只是提供了一种便利，并不是说 IPv6 本身会更安全。其次，网络节点大量使用端到端的加密方式，会对目前基于报文解析、内容扫描的安全体系造成严重影响，尤其是对安全隔离与信息交换系统的工作机制产生重要影响。最后，IPv6 在设计上仍存在缺陷，Any-cast 服务、路由头协议、Internet 控制消息协议第 6 版（ICMPv6）、碎片包、

无状态地址自动配置（SLAAC）和巨大地址数量都可能给下一代互联网带来潜在安全威胁。

面对信息网络不断朝IPv6下一代互联网协议演进的趋势及IPv6带来的新安全形势与威胁，安全隔离与信息交换系统必须进行全新的设计以应对下一代互联网对网络隔离与信息安全交换的需求，支持 IPv4 向 IPv6 的网络过渡，支持IPv6 网络环境下访问控制、身份鉴别及数据内容过滤，优化 IPv6 网络报文的应用代理转发性能与隔离摆渡交换性能，确保把有害的攻击隔离在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网络之间的数据安全交换。

安全隔离与信息交换系统结构安全可靠，具备强大的抗攻击性，作为新一代网络安全边界防御技术已经逐渐成为我国信息化建设的核心边界防护产品，尤其是在下一代互联网应用中，面对新增协议类型的安全风险不确定性，更需要采用强隔离技术手段建立 IPv4 与 IPv6 网络域隔离及 IPv6 环境下的不同域间隔离，增强可信网络的保护能力。下一代互联网的主要应用包括基于 IPv6 的物联网、移动互联网、云计算、三网融合、视频播客等，这些应用必须满足同时对各类 IPv4、IPv6 客户端、机顶盒、手机、PDA、物联传感设备等终端设备提供可信接入的安全措施，既实现数据的交换，又有效防止针对应用系统及核心业务网络的各类 3～7 层的网络攻击，而安全隔离与信息交换系统的技术原理具有独特的安全特性，能够满足用户的边界安全接入要求，包括国土资源视频监控、移动办公、数字城市、移动支付、移动警务、电子警察等应用都纷纷采用安全隔离与信息交换技术实现网络边界安全控制，随着 IPv6 的下一代互联网发展，越来越需要具有 IPv4 和 IPv6 互联互通能力的安全隔离与信息交换设备。

本章首先对下一代互联网的背景进行描述，简要介绍下一代互联网的发展情况、IPv6 协议的技术特点及下一代互联网面临的安全威胁，还分析了传统安全技术的优缺点及应用下一代安全隔离与信息交换系统的必要性。使读者从宏观上对下一代互联网安全隔离与信息交换系统的应用场景有充分的认识，为下个章节介绍具体的技术细节奠定基础。

1.1 下一代互联网背景

1.1.1 下一代互联网的发展

目前，世界上著名的下一代互联网计划（组织）及其试验网主要包括：美国的 Internet2 计划的主干网 Abilene、第二代欧盟学术网的主干网 GEANT2、亚太地区先进网络 APAN 及其主干网、跨欧亚高速网络 TEIN2 及其主干网、中国的 CNGI 及其主干网、日本的第二代学术网 SUPERSINET 和加拿大新一代学术网 CA×net4 等。

下一代互联网的主要特征有如下几点。

（1）更大。采用 IPv6 协议，使下一代互联网具有非常巨大的地址空间，网络规模将更大，接入网络的终端种类和数量更多，网络应用更广泛。

（2）更快。100MB/s 以上的端到端高性能通信。

（3）更安全。可进行网络对象识别、身份认证和访问授权，具有数据加密和完整性，实现一个可信任的网络。

（4）更及时。提供组播服务，进行服务质量控制，可开发大规模实时交互应用。

（5）更方便。无处不在的移动和无线通信应用。

（6）更可管理。有序的管理、有效的运营、及时的维护。

（7）更有效。有赢利模式，可创造重大社会效益和经济效益。

在世界范围内，由 IPv4 向 IPv6 的协议转型已经启动，下一代互联网 IPv6 具有比 IPv4 大得多的地址空间，IPv6 采用 128 位地址长度，几乎可以不受限制地提供地址，可以形象地说，地球上的每一粒沙子都能获得一个 IPv6 地址。在

IPv6 的设计过程中，除了一劳永逸地解决了地址短缺问题以外，还考虑了在 IPv4 中解决不好的其他问题。IPv6 的主要优势体现在以下几方面：扩大了地址空间，提高了网络的整体吞吐量，改善了服务质量（QoS），安全性有了更好的保证，支持即插即用，能更好地实现多播功能。

目前 IPv4 地址逐步用完，如欧洲的 IPv4 地址在 2012 年已经用完，美国也在 2015 年 3 月 20 日耗尽 IPv4 地址。亚太地区首先于 2011 年用完 IPv4 地址，我国在 2011 年至今 IPv4 地址总数基本维持不变，目前约有 3.3 亿个。

而将来选用新协议 IPv6 是必然趋势，目前已经有相当数量的互联网用户和其使用的网络已经换成 IPv6。互联网协会称："IPv6 部署的步伐正在迅速加快！谷歌测得的 IPv6 数字于 2014 年 2 月 10 日超过 3%的里程碑，而仅在不足五个月超过 2%的里程碑。在这以前，从 1%到 2%花掉 11 个月。"但截止到 2014 年 7 月，我国 IPv6 的地址数仅为约 1.7 万个，仅比 2013 年年底增长 0.1%。

互联网进入 IPv4 和 IPv6 共存的阶段，而 IPv6 的部署规模将更大。虽然 IPv6 并不等同于下一代互联网，但下一代互联网必然选择 IPv6。国际互联网普遍认同的是，互联网的核心问题是目前的 IP 地址、前缀、路由的增长态势在很长一段时期内不会改变，而且用 IPv6 取代 IPv4 是维持当前增长趋势或创造一种全新的可持续增长方式的唯一途径。

早在 2003 年 12 月，我国便启动了中国下一代互联网示范工程 CNGI 的建设。在 CNGI 示范网的试验过程中，从关键设备 IPv6 路由器到相关软件及应用，初步形成了仅次于美国的下一代互联网产业群，彻底改变了第一代互联网时期受制于人的被动局面。目前，我国三大电信运营商已经迈出了商用化的实质性步伐。中国电信率先启动向下一代互联网过渡的试点工作，在湖南长沙、江苏无锡、四川成都、广东广州、浙江杭州和山东济南等六个城市提供 IPv6 试商用工作。中国移动、中国联通也紧随其后，百度、新浪、腾讯等大型网站宣布将支持 IPv6。除此之外，IPv6 过渡还涉及 IT 支撑系统、终端等各个环节。

目前，中国下一代互联网示范工程中的相关国产设备及产品占 50%以上，部分甚至达到 80%。因此，IPv6 在提高中国在全球下一代互联网产业中的战略地位和高端装备出口的竞争力方面，是一次难得的战略发展机遇。中国下一代互联网研究与产业化获得重大突破：现已建成包括 6 个核心网络、22 个城市 59 个节点及北京和上海两个国际交换中心的网络，以及含 273 个驻地网的 IPv6 示范网络。2013 年 12 月 25 日，国家发展和改革委员会等四部委公布下一代互联网示范城市建设名单，16 个下一代互联网示范城市（群）将把 IPv6 下一代互联网作为基础设施，全面快速推进，中国下一代互联网建设将进入快车道。

中国下一代互联网示范工程中已经开展了大规模的基于下一代互联网的应用研究，如视频监控、环境监测等，并服务于北京奥运会，开通了基于 IPv6 的奥运官方网站。依托 6 大核心网，先后布置了与产业化相关的项目 103 项，参与企业多达数十家。取得了一系列具有自主知识产权的技术成果，共申请国内专利 800 多项、国外专利几十项；形成了国家标准 4 项，提交国标草案 10 多项，中国通信标准化协会等行业标准 10 多项。中国下一代互联网示范工程核心网已经完成建设任务，该核心网由 6 个主干网、两个国际交换中心及相应的传输链路组成，6 个主干网由在北京和上海的国际交换中心实现互联。目前 CERNET2、中国电信、中国网通/中科院、中国移动、中国联通和中国铁通这 6 个主干网含国际交换中心已全部完成验收。向互联网标准组织 IETF 申请互联网标准草案 9 项，已获批准 2 项，这也是中国第一次进入互联网核心标准领域。这一项目得到八个部委的联合支持，由五大全国性电信运营商和教育科研网、100 多所高校和研究单位、几十个设备制造商承担，上万人参与，产学研用合作，在中国通信网络科技工程建设史上是第一次，对中国下一代互联网技术和产业的发展具有深刻影响。由中国下一代互联网示范工程（CNGI）项目是由国家发展和改革委员会主导，由中国工程院、科技部、教育部、中科院等八部委联合于 2003 年酝酿并启动的。下一轮的互联网竞争对中国来讲是一个绝好的发展机会。在下一代互联网建设中，中国应利用自己的优势，把技术开发放在第一位，并尽快实现相关产品的产业化。

随着全球技术变革的不断加快、经济和社会的不断发展，互联网发展及其应用水平不断提高，应用领域不断拓展。随着互联网 IP 地址的枯竭，以及对互联网安全性和管理、维护、运营的更高要求，下一代互联网建设逐步受到重视。20 世纪末以来，欧美日韩等发达国家相继启动了下一代互联网研究和试验计划，力求在新一轮产业技术和国家经济竞争中占据主动，美国、欧洲、日本等发达国家和地区在审视技术路线和发展趋势后，又制定了下一代互联网发展计划。欧盟已经明确要求在 2010 年前推动 25%的个人及机构试用，美国也在今年突然加快了 IPv6 的部署与实施，所申请的 IPv6 地址从世界排名 11 位突然上升到第一位，中国仅处于第 16 位。中国在下一代互联网研究与建设上取得了一定的成果，但面临的形势依然严峻。下一代互联网的研究开发特别是产业化是一个长期过程，国际竞争日趋激烈，各方面应高度重视，并予以积极支持。在成果面前，仍需要保持清醒的头脑，增强工作紧迫感，保证中国在下一代互联网产业发展及科研上的领先优势，继续抢占国际下一代互联网竞争的战略制高点。

综上所述，互联网是人类社会重要的信息基础设施，对经济社会发展和国家安全具有战略意义，与构建和谐社会、建设创新型国家和走新型工业化道路等重大战略的实施紧密相关，需要从战略高度加以重视，中国在下一代互联网关键技术及产业上的突破，必将对中国的经济和产业转型产生重要而深远的意义，为后续发展提供重要的推动力。为抓住机遇，推进中国信息产业发展和信息化建设，促进产业发展，必须加速发展中国的下一代互联网产业。

1.1.2　下一代互联网中的 IPv6 技术

1. IPv6 的技术特点

针对目前互联网协议 IPv4 的不足，IETF 提出了下一代互联网协议 IPv6，因而其主要技术特点也是针对 IPv4 而言的。IPv6 的 128 位地址结构提供了充足的地址空间。近乎无限的 IP 地址空间是部署 IPv6 网络最大的优势。IPv6 层次化的网络结构提高了路由效率。IPv6 地址长度为 128 位，可提供远大于 IPv4 的

地址空间和网络前缀，因此可以方便地进行网络的层次化部署。IPv6 报文头简洁、灵活，效率更高，易于扩展，IPv6 和 IPv4 相比，去除了 IHL、identifiers、Flags、Fragment Offset、Header Checksum、Options、Paddiing 域，只增加了流标签域，因此 IPv6 报文头的处理较 IPv4 大大简化，提高了处理效率。另外，IPv6 为了更好地支持各种选项处理，提出了扩展头的概念，新增选项时不必修改现有结构就能做到，理论上可以无限扩展，体现了优异的灵活性。

（1）扩展地址，地址空间增大，IP 地址由 32 位增加到 128 位，地址结构更加层次化，地址空间增加到能支持 3.4×1038 台主机。

（2）简化头格式，IP 包头格式简化，IPv4 中的校验和、IHL（Internet Header Length）、鉴定标识、分段偏移等字段在新 IPv6 中不再保留。IPv6 仅包含 7 个字段，简化了数据报文头部，减少了路由表长度，同时，减少了路由器处理报头的时间，减少了报文通过网络的延迟。

（3）支持扩展和选项的改进，对选项的更好支持，以前必需的字段现在只是选项，更加灵活，便于分组处理。

（4）增加了流标识，可以标记数据所属的流类型以便路由器进行相应的处理，提供特定的 QoS（Quality of Service）。

（5）源端分割，只在发送者端分段，路由器不再执行分段功能，发送者应该检查所建立路径所需的最小 MTU（Maximum Transmission Unit）。

（6）路由选择：IPv6 路由与物理接口而不是接口关联（绑定）。IPv6 与 IPv4 的源地址选择功能不同。允许重复路由以提高稳健性，但在路由查找时将忽略重复路由。

（7）不需要 SUM 区域检查（Header Checksum）：在路由器中检查 SUM 区域的协议数据包被移除，数据包在网络传输前已通过检查。另外，高层协议如