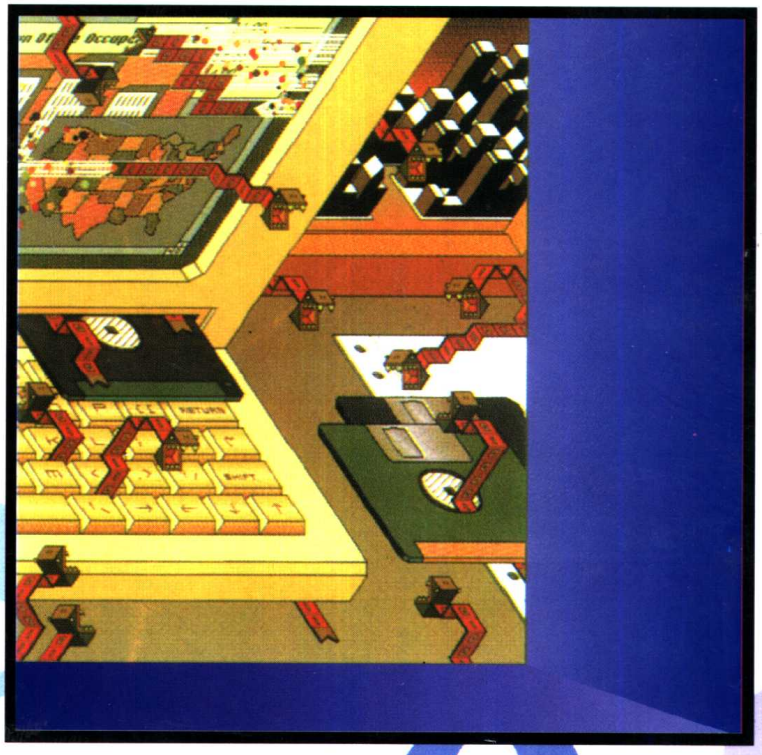
网络入侵检测原理与技术

蒋建春　冯登国　编著



国防工业出版社

蒋建春　冯登国　编著

网络入侵检测原理与技术

国防工业出版社

图书在版编目(CIP)数据

网络入侵检测原理与技术/蒋建春，冯登国编著.
—北京：国防工业出版社，2001.7
ISBN 7-118-02551-8

Ⅰ.网… Ⅱ.①蒋…②冯… Ⅲ.计算机网络
-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2001)第 027054 号

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号)
(邮政编码 100044)
三河市腾飞胶印厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 12¼ 274 千字
2001 年 7 月第 1 版 2001 年 7 月北京第 1 次印刷
印数：1—3000 册 定价：18.00 元

内 容 简 介

入侵检测是近年来网络安全研究的热点之一。本书首先说明了入侵检测的必要性，并给出了入侵检测的概念和模型，详述了多种入侵检测方法及体系结构。此外，对有关入侵检测系统的测试和标准化问题也作了阐述，同时讨论了该领域尚存在的问题及未来的研究方向。本书最后介绍入侵检测系统模型、设计和实现的具体工作。目的是让读者对入侵检测这一重要的信息安全研究领域有一个全面的了解。

本书适合于从事信息安全的教育、科研和工程技术人员参考，也适合于相关专业的高年级本科生和研究生作教科书使用。

前　言

随着社会信息化的普及，人们日常生活及工作环境逐步依赖于信息系统，信息作为一种无形的资源系统越来越得到人们的共识。随着数字化技术的发展，许多部门和单位都建立起基于网络的信息系统，但信息系统的脆弱性使其面临种种攻击、威胁安全的难题。信息安全拓宽了国家安全的概念，信息应当作为国家的重要战略资源。既然如此，信息的安全性就显得十分突出。计算机网络作为信息重要载体倍受研究者关注，1988 年著名的"Internet 蠕虫事件"和计算机系统 Y2K 问题足以让人们高度重视信息系统的安全。最近发生的黑客以网络瘫痪(拒绝服务攻击)为目标的攻击事件震惊了全美国，从受攻击的商业网站到各个网络公司，从联邦调查局到司法部，乃至白宫和国会，都受到了巨大的震撼。由于信息系统安全的独特性，人们已将其用于军事对抗领域，计算机病毒和网络黑客攻击技术将会用作军事武器。信息安全技术的发展将会改变以往竞争形式，包括战争。

在广泛应用的国际互联网上，黑客攻击事件时有发生。根据美国 GAO(General Accounting Office)在 1996 年 5 月 22 日披露，有将近 250000 次黑客尝试闯入联邦计算机系统的事件发生，估计这些攻击 64%是成功的。更坏的情况是，黑客攻击次数每年成倍增加。按照一些研究结果，GAO 预计只有 1%～4%的攻击被检测到，仅有 1%的攻击被报告。为此，美国高级研究计划局(DARPA)特别关注入侵检测技术的发明创新及应用研究，资助 20 多个项目，用于入侵检测系统(Intrusion Detection System，简称 IDS)测试评估的费用达 1000 万美元。计算机网络安全不再仅仅是一个学术问题，随着计算机网络的普及，它已经和我们的切身利益密切相关。网络入侵就在我们身边，昨天，你常去的网站被攻击而导致服务瘫痪；今天，你的邮件信箱被邮件炸弹炸掉，使 E-mail 丢失了；明天，黑客干脆侵入到你的 PC 里，取走了你放在硬盘里的电子情书，你的个人隐私就暴露了。入侵检测系统是一个程序，它始终驻留在被保护的主机上，不断监视系统的各种变化，发现入侵征兆，并及时向系统管理员或用户报警。

本书主要讨论了入侵检测技术，包括它的发展原因、发展现状和发展方向。目的是让读者对入侵检测这一重要的信息安全研究领域有一个全面的了解。本书适合于从事信息安全的教育、科研和工程技术人员参考，也适合于相关专业的高年级本科生和研究生作教科书使用。

目　录

第1章 绪 论

1.1 网络安全的目标

计算机网络的最简单的定义是一些互相连接的、自治的计算机的集合。计算机网络主要由三部分组成：

（1）若干主机；

（2）通信子网，包括通信处理机和连接各网络中节点的通信链路；

（3）系列协议，如以太网协议、TCP/IP 协议等。

从计算机网络的定义和组成来看，计算机网络安全将涉及到计算机、通信链路和协议的安全问题。因此，网络安全研究必将围绕这些问题来展开,特别是协议的安全问题是计算机网络安全中最困难的问题。

Sun 公司提出，“网络就是计算机”。从网络组成来分析，网络的安全问题与计算机系统安全问题紧密相关，但不完全等同。这里，先让我们简单地概括计算机系统的安全问题。Garfinkel 和 Spaf-ford 给出了安全计算机系统的全面的定义。安全计算机系统取决于所期望的系统行为,这种所期望的系统行为与计算机安全定义是一样的。可信级别表明计算机系统所期望的行为可信度,这些所期望的行为被作为计算机系统安全策略以及系统管理要达到的目标。这些策略可能包括功能性要求，而这些要求对计算机系统功能的有效性是必要的。[RS91]给出的计算机安全比较狭窄，安全的定义是基于计算机机密性、完整性和可用性的实现。

① 机密性要求只有授权才能访问信息；

② 完整性要求信息保持不被意外或者恶意地改变；

③ 可用性指的是计算机系统在不降低使用的情况下仍能根据授权用户的需要提供资源服务。

按照可用性这样的定义，如果可用性作为安全要求的一部分，那么不可靠的计算机系统是不安全的。 一个安全的计算机系统保护它的数据和资源免于非授权访问、篡改和拒绝使用。数据的机密性对公司的生存或者商业成功是重要的，数据的完整性对医院保存病人的病历是重要的，数据的可用性对实时业务控制是必须的。计算机系统功能正确性与其安全性的关系是紧密的。功能的正确性意味着计算机系统符合要求。如果功能需求包括安全的要求，那么功能的正确性意味着计算机系统的安全。但是，反过来是不正确的，功能的错误可能导致安全策略的冲突，尤其是与机密性、完整性和可用性相关的安全策略方面。例如：操作系统服务调用不可能处理所有的有效参数，按照这样的事

实，安全策略冲突不可能。另外的例子是，考虑到可视化的字处理程序(WYSIWYG)，当用户选择显示为高亮度时程序就失效。这个程序的功能很可能不正确，可是这样做不可能引起系统安全策略冲突。

随着网络技术的发展和应用范围的扩大，我们越来越依赖于网络进行迅速地访问和处理信息。这样的需求逐渐增加，而且大量的信息被保存在计算机中。计算机使用范围的日益增长使得不同来源的数据能快速地被搜集整理。特别是最近几年，计算机联网技术得到迅速地发展，Internet 网的发展大大地改变了以往以单机为主的计算模式。一方面，网络提供了资源的共享性，提高了系统的可靠性，通过分散工作负荷提高了工作效率，并且还具有可扩充性。网络的这些特点使得计算机网络深入科研、文化、经济、国防及日常生活等各个领域。另一方面，正是这些特点，增加了网络安全的脆弱性。资源的共享和分布增加了网络受攻击的可能性。1988 年 11 月，Robert T. Morris 设计 Internet 蠕虫程序攻击了数千台主机。蠕虫程序主要采用了三种攻击方法：一是弱点攻击，利用 Sendmail 和 finger 程序的漏洞进行；二是协议攻击，主机信任关系；三是破解口令。这三种攻击方法开辟了网络攻击先例，直到现在为止仍然为攻击者所用，同时也成为安全研究人员所研究的课题之一。从那时起，不断传出侵犯安全的事件报道。企图闯入系统者有之，成功闯入系统者有之，抓住 Internet 上主机的其它种种弱点和漏洞加以利用者也有之。有关网络入侵事件近年来时有发生。图 1.1 给出了网络攻击示意图。

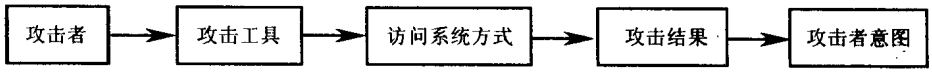


图 1.1　计算机网络攻击示意图

图 1.1 从攻击者、攻击工具、访问系统方式、攻击结果、攻击者意图角度刻划了网络攻击整体过程，下面将详细阐述这几个方面。

（1）攻击来源　对计算机和网络攻击来讲，攻击者是明显的创造者。可以根据他们的来源识别，例如某个城市的高中生、公司以前的雇员或国外。也可以根据他们的能力识别，例如小偷、初级技术爱好者、高级技术爱好者、专业高级黑客。攻击者初步地可分成黑客、间谍、恐怖主义者、公司雇佣者、职业犯罪、破坏者六种类型。

（2）攻击工具　攻击者为了实现其目的，会使用各种各样的工具，通过工具相互配合完成，常见的工具有操作系统命令、脚本程序、工具包、数据窃取等。例如，计算机病毒、特洛伊木马、蠕虫、隐蔽通道和嗅探程序。

（3）访问系统方式　攻击者以非授权方式访问系统或使用资源。由于软件或硬件设计、实现、配置错误导致系统中存在弱点，攻击者就利用这些漏洞，对系统数据进行非法访问。例如，几乎所有的操作系统，包括 UNIX、Windows NT、Windows 98 都存在漏洞。

（4）攻击结果　攻击的结果有拒绝服务、信息泄漏、服务盗用、信息破坏四个方面，例如最早的拒绝服务攻击是“电子邮件炸弹”，它能使用户在很短时间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。

（5）攻击者意图　攻击者意图分为挑战和获取访问权限、政治情报信息、政治目

的而制造恐怖、竞争经济利益、个人的经济利益和实现破坏。

从防卫者的角度来看，针对上述内容，可以得到网络安全的目标为以下几个方面。

（1）网络服务的可用性（Availability） 无论何时，网络服务必须是可用的，如抗击拒绝服务攻击。

（2）网络信息的保密性（Confidentiality） 网络服务要求能防止敏感服务信息泄露，要求只有在授权的条件下，才能获取服务信息。

（3）网络信息的完整性（Integrity） 网络服务必须保证服务者提供的信息内容不能被非授权篡改，不管是有意或故意，完整性是对信息的准确性和可靠性的评价指标。

（4）网络信息的非否认（抗抵赖）性（No-repudiation） 用户不能否认消息或文件来源地，也不能否认接收了信息或文件。

（5）网络运行的可控性（Controlability） 是指网络管理的可控性，包括网络运行的物理的可控性和逻辑或配置的可控性等，能够有效地控制网络用户的行为及信息的传播范围。

1.2 传统的网络安全模型

设计安全措施来防范未经授权访问系统的资源和数据，这是当前网络安全领域一个十分重要而迫切的问题。就目前来说，要想完全避免安全事件的发生并不太现实。网络安全人员所能做的只能是尽力发现和察觉入侵及入侵企图，以便采取有效的措施来堵塞漏洞和修复系统。 提到传统的网络安全模型，我们首先看看单机系统的安全控制模型，如图 1.2 所示。

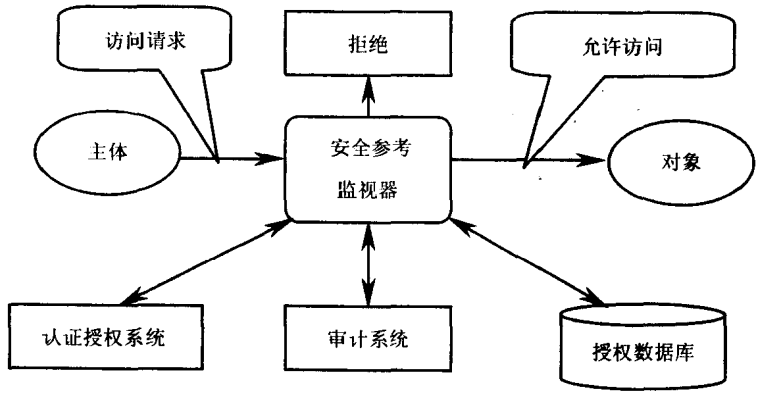


图 1.2 单机安全模型

由于计算机联网，单机系统的安全问题不仅涉及到本身，而且会危及到其它的单机系统，与此同时，单机系统所受到的威胁增多，如远程攻击和主机信任欺骗攻击等。因而基于单机系统的安全控制已不足以保证网络的安全。J. Bryan Lyles 和 Christoph

L.Schuba 给出了一个网络安全控制模型，如图 1.3 所示。

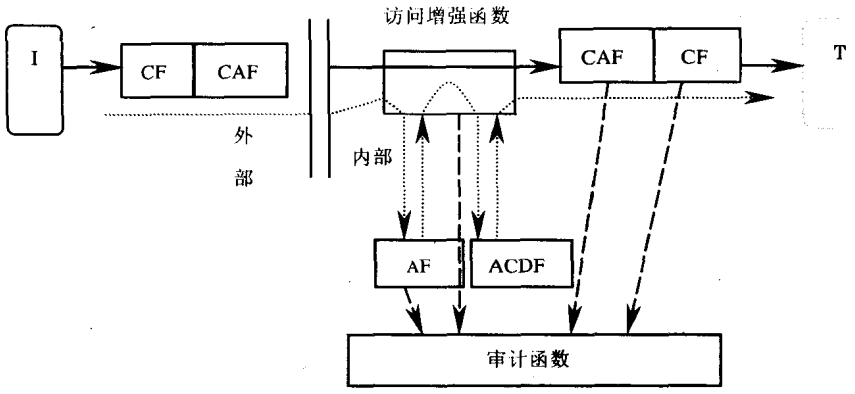


图 1.3　网络安全控制模型

I-Initiator；T—Target；CF—Confidentiality Function；CAF—Connection Authentication Function；

AF-Authentication Function；ACDF—Admission Control Decision Function。

——数据流（Data Traffic）；……→ —信号流（Signaling Traffic）；

- - - -→ —审计流(Audit data flow)。

图 1.3 通过使用 CF、CAF、AF、ACDF 安全函数从高层次角度抽象地刻划了网络安全通用模型，并将端点认证、连接授权、数据完整性、数据保密性、管理控制和审计结合起来。值得一提的是，网络安全控制模型融进其它的安全模型，如保密性模型和完整性模型等。在网络安全实际应用当中，大多数的安全防范机制是基于这个模型，如防火墙。

1.3　传统网络安全技术

传统网络安全技术主要使用以下几种安全机制。

1. 加密机制

加密是一种最基本的安全机制,它能防止信息被非法读取。加密是一种在网络环境中对抗被动攻击的行之有效的安全机制。数据加密是保护数据的最基本的方法。但是，这种方法只能防止第三者获取真实数据，仅解决了安全问题的一个方面。而且，加密机制并不是牢不可破。

2. 数据签名机制

签名与加密很相似，一般是签名者利用秘密密钥(私钥)对需签名的数据进行加密,验证方利用签名者的公开密钥(公钥)对签名数据做解密运算。如图 3 所示，签名可以实施在一个完整的数据包上,也可以实施在某条消息(或某块数据)的校验和上,这可以根据不同的应用需求来确定。如果能保证一个签名者的签名只能唯一地从他自己产生,那么当收发双方发生争议的时候(如接收方收到了某条消息，而发送方却否认曾经发出过这条

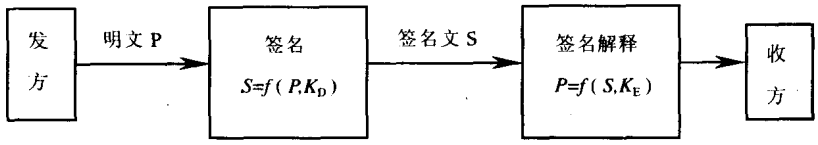


图 1.4　数据签名原理图

注：密钥 K_E,K_D 由发方编制，K_E 可公开，K_D 必须由发方保管。

消息)，仲裁机构就能够根据消息上的数字签名来裁定这条消息是否确实是由发送方发出的。

3. 访问控制机制

访问控制机制是按照事先确定的规则决定主体对客体的访问是否合法。当一个主体试图非法使用一个未经授权使用的客体(资源)时，访问控制功能将拒绝这一企图，并可附带报告这一事件给审计跟踪系统，审计跟踪系统产生一个报警或形成部分追踪审计。访问控制一般以下述机制为基础：

（1）访问控制数据库；

（2）口令；

（3）安全标记,当它与实体(程序、数据等)有关时，可用来允许或拒绝与安全有关的访问；

（4）能力表,决定主体对客体访问的权利的凭证。

4. 数据完整性机制

数据完整性技术可以发现网络上传输的数据已经被非法修改,从而使用户不会被非法数据所欺骗。

5. 认证机制

认证是以交换信息的方式来确认实体身份的机制，是进行存取控制所必不可少的条件，因为不知道用户是谁，就无法判断其存取是否合法。用于认证的技术如下。

（1）口令机制　口令一般由发方实体提供，由收方实体检测；

（2）安全协议机制　收发双方事先经过约定,按照约定的协议进行鉴别交换；

（3）使用密码技术　将交换的数据加密，只有合法用户才能解密，得出有意义的明文；

（4）使用实体的特征或实体所有的物件　这时常采用的技术是指纹识别和身份卡等。

6. 系统脆弱性检测

系统中脆弱性的存在是系统受到各种安全威胁的根源。外部黑客的攻击主要利用了系统提供的网络服务中的脆弱性；内部人员作案则利用了系统内部服务及其配置上的脆弱性；而拒绝服务攻击主要是利用资源分配上的脆弱性，长期占用有限资源不释放，使其它用户得不到应得的服务，或者是利用服务处理中的弱点，使该服务崩溃。保护系统的安全，在于消除系统中存在的各种脆弱性，而消除脆弱性的第一步应该是检测出系统内是否存在各种脆弱性，在此基础上才能进一步去考虑脆弱性的修补与消

除。

7. 构筑防火墙系统

防火墙系统软件实现将定义好安全策略转换成具体的安全控制操作，它使得内部网络与因特网之间或者与其它外部网络互相隔离、限制网络互访。按照一定的安全策略规则对其检查网络包或服务请求，来决定网络之间的通信是否被允许，其中被保护的网络称为内部网络或私有网络，而与内部网络或私有网络相连的网称为外部网络或公用网络。防火墙能有效地控制内部网络与外部网络之间的访问及数据传送，从而实现保护内部网络的信息不受外部非授权用户的访问或者过滤信息的目的。防火墙的实现从层次上大概可以分两种：报文过滤和应用层网关。报文过滤是在 IP 层实现的，因此，它可以只用路由器完成。报文过滤根据报文的源 IP 地址、目的 IP 地址、源端口、目的端口及报文传递方向等报头信息来判断报文是否被允许通过。现在也出现了一种可以分析报文数据区内容的智能型报文过滤器。报文过滤器的应用非常广泛，因为 CPU 用来处理报文过滤的时间可以忽略不计。而且这种防护措施对用户透明，合法用户在进出网络时，根本感觉不到它的存在，使用起来很方便。但是在首次安装时，需要定义一个完备的过滤规则集，这是一项很麻烦的工作。管理员必须详细了解 Internet 的各种服务、报文格式和各个域的特定值。报文过滤的另一个也是很关键的弱点是不能在用户级别上进行过滤，即不能识别不同的用户和防止 IP 地址的盗用。如果攻击者把自己主机的 IP 地址设成一个合法主机的 IP 地址，就可以很轻易地通过报文过滤器。报文过滤的弱点可以用应用层网关解决。在应用层实现防火墙，方式多种多样。下面分别介绍几种应用层防火墙的实现原理。

（1）应用网关代理（Application Gateway Proxy） 这种防火墙技术是在网络应用层提供授权检查及代理服务。当外部某台主机试图访问（如 Telnet）受保护网时，它必须先在防火墙上经过身份认证。通过身份认证后，防火墙运行一个专门为 Telnet 设计的程序，把外部主机与内部主机连接。在这个过程中，防火墙可以限制用户访问的主机、访问时间及访问的方式。同样，受保护网络内部用户访问外部网时也需先登录到防火墙上，通过验证后，才可使用 Telnet 或 FTP 等有效命令。应用网关代理的优点是可以隐藏内部 IP 地址，也可以给单个用户授权，即使攻击者盗用了一个合法的 IP 地址，也通不过严格的身份认证。因此应用网关比报文过滤具有更高的安全性。但是这种认证使得应用网关不透明，用户每次连接都要受到“盘问”，这给用户带来许多不便。而且这种代理技术需要为每个应用写专门的程序。

（2）代理服务器 (Proxy Server) 顾名思义，代理服务器技术是把不安全的服务如 FTP、Telnet 等放到防火墙上，使它同时充当服务器，对外部的请求作出回答。与前一种实现相比，代理服务器技术不必为每种服务专门写程序。而且，受保护网内部用户想对外部网访问时，也需先登录到防火墙上，再向外提出请求，这样从外网向内就只能看到防火墙，从而隐藏了内部地址，提高了安全性。

（3）IP 隧道 (IP Tunnel) 或 VPN 技术 经常会出现这种情况，一个大公司的两个子公司相隔较远，通过 Internet 通信。这种情况下，可以采用 IP Tunnels 来防止 Internet 上的黑客获取信息，从而在 Internet 上形成一个虚拟的专网，如图 1.5 所示。

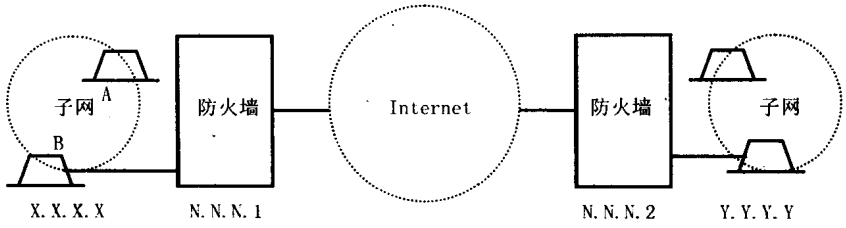


图 1.5　VPN 工作原理示意图

IP Tunnels 的工作原理是这样的，子网 A 中一主机（IP 地址为 X.X.X.X）欲向子网 B 中某主机（IP 地址为 Y.Y.Y.Y）发送包，该包经过本网防火墙 FW1（IP 地址 N.N.N.1）时，防火墙判断该包是否发往子网 B，若是，则再增加一包头，变成从此防火墙到子网 B 防火墙 FW2（N.N.N.2）的 IP 包，而将原 IP 地址封装在数据区内，同原数据一起加密后经 Internet 发往 FW2。FW2 接收到包后，若发现源 IP 地址是 FW1 的，则去掉附加包，解密，在本网上传送。从 Internet 上看，就只是两个防火墙的通信。即使黑客伪装了从 FW1 发往 FW2 的包，由于 FW2 在去掉包头后不能解密，会抛弃包。包的转发过程如图 1.6 所示。

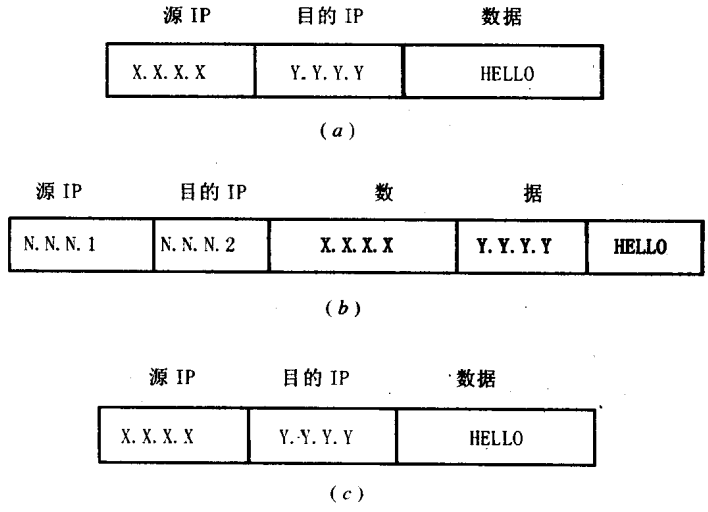


图 1.6　包的转发过程

（a）从主机 X 发出；（b）从防火墙 FW1 发往 Internet；（c）从防火墙 FW2 发往主机 Y。

（4）套接字服务服务器（Sockets Server）　套(Sockets)是一个网络应用层的国际标准。当受保护网络客户机需要与外部网交互信息时，在防火墙上的套服务器检查客户的 User ID、IP 源地址和 IP 目的地址，经过确认后，套服务器才与外部的服务器建立连接。对用户来说，受保护网与外部网的信息交换是透明的，感觉不到防火墙的存在，那是因为网络用户不需要登录到防火墙上。但是客户端的应用软件必须支持“Socketsified

API"，受保护网络用户访问公共网所使用的 IP 地址也都是防火墙的 IP 地址。

（5）网络地址转换器（Network Address Translater)

当受保护网连到 Internet 上时，受保护网用户若要访问 Internet，必须使用一个合法的 IP 地址。但由于合法 Internet IP 地址有限，而且受保护网络往往有自己的一套 IP 地址规划（非正式 IP 地址)。网络地址转换器就是在防火墙上装一个合法 IP 地址集，当内部某一用户要访问 Internet 时，防火墙动态地从地址集中选一个未分配的地址分配给该用户，该用户即可使用这个合法地址进行通信。同时，对于内部的某些服务器如 Web 服务器，网络地址转换器允许为其分配一个固定的合法地址。外部网络的用户就可通过防火墙来访问内部的服务器。这种技术既缓解了少量的 IP 地址和大量的主机之间的矛盾，又对外隐藏了内部主机的 IP 地址，提高了安全性。

（6）隔离域名服务器（Split Domain Name Server ） 这种技术是通过防火墙将受保护网络的域名服务器与外部网的域名服务器隔离，使外部网的域名服务器只能看到防火墙的 IP 地址，无法了解受保护网络的具体情况，这样可以保证受保护网络的 IP 地址不被外部网络获悉。

（7）邮件转发（Mail Forwarding） 当防火墙采用上面所提到的几种技术使得外部网络只知道防火墙的 IP 地址和域名时，从外部网络发来的邮件，就只能送到防火墙上。这时防火墙对邮件进行检查，只有当发送邮件的源主机是被允许通过的，防火墙才对邮件的目的地址进行转换，送到内部的邮件服务器，由其进行转发。

现在，建立防火墙系统是解决网络安全问题的主要方法，基于防火墙的网络安全结构主要有下面三种基本结构。

（1）双宿主主机结构 双宿主主机结构是最基本的防火墙系统结构。这种系统实质上就是至少具有两个网络接口卡的主机系统。这样的主机还可充当与这些网络接口卡相连的若干网络中间的路由器。

在这种结构中，一般都是将一个内部网络和外部网络分别连接在不同的网卡上，取消系统固有的将IP包从一个网卡无安全控制地转发到另一个网卡上的功能，使得内外网络不能直接通信。对从一块网卡上送来的IP包，经过一个安全检查模块检查后，如果是合法的，转发到另一块网卡上，以实现网络的正常通信；如果不合法，则阻止通信。这样，内外网络直接的IP数据流完全在双宿主主机的控制之中。

基于双宿主主机的防火墙的结构非常简单，双宿主主机位于内外网络中间并分别与内外网络相连，如图 1.7 所示。

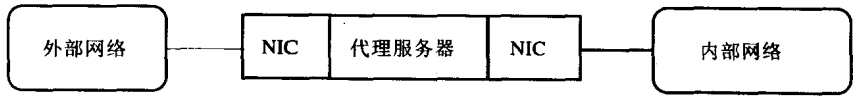


图 1.7 双宿主主机结构

双宿主主机可以提供很高程度的网络控制。它从物理上将内部和外部网络隔开。它是一个作为网络安全控制的基本框架，一般的以防火墙控制网络安全的结构都是用这样的结构放在网络边缘来控制进出信息的。但由于进出网络都必须通过该主机，而且要通过检查，所以，该主机的负载一般较大，容易成为网络瓶颈。

对于只进行IP层过滤的安全要求来说，只需要在两块网卡之间转发的模块上插入对IP包的ACL控制即可。通的常情况是，对于内外两块网卡的配置不同，要明确内外两块网卡的标识。

对于要进行应用层代理控制的安全结构，其代理就要设置到这台双宿主主机上，所有的应用要先与这个主机进行连接再连接到内部网络。这样，每一个连接必须在该主机上有一个登陆帐号，这样就增大了其危险性。所以一般应避免这种结构。

（2）主机过滤结构　双宿主主机结构是由一台同时连接内外网络的主机提供安全保障的，而主机过滤结构则不同，在主机过滤的结构中，提供安全保护的主机是与内部网络相连的，另外，主机过滤还需要一台路由器，如图 1.8 所示。这种结构中的堡垒主机位于内部网络，一般情况，过滤路由器可按如下规则进行配置。

图 1.8　主机过滤结构

①允许其它内部主机（非堡垒主机）为某些类型的服务请求与外部网络建立直接连接。

②任何外部网（或Internet）的主机只能与内部网络的堡垒主机建立连接。

③任何外部系统对内部网络的操作都必须经过堡垒主机。同时，堡垒主机本身要求要有较全面的安全维护。

由于这种结构允许包从外部网络直接传送到内部网（堡垒主机），所以这种结构的安全控制看起来似乎比双宿主主机结构差。在双宿主主机结构中，外部网络的包理论上不可能直接抵达内部网，但实际上，利用双宿主主机结构在防护数据包从外部网络进入内部网络也很容易失败，并且这种失败是随机的，所以无法有效地预先防范。一般来说，主机过滤结构比双宿主主机结构能够提供更好的安全保护，同时也更具有易操作性。

当然，与其它结构相比，主机过滤结构也有一些缺点。其主要缺点就是只要入侵者设法攻破了堡垒主机，那么对于入侵者来说，整个内部网络与堡垒主机之间就没有任何障碍了，它就变成了内部合法的用户，完全可以侦听到内部网络上的所有信息。

（3）子网过滤结构　如图 1.9 所示，子网过滤结构就是在主机过滤结构中增加一层周边网络的安全机制，使得内部网络和外部网络有两层隔离带，周边网络来隔离堡垒主机与内部网，就是为了减轻在入侵者冲开堡垒主机的时候对内部网络的冲击力。入侵者即使冲开了堡垒主机，也不能侦听到内部网络的信息，不能对内部网络直接操作。

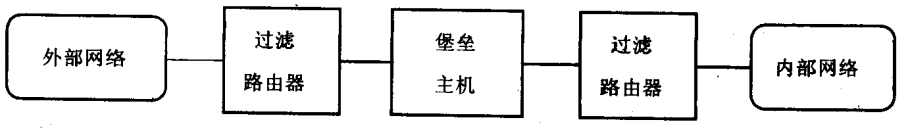


图 1.9　子网过滤结构