信息安全产品技术丛书

下一代互联网入侵防御产品

原理与应用

丛书主编　顾健

主编　顾建新　张艳　沈亮　陆臻

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

下一代互联网入侵防御产品原理与应用

丛书主编　顾　健

主编　顾建新　张　艳　沈　臻

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书内容共分为五章，从新一代入侵防御系统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 特性对下一代互联网入侵防御系统产品的产生需求、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。

本书适合入侵防御系统产品的使用者（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书，也可以供信息安全专业的学生及其他科研人员作为参考读物。

图书在版编目（CIP）数据

下一代互联网入侵防御产品原理与应用 / 顾建新等主编. —北京：电子工业出版社，2017.9
（信息安全产品技术丛书）
ISBN 978-7-121-32693-6

Ⅰ. ①下… Ⅱ. ①顾… Ⅲ. ①互联网络－安全技术 Ⅳ. ①TP393.408

中国版本图书馆 CIP 数据核字（2017）第 223293 号

策划编辑：李 洁
责任编辑：刘真平
印 刷：北京季蜂印刷有限公司
装 订：北京季蜂印刷有限公司
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：720×1 000 1/16 印张：12.5 字数：180 千字
版 次：2017 年 9 月第 1 版
印 次：2017 年 9 月第 1 次印刷
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）88254888，88258888。

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。

本书咨询联系方式：lijie@phei.com.cn。

前言

<<<<< PREFACE

与防火墙、入侵检测系统等产品比较起来，入侵防御系统是一种能防御防火墙所不能防御的深层入侵威胁的在线部署网络安全产品，因此入侵防御系统被认为是防火墙之后的第二道安全闸门。

随着互联网技术的飞速发展，尤其是基于 IPv6 技术的下一代互联网技术的迅速发展，新型网络环境下的攻击事件孕育而生，抵御网络攻击、保护网络安全，对传统的网络安全产品提出了新的要求。

IPv6 的安全威胁与 IPv4 相比是完全不同的，安全性策略是一项很重要的基本组成部分，基于 IPv6 的入侵防御系统成为了众多安全策略中的一种非常重要的解决方案。为了适应下一代互联网的发展需求，以及更好地应对新一代威胁的挑战，入侵防御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，从数据包高速捕获、数据负载均衡、模式匹配、硬件设计、协议栈处理等方面优化对 IPv6 报文的处理性能，支持 IPv6/IPv4 双栈、纯 IPv6 等多种 IPv6 应用环境，并充分发挥 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。

本书作为信息安全产品系列丛书之一，在下一代互联网入侵防御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，期望能够对读者了解入侵防御系统产品的安全防护技术和标准

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，常年从事入侵防御系统等信息安全产品的测评工作，对入侵防御系统有着深入的研究。本书的作者牵头组织和参与了下一代互联网入侵防御系统产品标准从规范、行标到国标制修订的全部工作。因此，本书在标准介绍和描述方面具有一定的权威性。

本书由顾健作为丛书主编负责把握全书技术方向，第 1 章主要由顾建新撰写，第 2 章主要由张艳、沈亮撰写，第 3 章主要由沈亮、陆臻撰写，第 4、5 章主要由顾建新、张艳撰写。此外，王志佳、俞优、杨元原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，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。

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）的资金支持。

本书在编写过程中，得到了华为技术有限公司、北京神州绿盟信息安全科技股份有限公司、东软集团股份有限公司、启明星辰信息技术有限公司、网神信息技术（北京）股份有限公司等的大力协助，在此表示衷心的感谢！

目录

CONTENTS

第1章 综 述

互联网正以惊人的速度改变着人们的生活方式和工作效率。从商业机构到个人都将越来越多地通过互联网处理银行事务、发送电子邮件、购物、炒股和办公。这无疑给社会、企业乃至个人带来前所未有的便利，所有这一切都得益于互联网的开放性和匿名性特征。然而，正是这些特征也决定了互联网不可避免地存在着信息安全隐患。网络安全所包含的范围很广：我们日常上网时碰到的邮件病毒、QQ 密码被盗，大一点的如一个企业或政府的网站被黑，数据内容被篡改，更大的乃至一个国家的国防、军事信息泄露或被截获等。所有这些都属于网络安全所研究讨论的范畴。

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。随着信息业的发展，信息安全也应运而生，信息安全的概念在 20 世纪经历了一个漫长的历史阶段，90 年代以来得到了深化。进入 21 世纪，随着信息技术的不断发展，信息安全问题也日显突出。如何确保信息系统的安全已成为全社会关注的问题。国际上对于信息安全的研究起步较早，投入力度大，已取得了许多成果，并得以推广应用。中国已有一批专门从事信息安全基础研究、技术开发与技术服务工作的研究机构与高科技企业，构成了中国信息安全产业的主要支柱。

1.1 网络信息安全背景

信息安全与技术的关系可以追溯到远古。埃及人在石碑上镌刻了令人费解

的象形文字，斯巴达人使用一种称为密码棒的工具传达军事计划，罗马时代的凯撒大帝是使用加密函的古代将领之一，“凯撒密码”据传是古罗马凯撒大帝用来保护重要军情的加密系统，它是一种替代密码，通过将字母按顺序推后 3 位起到加密作用，如将字母 A 换作字母 D，将字母 B 换作字母 E。英国计算机科学之父阿兰·图灵在英国布莱切利庄园帮助破解了德国海军的 Enigma 密电码，改变了第二次世界大战的进程。美国 NIST 将信息安全控制分为三类：

（1）技术，包括产品和过程（如防火墙、防病毒、入侵检测、加密技术）。

（2）操作，主要包括加强机制和方法、纠正运行缺陷、各种威胁造成的运行缺陷、物理进入控制、备份能力、免于环境威胁的保护。

（3）管理，包括使用政策、员工培训、业务规划、基于信息安全的非技术领域。信息系统安全涉及政策法规、教育、管理标准、技术等方面，任何单一层次的安全措施都不能提供全方位的安全，安全问题应从系统工程的角度来考虑。

信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。但是，对于不同的部门和行业来说，其对信息安全的要求和重点却是有区别的。

1. 网络安全威胁的类型

网络威胁是对网络安全缺陷的潜在利用，这些缺陷可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏等。网络安全所面临的威胁可以来自很多方面，并且随着时间而变化。网络安全威胁的种类有：窃听、假冒、重放、流量分析、数据完整性破坏、拒绝服务、资源的非授权使用等。

2. 网络安全机制应具有的功能

采取措施对网络信息加以保护，以使受到攻击的威胁减到最小是必需的。一个网络安全系统应有如下的功能：身份识别、存取权限控制、数字签名、保护数据完整性、审计追踪、密钥管理等。

3. 网络信息安全常用技术

通常保障网络信息安全的方法有两大类：以防火墙（Firewall）技术为代表的被动防卫型和建立在数据加密、用户授权确认机制上的开放型网络安全保障技术。

1）防火墙技术

防火墙安全保障技术主要是为了保护与互联网相连的企业内部网络或单独节点。它具有简单实用的特点，并且透明度高，可以在不修改原有网络应用系统的情况下达到一定的安全要求。防火墙一方面通过检查、分析、过滤从内部网流出的 IP 包，尽可能地对外部网络屏蔽被保护网络或节点的信息、结构，另一方面对内屏蔽外部某些危险地址，实现对内部网络的保护。

实现防火墙的技术包括四大类：网络级防火墙（也叫包过滤防火墙）、应用级网关、电路级网关和规则检查防火墙。

（1）网络级防火墙

一般是基于源地址和目的地址、应用或协议以及每个 IP 包的端口来做出通过与否的判断。一个路由器便是一个“传统”的网络级防火墙，大多数的路由器都能通过检查这些信息来决定是否将所收到的包转发，但它不能判断出一个 IP 包来自何方，去向何处。

先进的网络级防火墙可以判断这一点，它可以提供内部信息以说明所通过的连接状态和一些数据流的内容，把判断的信息同规则表进行比较，在规则表

中定义了各种规则来表明是否同意或拒绝包的通过。网络级防火墙检查每一条规则直至发现包中的信息与某规则相符，如果没有一条规则能符合，防火墙就会使用默认规则，一般情况下，默认规则就是要求防火墙丢弃该包；其次，通过定义基于 TCP 或 UDP 数据包的端口号，防火墙能够判断是否允许建立特定的连接，如 Telnet、FTP 连接。

（2）应用级网关

应用级网关能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的注册和稽核。但每一种协议需要相应的代理软件，使用时工作量大，效率不如网络级防火墙。

应用级网关有较好的访问控制，是目前最安全的防火墙技术，但实现困难，而且有的应用级网关缺乏“透明度”。在实际使用中，用户在受信任的网络上通过防火墙访问 Internet 时，经常会发现存在延迟并且必须进行多次登录才能访问 Internet 或 Intranet。

（3）电路级网关

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，这样来决定该会话（Session）是否合法，电路级网关是在 OSI 模型中的会话层上来过滤数据包，这样比包过滤防火墙要高二层。

实际上电路级网关并非作为一个独立的产品存在，它与其他的应用级网关结合在一起，如 Trust Information Systems 公司的 Gauntlet Internet Firewall、DEC 公司的 Alta Vista Firewall 等产品。另外，电路级网关还提供一个重要的安全功能：代理服务器（Proxy Server）。代理服务器是个防火墙，在其上运行一个叫作“地址转移”的进程，将所有内部的 IP 地址映射到一个“安全”的 IP 地址，这个地址是由防火墙使用的。但是，作为电路级网关也存在着一些缺陷，因为该

网关是在会话层工作的，它无法检查应用层级的数据包。

（4）规则检查防火墙

该防火墙结合了包过滤防火墙、电路级网关和应用级网关的特点。它同包过滤防火墙一样，能够在OSI网络层上通过IP地址和端口号过滤进出的数据包。它也像电路级网关一样，能够检查SYN、ACK标记和序列数字是否逻辑有序。当然它也像应用级网关一样，可以在OSI应用层上检查数据包的内容，查看这些内容是否能符合受保护网络的安全规则。

2）数据加密与用户授权访问控制技术

与防火墙相比，数据加密与用户授权访问控制技术比较灵活，更加适用于开放的网络。用户授权访问控制主要用于对静态信息的保护，需要系统级别的支持，一般在操作系统中实现。

数据加密主要用于对动态信息的保护。对动态数据的攻击分为主动攻击和被动攻击。对于主动攻击，虽无法避免，但却可以有效地检测；而对于被动攻击，虽无法检测，但却可以避免，实现这一切的基础就是数据加密。数据加密实质上是对以符号为基础的数据进行移位和置换的变换算法，这种变换是受“密钥”控制的。在传统的加密算法中，加密密钥与解密密钥是相同的，或者可以由其中一个推知另一个，称为“对称密钥算法”。这样的密钥必须秘密保管，只能为授权用户所知，授权用户既可以用该密钥加密信息，也可以用该密钥解密信息。DES是对称加密算法中最具代表性的算法。如果加密/解密过程各有不相干的密钥，构成加密/解密的密钥对，则称这种加密算法为“非对称加密算法”或“公钥加密算法”，相应的加密/解密密钥分别称为“公钥”和“私钥”。在公钥加密算法中，公钥是公开的，任何人都可以用公钥加密信息，再将密文发送给私钥拥有者。私钥是保密的，用于解密其接收的公钥加密过的信息，典型的公钥加密算法如RSA是目前使用比较广泛的加密算法。

3）入侵检测技术

入侵检测技术是指“通过对行为、安全日志、审计数据、其他网络上可以获得的信息进行操作，检测到对系统的闯入或闯入的企图”。入侵检测是检测和响应计算机误用的学科，其作用包括威慑、检测、响应、损失情况评估、攻击预测和起诉支持。入侵检测系统（Intrusion Detection System，IDS）是可以对计算机和网络资源的恶意使用行为进行识别的系统，包括系统外部的入侵和内部用户的非授权行为，是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术，能够实现入侵检测的软件与硬件的组合便是入侵检测系统。

4）防病毒技术

随着计算机技术的不断发展，计算机病毒变得越来越复杂和高级，对计算机信息系统构成极大的威胁。在病毒防范中普遍使用的防病毒软件，从功能上可以分为网络防病毒软件和单机防病毒软件两大类。单机防病毒软件一般安装在单台 PC 上，即对本地和本地工作站连接的远程资源采用分析扫描的方式检测、清除病毒。网络防病毒软件则主要注重网络防病毒，一旦病毒入侵网络或者从网络向其他资源传染，网络防病毒软件会立刻检测到并加以删除。

在计算机网络系统中，绝对的安全是不存在的，制定健全的安全管理体制是计算机网络安全的重要保证，应通过网络管理人员与使用人员的共同努力，运用一切可以使用的工具和技术，尽一切可能去控制、减少一切非法的行为，尽可能地把不安全的因素降到最低。同时，要不断加强计算机信息网络的安全规范化管理力度，大力加强安全技术建设，强化使用人员和管理人员的安全防范意识。网络内使用的 IP 地址作为一种资源以前一直为某些管理人员所忽略，为了更好地进行安全管理工作，应该对本网内的 IP 地址资源统一管理、统一分配。对于盗用 IP 资源的用户必须依据管理制度严肃处理。只有共同努力，才能使计算机网络的安全可靠得到保障，从而使广大网络用户的利益得到保障。

随着网络的发展、技术的进步，网络安全面临的挑战也在增大。一方面，对网络的攻击方式层出不穷，攻击方式的增加意味着对网络威胁的增大。另一方面，网络应用范围的不断扩大，使人们对网络依赖的程度增大，对网络的破坏造成的损失和混乱会比以往任何时候都大。这对网络信息安全保护提出了更高的要求，也使网络信息安全学科的地位越发显得重要，网络信息安全必然随着网络应用的发展而不断发展。

1.2 入侵防御的必要性

1.2.1 典型的黑客攻击过程

现在，黑客攻击事件频发，对于网络安全管理人员来说，成功防御的基础就是要了解“敌人”，就像防御工事必须进行总体规划一样，网络安全管理人员必须了解黑客的工具和技术，并利用这些知识来设计应对各种攻击的网络防御框架。不管是信息篡改、大流量攻击还是信息窃取，黑客对目标系统实施攻击的流程大致相同，主要包含五个步骤：搜索、扫描、获得权限、保持连接、消除痕迹。

（1）搜索

搜索可能是耗费时间最长的阶段，有时可能会持续几个星期甚至几个月。黑客会利用各种渠道尽可能多地了解企业类型和工作模式，包括互联网搜索、社会工程、垃圾数据搜寻、域名管理/搜索服务、非侵入性的网络扫描等。

这些类型的活动由于处于搜索阶段，所以属于很难防范的。很多公司提供的信息都很容易在网络上找到，员工也往往会受到欺骗而无意中提供了相应的信息，随着时间的推移，公司的组织结构及潜在的漏洞就会被发现，整个黑客攻击的准备过程就逐渐完成了。不过，这里也提供了一些你可以选择的保护措施，可以让黑客攻击的准备工作变得更加困难，主要是确保系统勿将信息泄露

到网络上，包括软件版本和补丁级别、电子邮件地址、关键人员的姓名和职务，确保纸质信息得到妥善处理，接受域名注册查询时提供通用的联系信息，禁止对来自周边局域网/广域网设备的扫描企图进行回应。

（2）扫描

一旦攻击者对公司网络的具体情况有了足够的了解，就会开始对周边和内部网络设备进行扫描，以寻找潜在的漏洞，包括：开放的端口和应用服务、包括操作系统在内的应用漏洞、保护性较差的数据传输、每一台局域网/广域网设备的品牌和型号。

在扫描周边和内部设备的时候，网络入侵检测/防御系统可以发挥有效的报警/阻断作用，但某些资深的老牌黑客有可能绕过这些防护措施。为了更好地抵御黑客扫描，网络安全管理员应关闭所有不必要的端口和服务；对于关键设备或处理敏感信息的设备，只容许响应经过核准设备的请求；加强管理系统的控制，禁止直接访问外部服务器，在特殊情况下需要访问时，也应该在访问控制列表中进行端到端连接的控制；确保局域网/广域网系统及端点的补丁级别是足够安全的。

（3）获得权限

攻击者获得了连接的权限就意味着实际攻击已经开始。通常情况下，攻击者选择的目标是可以为攻击者提供有用信息，或者可以作为攻击其他目标的起点。在这两种情况下，攻击者都必须取得一台或多台网络设备某种类型的访问权限。

（4）保持连接

为了保证攻击的顺利完成，攻击者必须保持连接的时间足够长，虽然攻击者能够到达这一阶段意味着已经成功地规避了系统的安全控制措施，但对于入