第 5 章　防火墙与入侵检测技术

本章学习目标

当前，很多企业已经将自己的内部网络和 Internet 连接，这样不仅可以便利地同商业伙伴开展业务，还可以充分利用 Internet 中广阔的资源。但是在获取资源的同时也带来了一些安全隐患，防火墙和入侵检测技术应运而生。

通过对本章的学习，应掌握以下内容：

(1) 网络安全的目的、意义及相关技术。

(2) 防火墙的基本概念和种类。

(3) 防火墙的体系结构及功能。

(4) 入侵检测技术的种类及各类技术的相关性能。

防火墙技术是应用广泛的网络安全技术，它通过监测、限制和更改跨越防火墙的数据流等多种技术，尽可能地对外部网络屏蔽有关受保护网络的结构信息。防火墙可以隔离风险区域和安全区域的连接，同时不会妨碍对风险区域的访问，还可以监控进出网络的通信量，预防不希望的、未授权的信息进出被保护的网络，筑起网络的第一道安全防线。

作为网络安全技术的重要一员，入侵检测技术已成为当今一种非常重要的动态安全技术，它与传统的静态安全技术相结合，达到了比较理想的安全目的。入侵检测技术的重点在于如何有效地提取攻击特征数据并准确地分析出不正常的入侵行为。

5.1　防火墙技术

5.1.1　防火墙的概念

防火墙是指隔离在本地网络与外界网络之间的一个执行访问控制策略的防御系统，是这一类防范措施的总称。在 Internet 上防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域与安全区域(局域网)的连接，同时不会妨碍用户对风险区域的访问。防火墙放在受保护网络与外部网络之间，如图 5-1 所示。

防火墙实质上是一种隔离控制技术，其核心思想是在不安全的网络环境下构造一种相对安全的内部网络环境。从逻辑上讲它既是分析器又是限制器，它要求所有进出网络的数据流都必须遵循安全策略，同时将内外网络在逻辑上分离。

防火墙能增强机构内部网络的安全性。防火墙系统决定了哪些内部服务可以被外界访问，外界的哪些人员可以访问内部的服务，哪些外部服务可以被内部人员访问。防火墙必须只允许授权的数据通过，而且防火墙本身也必须能够免于渗透。

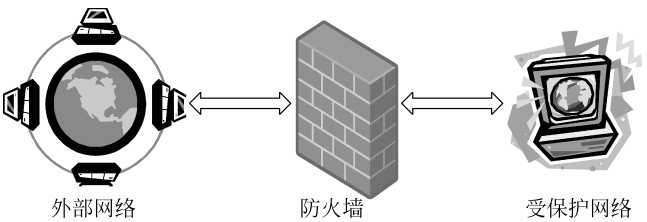

图 5-1 防火墙示意图

5.1.2 防火墙的种类

防火墙有许多种形式，有以软件形式运行在普通计算机之上的，也有以固件形式设计在路由器之中的。总的来说可以分为 3 种：包过滤防火墙，应用级网关防火墙，状态监测型防火墙。

1. 包过滤防火墙

在互联的 TCP/IP 网络上，所有往来的信息都被分割成许许多多一定长度的数据包，每一个数据包中都会包含一些特定信息，例如数据的源地址、目标地址、TCP/UDP 源端口和目标端口等。当这些数据包被送上互联网络时，路由器会读取接收者的 IP 并选择一条合适的物理线路发送出去，数据包可能经由不同的路线抵达目的地，当所有的包抵达目的地后会重新组装还原。包过滤型防火墙会检查所有通过的数据包中的 IP 地址，并按照系统管理员所给定的过滤规则进行过滤，一旦发现来自危险站点的数据包，防火墙便会将这些数据拒之门外。

包过滤技术的优点是它对于用户来说是透明的，处理速度快而且易于维护，实现成本较低，在应用环境比较简单的情况下，能够以较小的代价在一定程度上保证系统的安全。

但包过滤技术的缺陷也是很明显的。包过滤技术是一种完全基于网络层的安全技术，只能根据数据包的来源、目标和端口等网络信息进行判断，无法识别基于应用层的恶意入侵，例如恶意的 Java 小程序以及电子邮件中附带的病毒等。有经验的黑客也很容易伪造 IP 地址，骗过包过滤型防火墙。

2. 应用级网关防火墙

应用级网关指的是通常所说的代理服务器。它适用于特定的 Internet 服务，例如超文本传输(HTTP)、远程文件传输(FTP)等。代理服务器通常运行在两个网络之间，阻挡了二者间的数据交流，它对于客户机来说像是一台真的服务器，而对于外界的服务器来说，它又是一台客户机。当客户机需要使用服务器上的数据时，首先将数据请求代理服务器，代理服务器再根据这一请求向服务器索取数据，当代理服务器接收到对某站点的访问请求后会检查该请求是否符合规定，如果规则允许用户访问该站点，代理服务器会像一个客户一样去那个站点取回所需信息再转发给客户。

代理服务器通常都拥有一个高速缓存，这个缓存存储着用户经常访问的站点，在下一个用户要访问同一站点时，服务器就不需要重复地获取相同的内容，直接将缓冲内容发出即可，既节约了时间也节约了网络资源。代理服务器像一堵墙一样挡在内部用户和外界之间，从外部只能看到该代理服务器而无法获知任何的内部资源(例如用户 IP 地址等)，外部的恶

意侵害也就很难伤害到企业内部网络系统。应用级网关比单包过滤更为可靠，而且会详细地记录所有的访问状态信息。

但是应用级网关也存在一些不足：它对系统的整体性能有较大影响，使访问速度变慢，因为它不允许用户直接访问网络，而且应用级网关需要对客户机可能产生的每一个特定的 Internet 服务安装相应的代理服务软件，从而大大增加了系统的复杂度；用户不能使用未被代理服务器支持的服务，对每一类服务要使用特殊的客户端软件，但并不是所有的 Internet 应用软件都可以使用代理服务器。

3. 状态监测型防火墙

状态监测型防火墙是新一代的产品，这一技术实际已经超越了最初的防火墙定义。状态监测型防火墙能够对各层的数据进行主动的、实时的监测，在对这些数据加以分析的基础上有效地判断出各层中的非法侵入。这种防火墙具有非常好的安全性，它使用了一个在网关上执行网络安全策略的软件模块，称为检测引擎。检测在不影响网络正常运行的前提下，采用抽取有关数据的方法对网络通信的各层实时监测，抽取状态信息，并动态地保存起来作为以后执行安全策略的参考。检测引擎支持多种协议和应用程序，并可以很容易地实现应用和服务的扩充，同时这种监测型防火墙产品一般还带有分布式探测器，这些探测器安置在各种应用服务器和其他网络的节中，不仅能够检测来自网络外部的攻击，同时对于来自内部网络的恶意破坏也有极强的防御。

与前两种防火墙不同，当用户访问请求到达网关的操作系统前，状态监视器要抽取有关数据进行分析，结合网络配置和安全规定做出接纳、拒绝、身份认证、报警或给该通信加密等处理动作。一旦某个访问违反安全规定，就会拒绝该访问，并报告有关状态作日志记录。状态监测型防火墙的另一个优点是它会检测无连接状态的远程过程调用(RPC)和用户数据报(UDP)之类的端口信息，而包过滤和应用级网关防火墙都不支持此类应用。

这种防火墙无疑是非常坚固的，但它会降低网络的速度，而且配置也比较复杂。好在有关防火墙厂商已注意到这一问题，例如 Checkpoint 公司的防火墙产品 Firewall-1，它所有的安全策略规则都是通过面向对象的图形用户界面(GUI)来定义以简化配置过程。

5.1.3　防火墙的体系结构

1. 屏蔽路由器

屏蔽路由器是一个具有数据包过滤功能的路由器，既可以是一个硬件设备，也可以是一台主机。路由器上安装有 IP 层的包过滤软件，可以进行简单的数据包过滤。因为路由器是受保护网络和外部网络连接的必然通道，所以屏蔽路由器的使用范围很广。但其缺点也非常明显，一旦屏蔽路由器的包过滤功能失效，则受保护网络和外部网络就可以进行任何数据通信了。

2. 双宿主机网关

如果一台主机装有两块网卡，一块连接受保护网络，一块连接外部网络，那么这台堡垒主机就是双宿主机(双重宿主主机)网关，如图 5-2 所示。双宿主机体系结构围绕保垒主机构筑。保垒主机至少有两个网络接口，可以充当与这些接口相连的网络之间的路由器。外部网络能与保垒主机通信，内部网络也能与保垒主机通信，但是外部网络与内部网络不能直

接通信，IP 数据包并不是从一个网络（例如外部网络）直接发送到另一个网络（例如内部网络），保垒主机的防火墙体系结构禁止这种发送。它们之间的通信必须经过保垒主机的过滤和控制。

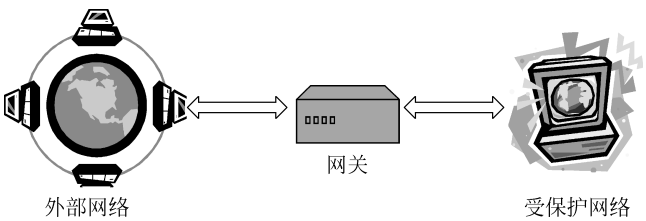

图 5-2 双宿主机网关示意图

堡垒主机装有相应的路由软件，可以很容易地实现网关的功能，并且可以有详尽的日志，也可以安装相应的系统管理软件，便于系统管理员使用。双宿主机网关优于屏蔽路由器的地方是：堡垒主机的系统软件可用于维护系统日志、硬件复制日志或远程日志。这一点对于日后的检查很有用，但不能帮助网络管理者确认内网中哪些主机可能被黑客入侵。双宿主机网关的一个致命弱点是：一旦入侵者侵入堡垒主机并使其只具有路由功能，则任何网络上的用户均可以随便访问内部网络。

3. 被屏蔽主机网关

这种结构由一台屏蔽路由器和一台堡垒主机组成，如图 5-3 所示。

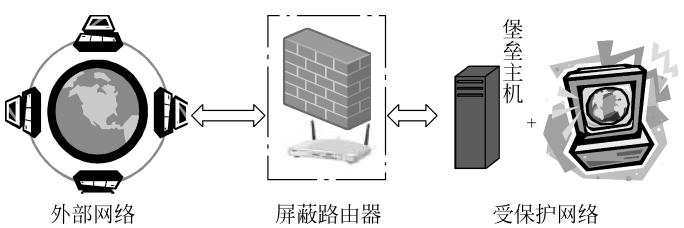

图 5-3 被屏蔽主机网关示意图

堡垒主机在受保护网络中，可以与受保护网络的主机进行通信，也可以和外部网络的主机建立连接。屏蔽路由器的作用是允许堡垒主机和外部网络之间的通信，同时所有受保护网络的其他主机和外部网络直接通信。堡垒主机成为从外部网络唯一可到达的主机，此时它就起到了网关的作用。内部网络的安全由屏蔽路由器和堡垒主机同时保证，如果屏蔽路由器被攻破，则内部网络就直接暴露了。

4. 被屏蔽子网

由两台屏蔽路由器将受保护网络和外部网络隔离开，中间形成一个隔离区（DMZ），就构成了被屏蔽子网结构，如图 5-4 所示。

隔离区可以被外部网络访问，这一点是由靠近外部网络的屏蔽路由器控制的。企业的 IIS 服务器、FTP 服务器放在隔离区中。外部网络是不能够直接访问内部网络的，这一点由靠近内部网络的屏蔽路由器控制。为了让受保护网络的主机可以和外部网络的主机通信，一般采用的方法是在隔离区内增加一台堡垒主机，这台堡垒主机可以被内部网络的主机访

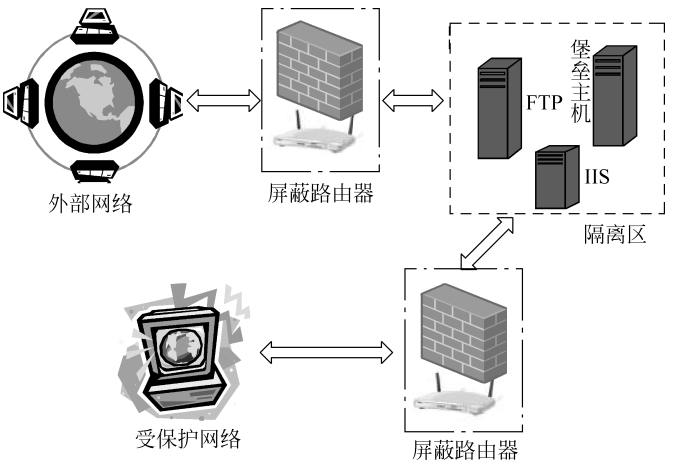

图 5-4　被屏蔽子网结构

问，也可以访问外部网络，此时这台堡垒主机起到了网关的作用，这一点和被屏蔽主机网关的情形类似。这种体系结构比较复杂，但是安全性得到了提升，它将受保护网络的主机和提供服务的服务器隔离起来，使外部网络无法直接到达内部，从而增加了入侵受保护网的难度。

5.1.4　防火墙的功能

随着防火墙技术的不断进步，防火墙的功能也在不断增加，下面介绍几种常见的功能。

1. 包过滤

包过滤功能是防火墙的基本功能，它通过允许或禁止数据包通过防火墙来保证信息安全。对于 5.1.2 节中提出的 3 种类型的防火墙，从本质上来说都是进行了数据包过滤，它们的区别仅仅在于进行包过滤的方法或者位置不同而已。

2. 审计和报警

防火墙具有审计功能是很重要的，安全管理员可能经常要对通过防火墙的信息进行分析，而审计功能的存在就是分析的基础。一般的防火墙会把日志保存到自身或者独立的主机上，后者可以采用更加复杂的分析手段。另外，防火墙也应该具有一定的报警功能，当发现紧急情况时，应该可以通过 E-mail 或手机短信息等方式及时地通知安全管理人员。

3. 代理

代理功能是应用级网关型防火墙的主要功能。一般有两种形式的代理功能：透明代理和传统代理。透明代理可以直接转发受保护网络客户主机的请求，不需要客户主机软件进行相应的设置，对用户保持透明。传统代理则需要客户软件进行必要的设置，最基本的就是要把代理服务器的地址告诉客户软件，5.1.2 节中介绍的应用级网关型防火墙主要就是指的传统代理。

4. NAT

NAT 指的是网络地址转换，主要有两种类型：SNAT（源地址转换）和 DNAT（目的地

址转换)。源地址转换经常用于将保留 IP 地址转换为合法 IP 地址的时候,例如企业内部网络采用保留的 IP 地址,也就是不可路由的 IP 来区分内部主机,当这些主机需要和外部网络进行通信时,就需要转换成一个可以在 Internet 上路由的 IP 地址,这也是源地址转换的典型应用。它既可以解决 IP 地址短缺的问题,又可以对外屏蔽内部网络结构,增加安全性。目的地址转换的一个例子就是刚刚提到的代理功能。

5. VPN

VPN(虚拟专用网络)是近来非常流行的一种功能。随着企业的分布范围越来越广,跨地区的企业网络也越来越多,如果企业的每个部分都采用专线连接,则价格太昂贵,因此大部分企业都采用了 VPN。其实现方法一般是,企业建立 VPN 服务器,外部的办事处或企业分部连接到此服务器上,这条连接一般不采用专线,而是直接通过公共网络,保证传输数据安全的方法是数据加密,IPSec 技术是目前采用的主要技术。

6. 流量统计和控制

防火墙的流量统计功能要求也越来越高,一般的防火墙要实现根据用户的流量统计和根据 IP 地址的流量统计。有了这些统计功能,进行流量控制的要求也就出现了,例如要保证某些 IP 地址的带宽不得低于 10MB 等。

5.1.5 分布式防火墙的实现及应用

1. 分布式防火墙的概念

由于传统防火墙的缺陷不断显露,于是有人认为防火墙是与现代网络的发展不相容的,并认为加密的广泛使用可以废除防火墙。但加密不能解决所有的安全问题,防火墙依然有它的优势,例如通过防火墙可以关闭危险的应用,通过防火墙管理员可以实施统一的监控,也能对新发现的 bug(漏洞)快速做出反应等。也有人提出了对传统防火墙进行改进的方案,例如多重边界防火墙、内部防火墙等,但这些方案都没有从根本上摆脱拓扑依赖,因而也就不能消除传统防火墙的固有缺陷,反而增加了网络安全管理的难度。

个人防火墙的出现弥补了传统防火墙的一些缺陷,它更明确主机会话的上下文关系,同时为网络增加了一道安全屏障,但是它依然无法从根本上解决内部网络的安全问题。原因如下:

(1) 个人防火墙依然依赖网络拓扑结构,容易受 IP 地址欺骗。

(2) 个人防火墙难以统一,网络管理难度大。

(3) 个人防火墙无法实现安全策略的统一配置和管理。

企业中大多数部门员工并非从事计算机行业,为使每个员工掌握防火墙配置技术而对其进行复杂的网络和网络安全知识培训是不现实的。另外,由不精通网络安全知识的员工配置防火墙,导致防火墙形同虚设。因此个人防火墙配合传统防火墙的方案在企业中也同样不可行。

为了克服以上缺陷而又保留防火墙的优点,美国 AT&T 实验室研究员 Steven M Bellovin 教授在他的论文《分布式防火墙》中首次提出了分布式防火墙(Distributed Firewall,DFW)的概念,给出了分布式防火墙的原型框架,奠定了分布式防火墙研究的基础。

传统防火墙缺陷的根源在于它的拓扑结构，分布式防火墙打破了这种拓扑限制，将内部网的概念由物理意义变成逻辑意义。按照 Steven 的说法，分布式防火墙是由一个中心来制定策略，并将策略分发到主机上执行，它使用一种策略语言（例如 Keynote）来制定策略，并被编译成内部形式存于策略数据库中，系统管理软件将策略分发到被保护主机，而主机根据这些安全策略和加密的证书来决定是接收还是丢弃数据包，从而对主机实施保护。在 DFW 中，主机的识别虽然可以根据 IP 地址，但 IP 地址是一种弱的认证方法，容易被欺骗，在分布式防火墙中建议采用强的认证方法，例如 IPSec。加密的证书作为主机认证识别的依据，一个证书的拥有权不易伪造，并独立于拓扑，所以只要拥有合法的证书，不管它处于物理上的内部网还是外部网都被认为是“内部”用户。加密认证是彻底打破拓扑依赖的根本保证。在 DFW 系统中，各台主机的审计事件都被上传到中心日志数据库中统一保存。

2. 分布式防火墙的本质特征

弄清分布式防火墙的本质特征有助于正确认识分布式防火墙，从而划清分布式防火墙和非分布式防火墙之间的界限。

（1）安全策略必须由管理员统一制定。这是分布式防火墙区别于个人防火墙的根本所在，虽然它们都是主机驻留防火墙，但个人防火墙中的所有行为都是个人行为，别人不能干涉。而分布式防火墙中的行为是集体行为，用户个人不能干涉，每台主机的安全策略都是整个组织安全策略的一部分，全部主机的安全策略之和构成一个组织的整体安全策略，所以分布式防火墙要求实行统一的策略管理。

（2）策略必须被推到网络的边缘即主机上实施。这是分布式防火墙的又一本质特征，因为分布式防火墙的本意就是要将策略从边界集中实施点迁移到网络末端即主机中来实施。

（3）日志统一收集管理。因为管理员要对全网进行安全监控，他必须掌握充分的信息，日志是管理员了解信息、追踪攻击者的主要依据。

综上所述，分布式防火墙的本质特征可概括为：策略集中制定分散实施，日志分散产生集中保存。这一本质特征保证了从管理员的角度来看，他管理分布式防火墙就像管理边界防火墙一样，由他负责制定全网的安全策略并对全网的安全状况进行监控，只不过策略的实施不在单一节点上而是分散到了多个节点而已。

3. 分布式防火墙的实现方法

自从 1999 年 11 月 Steven 的《分布式防火墙》发表以来，人们对分布式防火墙的实现进行了研究，提出了一些实现方法，并实现了原型系统，第一个商用分布式防火墙 CyberwallPLUS 也于 2001 年问世。下面介绍分布式防火墙的几种实现方法。

1）基于 OpenBSD UNIX 的实现

这是提出分布式防火墙概念的 Steven 等人实现的原型系统。该原型系统是在 OpenBSD UNIX 操作系统上修改内核并利用 KeyNote、IPSec 等技术加以实现的。OpenBSD 是理想的开发安全应用的平台。

该原型系统由 3 部分组成：内核扩展模块，用于实施安全机制；用户层策略后台处理程序，用于执行分布式防火墙策略；设备驱动程序，为内核和策略后台程序之间的双向通信提供接口。该原型系统在主机一端的功能模块如图 5-5 所示。

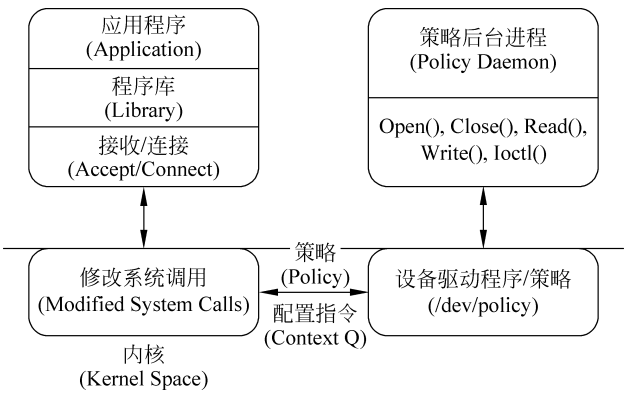

图 5-5 基于 OpenBSD UNIX 的分布式防火墙实现方案

(1) 内核扩展模块：是整个系统的执行模块，其功能是产生并提交策略上下文、根据策略守护进程的答复对数据包进行处理。在 UNIX 系统中用户使用系统调用 connect(2)创建连接请求，使用 accept(2)接收连接请求，一般情况下这两个系统调用不对数据流进行安全检查，为了在内核中实现包过滤功能需要对它进行修改。

(2) 策略后台处理程序：它运行在用户层，作用是根据策略服务器传输过来的安全策略和通信中对方传输的信任书(Credential，相当于证书)来决定接收还是丢弃数据包，并将判断结果返回内核。

(3) 设备驱动程序：该模块的功能是在用户策略后台处理程序和内核中被修改的系统调用之间建立一个通路。它运行于内核态，并向策略后台处理程序提供 read(2)、write(2)等功能调用，后台程序通过调用这些函数与内核交互。

2) 基于 IPsec 的分布式防火墙模型

Steven 在他的《分布式防火墙》中描述了一个基于 IPSec 的分布式防火墙模型。在 Steven 的模型中使用基于 IPSec 的加密证书名称表示网络主机，完全摒弃了以往使用 IP 地址表示主机的方法。该模型共由 3 个部分组成：系统管理模块、翻译器和主机策略执行模块。

网络安全管理员使用系统管理模块来管理所有的主机，定义安全策略，还可以向主机分发新的防火墙软件或安装补丁。网络安全管理员根据主机标识符定义安全策略，然后将定义好的安全策略使用翻译器编译成某种环境的内部格式送出。策略被分发到参与分布式防火墙的各个主机上，有主机策略执行模块负责执行。

3) 基于网卡(NIC)的实现

该方案是美国国防部资助的研究项目，它是基于一种特殊的网卡(3Com3CR990 系列网卡)实现的，称为 EFW(Embedded Firewall，嵌入式防火墙)。这种网卡有内置的处理器和存储器，能独立于主机操作系统而运行；还有内置的加密引擎，使 NIC 之间可以通过 IPSec 加密通信；另外这种网卡使用广泛且价格相对便宜。

(1) EFW 组件：EFW 的主要组件分为主机端组件和服务器端组件，如图 5-6 所示。

① EFW 主机端组件：主要包括 EFW 增强的 NIC、NIC 驱动程序与运行时映像和助理这 3 个部分。EFW 增强的 NIC 中的固件是在安装 EFW 时装入的，它包括包过滤引擎和管

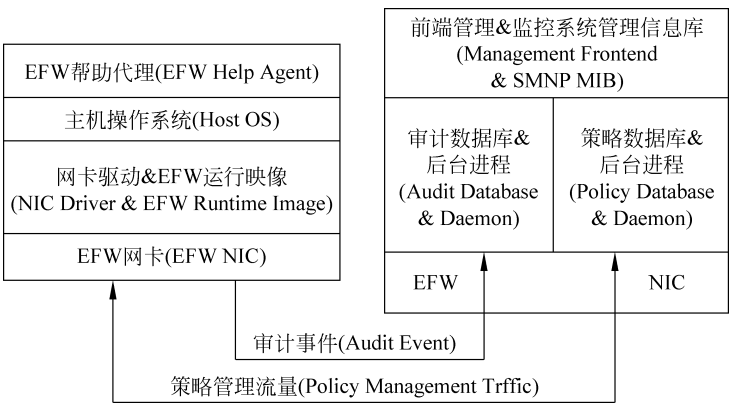

图 5-6　基于网卡的分布式防火墙实现方案

理接口。包过滤引擎能根据标准的参数决定接收或拒绝数据包。管理接口负责从服务器下载策略并上传审计事件到审计数据库，它也负责管理本地 NIC 与服务器之间的安全隧道。驱动程序在机器启动时下载运行时映像(Running Image)并放入固件中，运行时映像的完整性如果受到破坏，NIC 将无法正常工作，从而保证一旦 EFW NIC 被安装，用户将不能废除它，除非通过策略服务器进行适当的操作，因为用户的改动会破坏运行时映像的完整性。EFW 助理的作用有两个，一个作用是给 NIC 传输本机的 IP 地址，另一个作用是定期向策略服务器发送“心跳(Heartbeat)”，这是为了防止恶意的用户用其他 NIC 取代 EFW NIC，因为这样心跳就会停止，从而引起管理员的注意。

② EFW 服务器端组件：主要包括管理组件、策略组件和审计组件 3 个部分。管理组件的主要目的是给管理员提供一个工具去建立和分发策略，也提供一个事件日志浏览器。策略组件的作用是接收管理员定义的策略并编译成过滤规则，然后放入策略数据库中。被保护的机器启动时自动到策略数据库中取回自己的安全策略。当服务器中的策略被修改时，策略组件能自动地将它“推”到相应主机上执行。审计组件收集并整理从各个 NIC 传输过来的审计事件，并提供给管理组件处理。

(2) EFW 的集中管理模式：EFW 将主机分成若干个策略域，每个策略服务器管理一个策略域，一个策略域可以包含整个组织，也可只包含一两个部门。在每个策略域中，NIC 根据主机执行的功能分成若干个组，每个组被分配相同的策略。策略中的规则也可以进行分组，以简化策略的制定、分发和更新。审计事件的设置可建立在整个策略、策略类型或单个策略上。

该实现方案的主要优点是基于硬件、不依赖操作系统，因而难以被绕过，具有坚固的基础。缺陷是 NIC 的处理能力有限。

4) 基于 Windows 平台实现的原型系统

CyberwallPLUS 是 Network-1 公司于 2001 年发布的分布式防火墙产品，基于 Windows 平台实现，用于保护 Windows NT/2000 桌面机和服务器。它包括中心管理部件、桌面机防火墙部件和服务器、边界防火墙部件等。所有这些部件都包含如图 5-7 所示的结构，包括包过滤引擎和用户配置接口(可选的)。包过滤引擎采用嵌入内核的方式运行，处于链路层和网络层之间，能够提供访问控制、状态检测和入侵检测的功能。用户配置接口在安

装时是可选的，如果选择安装则用户或管理员可在本地配置安全策略，如果不安装则策略只能由管理员从管理中心加以配置或使用远程管理模块进行配置。该产品实现了中心管理功能，管理员通过中心管理模块可对各台主机实施全方位的控制，包括分发安全策略和远程配置。该产品也具有较完善的审计功能，审计日志可通过建立的连接、阻塞的数据包、入侵尝试和应用类型等来建立（可配置选项）。中心管理模块可对日志和报警信号进行汇集。

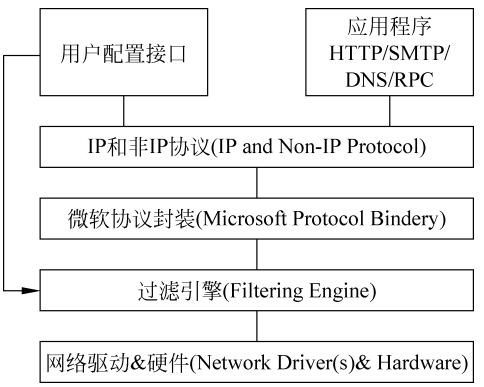

图 5-7 基于 Windows 平台的分布式防火墙实现方案

4. 分布式防火墙的典型应用

对大型网络以及需要打破网络拓扑限制的组织，分布式防火墙是最佳的选择。下面列举两个分布式防火墙的典型应用

1）锁定关键服务器

对企业中的关键服务器，可以安装分布式防火墙作为第二道防线，使用分布式防火墙的集中管理模块对这些服务器制定精细的访问控制规则，增强这些服务器的安全性。

2）商务伙伴之间共享服务器

随着电子商务的发展，商务伙伴之间需要共享信息，外联网是一般的解决方案，但外联网的实施代价较高。可以用上面介绍的 EFW 在一台服务器上安装两个 NIC，一个与内部网络相连，另一个与伙伴相连，这样可以方便地实现服务器共享。拥有服务器的一方控制服务器的两个 NIC，分别对其进行设置，使对方能够进入共享服务器，但不能进入本方的内部网络。

5.2 入侵检测技术

5.2.1 入侵和入侵检测

1. 入侵

入侵（Intrusion）是所有试图破坏网络信息的完整性、保密性、可用性、可信任性的行为。入侵是一个广义的概念，不仅包括发起攻击的人取得超出合法范围的系统控制权，也包括收集漏洞信息，造成拒绝服务等危害计算机和网络的行为。入侵行为主要有以下几种：

（1）外部渗透：指既未被授权使用计算机，又未被授权使用数据或程序资源的渗透。

(2) 内部渗透：指虽被授权使用计算机，但是未被授权使用数据或程序资源的渗透。

(3) 不法使用：指利用授权使用计算机、数据和程序资源的合法用户身份的渗透。

这 3 种入侵行为是可以相互转变，互为因果的。例如，入侵者通过外部渗透获取了某用户的账户和密码，然后利用该用户的账户进行内部渗透，最后，内部渗透也可能转变为不法使用。

2. 入侵检测

入侵检测(Intrusion Detection)是一种试图通过观察行为、安全日志或审计资料来检测发现针对计算机或网络入侵的技术，这种检测通过手工或专家系统软件对日志或其他网络信息进行分析来完成。而更广义的说法是：识别企图侵入系统非法获得访问权限行为的过程，它通过对计算机系统或计算机网络中的若干关键点收集信息并对其进行分析，从中发现系统或网络中是否有违反安全策略的行为和被攻击的迹象。

入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时防护，在网络系统受到危害之前拦截和对入侵做出响应。强大的入侵检测软件的出现极大地方便了网络管理，其实时报警功能为网络安全增加了又一道保障。从网络安全立体纵深、多层次防御的角度出发，入侵检测理应受到人们的高度重视，但现状是入侵检测还不够成熟，处于发展阶段，或者是防火墙中集成较为初级的入侵检测模块，所以对于入侵检测技术的研究是很重要的。未来的入侵检测系统将会结合其他网络管理软件，形成入侵检测、网络管理、网络监控三位一体的结构。

5.2.2　入侵检测的分类

1. 特征检测

特征检测又称基于知识的入侵检测，这类检测方法的原则是，任何与已知入侵模型符合的行为都是入侵行为。它要求首先对已知的各种入侵行为建立签名，然后将当前的用户行为和系统状态与数据库中的签名进行匹配。通过收集入侵攻击和系统缺陷的相关知识构成入侵系统中的知识库，然后利用这些知识寻找那些企图利用这些系统缺陷的攻击行为，来识别系统中的入侵行为。系统中任何不能明确地认为是攻击的行为，都可以认为是系统的正常行为。因此，基于入侵知识的入侵检测系统具有很好的检测精确度，至少在理论上具有非常低的虚警率，但是其检测完备性则依赖于入侵攻击和系统缺陷的相关知识的不断更新和补充。

使用这类入侵检测系统，可避免系统以后再遭受同样的入侵攻击，对于网络入侵检测技术的研究可以使系统安全管理员很容易地知道系统遭受到哪种攻击并采用相应的行动。但是，知识库的维护需要对系统中的每一个缺陷都要进行详细分析，这不仅是一个耗时的工作，而且关于攻击的知识，依赖于操作系统、软件版本、硬件平台以及系统中运行的应用程序。这种入侵检测技术主要有以下局限性：

(1) 检测系统知识库中的入侵攻击知识与系统运行环境有关。

(2) 对于系统内部攻击者的越权行为，由于它们没有利用系统的缺陷，因而很难检测出来。

特征检测的关键问题是规则的获取和表示，构成入侵威胁的审计记录会触发相应规则。

这些规则可以识别出危及系统安全的单个审计事件，也可以分析出构成一个入侵过程的简单审计事件序列。

这种检测方法的特点是检测正确率高而覆盖率偏低，它的弱点是只能发现已知入侵行为。但由于实际情况中大部分入侵者使用的都是已知的攻击方法，因此该技术还是可以有效抵御大部分攻击行为的。

1）专家系统

专家系统是基于知识的检测中运用最多的一种方法。将有关入侵的知识转化成 if-then 结构的规则，即将构成入侵所要求的条件转化为 if 部分，将发现入侵后采取的相应措施转化成 then 部分，当其中某个或部分条件满足时，系统就判断为入侵行为发生。其中的 if-then 结构构成了描述具体攻击的规则库，状态行为以及其语义环境可以根据审计事件得到，推理模块根据规则和行为完成判断工作。

2）状态转换分析

状态转换分析最早由 R. Kemmerer 提出，即将状态转换图应用于入侵行为的分析。状态转换法将入侵过程看作一个行为序列，这个行为序列网络入侵检测技术的研究导致系统从初始状态转入被入侵状态。分析时首先针对每一种入侵方法确定系统的初始状态和被入侵状态，以及导致状态转换的转换条件，和导致系统进入被入侵状态必须执行的操作。然后用状态转换图来表示每一个状态和特征事件，这些事件被集成于模型中，所以检测时不需要一个个地查找审计记录。但是，状态转换是针对事件序列分析的，所以不善于分析过分复杂的事件，而且不能检测与系统状态无关的入侵。

Petri 网用于入侵行为分析是一种类似于状态转换图分析的方法。利用 Petri 网的有利之处在于它能一般化、图形化地表达状态，并且简洁明了。虽然很复杂的入侵特征能用 Petri 网表达得很简单，但是对原始资料匹配时的计算量会很大。下面是这种方法的一个简单示例，如图 5-8 所示，表示在一分钟内如果登录失败的次数超过 4 次，系统便发出警报。其中竖线代表状态转换，如果在状态 S1 发生登录失败，则产生一个标志变量，并存储事件发生时间 T1，同时转入状态 S2。如果在状态 S4 时又有登录失败，而且这时的时间（T2－T1）＜60 秒，则系统转入状态 S5，即为入侵状态，系统发出警报并采取相应措施。

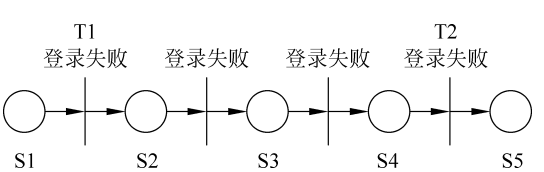

图 5-8　Petri 网—分钟内 4 次登录失败分析

基于知识的检测技术的关键是如何从已知的入侵行为中提取特征，以正确区分真正的入侵与正常行为；如何构造入侵行为的描述语言，并使这种描述语言具有一定的扩展性和适应性。随着对计算机系统弱点和攻击行为的不断收集和研究，入侵行为的特征越来越精确，这使得特征检测技术的使用也越来越广泛。

2. 异常入侵检测

异常检测又称为基于行为的入侵检测，根据使用者的行为或资源使用网络入侵检测技术的研究使用状况来判断是否入侵，而不依赖于是否出现具体行为来检测，任何与已知正常

行为不符合的行为都是入侵行为。这类检测方法的基本思想是：通过对系统审计资料的分析建立起系统主体的正常行为的特征轮廓，检测时，如果系统中的审计资料与已建立的主体正常行为特征有较大出入，就认为系统遭到入侵。特征轮廓是借助主体登录的时间、位置、CPU 的使用时间以及文件的存取属性等，来描述主体的正常行为特征。当主体的行为特征改变时，对应的特征轮廓也相应改变。

异常检测系统在准备阶段通过一定时间的学习为用户正常情况下的行为建立行为轮廓(Profile)，在使用阶段系统一方面通过比较用户当前行为与原先行为轮廓的偏差来检测入侵，另一方面继续根据用户的正常行为来修正行为轮廓。同样，异常检测系统也可为整个计算机系统建立正常行为轮廓。

异常入侵检测方法的关键在于对用户或者系统建立正确的行为轮廓，在早期的异常入侵检测系统中通常用统计模型来进行，例如将用户登录时间、登录失败次数、资源访问频度等一些特征量作为随机变量，通过统计模型计算出这些随机变量的新观察值落在一定区间内的概率，并且根据经验规定一个阈值，超过阈值则认为发生了入侵。后来有很多人工智能技术应用于异常检测，例如神经元网络技术和资料挖掘技术等。

异常入侵检测的最大优点是能检测出一些未知攻击，最大缺点是会产生很大的虚警率，因为异常并不一定是入侵，而且结果缺乏可解释性。

1) 概率统计方法

概率统计方法是基于异常检测中应用最早也是最多的一种方法。检测器根据用户对象的动作为每个用户都建立一个用户特征表，通过比较当前特征与已存储的固定模式的以前特征，从而判断是否是异常行为。

用户特征表需要根据审计记录情况不断地加以更新。用于描述特征的变量类型有：

(1) 操作密度：度量操作执行的速率，常用于检测通过长时间平均觉察不到的异常行为。

(2) 审计记录分布：度量在最新记录中所有操作类型的分布。

(3) 范畴尺寸：度量在一定动作范畴内特定操作的分布情况。

(4) 数值尺度：度量那些产生数值结果的操作，例如 CPU 使用量、I/O 使用量等。

这些变量所记录的具体操作包括：CPU 的使用，I/O 的使用，使用地点及时间，邮件使用，编辑器使用，编译器使用，所创建、删除、访问或改变的目录及文件，网络上的活动等。在 SRI/CSL 的入侵检测专家系统中给出了一个特征简表的结构：

<变量名，行为描述，例外情况，资源使用，时间周期，变量类型，门限值，主体，客体，值>

其中的变量名、主体和客体唯一地确定了每一个特征简表，特征值由系统根据审计资料周期性地产生。这个特征值是所有有悖于用户特征的异常程度值的函数。如果假设 S_1，S_2，…，S_n 分别是用于描述特征的变量 M_1，M_2，…，M_n 的异常程度值，S_i 值越大说明异常程度越大。则这个特征值可以用所有 S_i 值的加权平方和来表示：

$$M = \sum_{i=1}^{n} a_i S_i^2, \quad a_i > 0$$

其中，a_i 表示每一个特征的权值。

如果选用标准偏差作为判别准则，则标准偏差为：$\sigma^2 = M/(n-1) - \mu^2$，其中 $\mu = M/n$。如果某 S 值超过了 $\mu \pm d\sigma$，就认为出现了异常。

概率统计方法的优越性在于能够发现未知的入侵，并能对用户活动进行适应性学习，以发现内部用户的渗透和异常，有成熟的概率统计理论基础。但也有些不足之处：统计检测对事件发生的次序不敏感，完全依靠统计理论可能漏检那些利用彼此关联事件的入侵行为；定义是否入侵的判断阀值的选择困难，如果该值设的过高则漏检率提高，如果阀值过低则会造成误检率提高。

2）神经网络方法

利用神经网络检测入侵的基本思想是用一系列信息单元（命令）训练神经单元，这样在给定一组输入后，就可能预测出输出。与统计理论相比，神经网络更好地表达了变量间的非线性关系，并且能自动学习和更新。实验表明 UNIX 系统管理员的行为几乎全是可以预测的，对于一般用户，不可预测的行为也只占了很少的一部分。用于检测的神经网络模块结构大致是这样的：当前命令和刚过去的 w 个命令组成了网络的输入，其中 w 是神经网络预测下一个命令时所包含的过去命令集的大小。根据用户的代表网络入侵检测技术的研究性命令序列训练网络后，该网络就形成了相应用户的特征表，于是网络对下一事件的预测错误率在一定程度上反映了用户行为的异常程度。基于神经网络的检测思想可用图 5-9 表示。

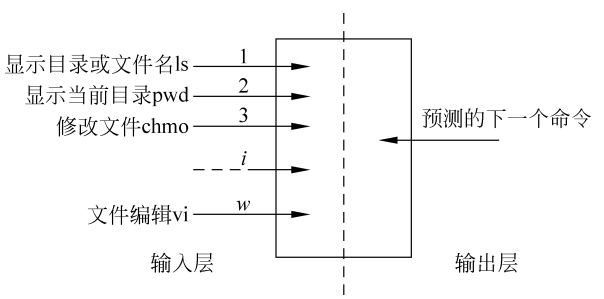

图 5-9 神经网络的检测思想

图 5-9 中输入层的 w 个箭头代表了用户最近的 w 个命令，输出层预测用户将要发生的下一个动作。神经网络方法的优点在于能更好地处理原始资料的随机特性，即无须对这些资料作任何统计假设，并且有较好的抗干扰能力。缺点在于网络拓扑结构以及各元素的重复性很难定；命令窗口 w 的大小也难以选取，窗口太小则网络输出不好，窗口太大则网络会因为大量无关资料而降低效率。

如果能在一个检测系统中将异常入侵检测和特征的入侵检测有机地结合起来，那么会大大减少入侵检测的虚警率和漏警率，基于安全规范的入侵检测方法可以起到这种作用，它的优点是不仅能识别已知攻击，还能识别出未知的攻击。

5.2.3 入侵检测系统及其分类

最早的入侵检测模型由 Dorothy Denning 在 1968 年提出。这个模型与具体输入无关，对此后的大部分实用系统都很有借鉴价值。入侵检测系统（Intrusion Detection System，IDS）在逻辑上必须包含最基本的 3 个部分：数据提取模块、数据分析模块和结果处理模块。入侵检测一般分为 3 个步骤：数据提取、数据分析和结果处理。入侵检测系统基本结构如图 5-10 所示。

图 5-10 中模块划分是基于功能的划分，省略了界面管理模块、配置管理模块等其他

模块。

数据提取模块的作用在于为系统提取数据。数据为网络数据包、计算机的日志文件和系统调用记录等。如果系统是基于主机的入侵检测系统，数据主要为主机的日志文件、审计记录等。如果系统是基于网络的入侵检测系统，数据就为网络中传输的数据包。

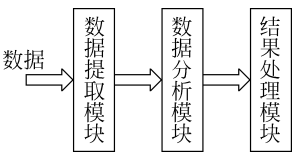

图 5-10　入侵检测系统的基本结构图

数据分析模块对数据进行深入分析，发现攻击并根据分析的结果产生事件，传递到结果处理模块。数据分析的方式有很多种，并大致分为误用检测和异常检测两大类型。数据分析模块是入侵检测系统的核心模块。

结果处理模块的作用在于告警与反应，这实际上与 PPDR 模型的 R 有所重叠。结果处理模块应该对不同的攻击有不同的响应策略，一般发现攻击后，模块会启动一些相对应的事件，例如通知管理员、系统自动恢复以前的状态、切断网络等。

入侵检测系统的具体原理如图 5-11 所示。

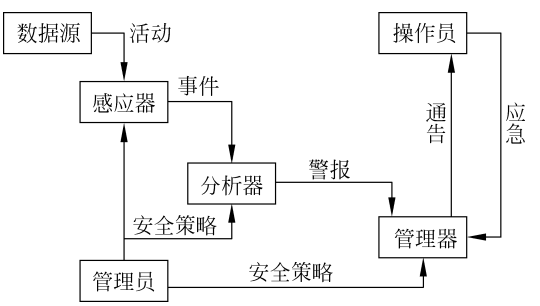

图 5-11　入侵检测系统原理示意图

入侵检测系统的原理比较简单，当感应器感知到数据后，由系统管理员所提供的安全策略对该感应事件进行分析审计数据，一旦分析结果认定为入侵则发出警报信息，启动管理器通知操作人员并启动相应的应急措施，如关闭相应连接、切断网络，以便帮助管理员采取进一步的应急措施。

目前国内外已经开发出许多入侵检测系统，这些 IDS 从不同的角度有着不同的分类方法，其中最主要的是按照入侵检测的信息来源和检测方法来进行分类的。

1. 基于主机和网络的入侵检测系统

入侵检测系统根据信息来源的不同可以分为基于主机的入侵检测系统（Host-based Intrusion Detection System，HIDS）和基于网络的入侵检测系统（Network-based Intrusion Detection System，NIDS）两大类。基于主机的入侵检测系统从单个主机上提取资料（例如系统日志等）作为入侵分析的资料源，而基于网络的入侵检测系统从网络上提取网络报文作为入侵分析的资料源。通常来说基于主机的入侵检测系统只能检测单个主机系统，而基于网络的入侵检测系统可以对本网段的多个主机系统进行检测，多个分布于不同网段上的基于网络的入侵检测系统可以协同工作以提供更强的入侵检测能力。

1）基于主机的入侵检测系统（HIDS）

基于主机的入侵检测系统（HIDS）主要从主机的审计记录和日志文件中获得所需的数

据，并辅以主机上的其他信息，例如文件系统属性、进程管理状态、系统资源使用情况等，在此基础上完成检测入侵行为的任务。基于主机的入侵检测在 20 世纪 80 年代初期就出现了，早期的入侵检测系统都是基于主机的入侵检测技术。那时网络环境比较简单，在这种情况下通过记录检查可疑行为是非常常见的操作。由于入侵在当时是相当少见的，在对攻击的事后分析就可以防止今后的攻击。HIDS 在发展过程中还结合了一些其他技术，对关键的系统文件和可执行文件的检查是入侵检测的一个常用方法，主要是通过定期检查校验和来进行，以便发现意外的变化；还有一些监测端口活动的方法，通过监测特定端口，当发现它们被访问时向管理员报警。

HIDS 的主要目的是在事件发生后提供足够的分析研究来阻止进一步的攻击，尽管它不如 NIDS 快捷，但它确实具有 NIDS 无法比拟的优点。这些优点包括：

(1) 能够监视特定的系统行为。HIDS 能够监视所有的用户登录和退出，甚至用户所做的所有操作，审计系统在日志里记录的策略改变，监视关键系统文件和可执行文件的改变等。

(2) 因为检测在主机上运行的命令序列要比检测网络流相对简单得多，系统的复杂性也小得多。HIDS 通常情况下比 NIDS 的虚警率要低，由于使用含有已发生事件信息，HIDS 可以比 NIDS 更加准确地判断攻击是否成功。

(3) 有些攻击在网络的数据流中很难发现，或者根本没有通过网络而是在本地进行，这时 NIDS 将无能为力，只能借助于 HIDS。

(4) 适用被加密的和交换的环境。由于 HIDS 安装在遍布企业的各种主机上，它们比 NIDS 更加适于交换和加密的环境。交换设备可将大型网络分成许多小型网络段加以管理，所以从覆盖足够大的网络范围的角度出发，很难确定配置 NIDS 的最佳位置。HIDS 可安装在所需的重要主机上，在交换的环境中具有更高的能见度。某些加密方式也向 NIDS 发出了挑战。根据加密方式在协议堆栈中的位置不同，NIDS 可能对某些攻击没有反应，而 HIDS 没有这方面的限制，当操作系统及 HIDS 发现即将到来的业务时，数据流已经被解密了。

HIDS 的主要缺点有：

(1) HIDS 安装在需要保护的设备上，这会降低应用系统的效率。因为它依赖于服务器固有的日志与监视能力，如果服务器没有配置日志功能则必须重新配置，否则会给运行中的业务系统带来不可预见的性能影响。

(2) 全面布置 HIDS 代价较大。企业中很难将所有主机都采用 HIDS 保护，只能选择部分主机保护。那些尚未安装 HIDS 的机器将成为保护的盲点，入侵者可以利用这些机器达到攻击目标。

(3) HIDS 除了监测自身的主机以外，根本不检测网络上的情况。而且对入侵行为的分析的工作量会随着主机数目的增加而增加。

2) 基于网络的入侵检测系统(NIDS)

基于网络的入侵检测系统(NIDS)通常是作为一个独立的单元放置于被检测网络上的。它使用原始网络数据包作为入侵检测的数据来源，通常利用一个运行在混杂模式下的网络适配器来实时监视并分析网络中所有通信数据。NIDS 通常使用 4 种常用检测技术来识别入侵：模式、表达式或字节匹配；频率或阈值判断；低级事件的相关性；统计学意义上的非常规现象检测。一旦检测到了攻击行为，NIDS 的响应模块就提供多种选项以通知、报警并对攻击采取相应的反应。反应会因产品而异，但通常都包括通知管理员、报警、中断连接和

作为证据支持起诉而做的会话记录。

NIDS 的主要优点有：

(1) 成本较低。NIDS 可在几个关键访问点上进行策略配置，以观察发往多个系统的网络通信。

(2) 能够检测到 HIDS 无法检测的入侵。NIDS 能够检查数据包的头部而发现非法攻击；能够检测到那些来自网络的攻击；能够检测到超过授权的非法访问。

(3) NIDS 不依赖于保护主机的操作系统，而且隐蔽性好。一个网络上的监测器不像一个主机那样显眼和易被存取，因而也不那么容易遭受攻击。

NIDS 的主要缺点有：

(1) 只检查它直接连接网段的通信，不能检测在不同网段的网段包。在使用交换以太网的环境中就会出现检测范围的局限，而安装多台 NIDS 的传感器会使部署整个系统的成本大大增加。

(2) NIDS 可能会将大量的数据传回分析系统中。在一些系统中监测特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少回传的资料量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器。这样的系统中的传感器协同工作能力较弱。

(3) 网络入侵检测系统处理加密的会话过程较困难。目前通过加密信道的攻击尚不多，随着 IPv6 的普及，这个问题会越来越突出。

这两种入侵检测系统都具有自己的优点和不足，互相可作为补充。HIDS 可以精确地判断入侵事件，可对入侵事件立即进行反应，还可以针对不同操作系统的特点判断应用层的入侵事件，其缺点是会占用主机宝贵的资源。而 NIDS 只能监视本网段的活动，并且精确度较差，在交换网络环境中难于配置，防入侵欺骗的能力也比较差，但是它可以提供实时网络监视，并且监视粒度更细致。

随着高速网络和交换式网络的迅速发展，入侵检测领域的实践者们倾向于将这两种不同的方法结合起来，IDS 必须包含紧密融合的主机和网络部分，以便得到更多的攻击和入侵信息。必须大幅度提高网络对攻击和错误使用的抵抗力，使安全措施的实施更加有效，并使设置更加灵活。目前出现了一种网络节点入侵检测系统(Network Node Intrusion Detection System，NNIDS)，它结合了上述两种方法，将入侵检测任务委派到网络中的各个主机上，以减轻由于高速和交换式网络而给入侵检测系统带来的巨大压力，同时它还非常适用于网络中存在加密资料的情况。

2. 误用和异常入侵检测系统

入侵检测系统根据检测方法可分为两种基本检测类型：误用入侵检测系统(Misuse Intrusion Detection System)和异常入侵检测系统(Anomaly Intrusion Detection System)。

1) 误用入侵检测系统

误用入侵检测系统根据已知入侵类型(知识、模式等)来检测目标网络系统中的入侵，它是指运用已知攻击方法，根据已定义好的入侵模式，通过分析数据判断这些入侵模式是否出现来进行检测。首先收集入侵行为的特征，建立相关的误用模式库，在后续的检测过程中，将收集到的数据与库中的特征代码进行比较，得出是否入侵的结论。这种方法由于依据具体特征库进行判断，所以检测准确度很高，并且因为检测结果有明确的参照，也为系统管理

员做出相应措施提供了方便。

误用检测主要不足在于只能检测已知的攻击模式，当新漏洞或新入侵方式出现时，需要由人工或其他机器学习系统得出新入侵行为的特征模式，添加到误用模式库中，才能使系统具备检测新的入侵行为的能力。

2）异常入侵检测系统

异常入侵检测系统将被监控系统正常行为的信息作为检测目标系统中是否有入侵的异常活动的依据，它根据使用者的行为或资源使用状况的正常程度来判断是否入侵。其特点是首先总结正常操作应该具有的特征，得出正常操作的模型，然后对后续的操作进行监视，一旦发现偏离正常统计等意义上的行为，立即进行报警。异常检测的优点是它能抽取系统的正常行为以此检测系统异常行为。这种能力不受系统以前是否知道这种入侵与否的限制，所以能够检测新的入侵行为。

异常入侵检测的主要不足则是误报率很高。此外，若入侵者了解到检测方法，就可以通过慢慢训练检测系统，避免系统指标突变，到最后连异常行为也可能认为是正常的方法来进行欺骗以达到入侵目的。

误用入侵检测系统通常需要定义一组规则，而这种工作模式不能发现新的攻击行为，故不能提供全面的保护，但误报率很低。异常入侵检测系统所能检测到的威胁行为更多，包括已知的和未知的威胁，但这种模式会导致大量的误报。通过这一比较，不难发现它们在很大程度上具有互补性。要在提高检测率的同时避免过高的误报率，就必须将两种检测方法有效地结合起来。

3. 集中式和分布式入侵检测系统

根据入侵检测系统各模块运行的分布方式不同，可分为集中式入侵检测和分布式入侵检测两类。

1）集中式入侵检测系统(Centralized Intrusion Detection System，CIDS)

CIDS 的各个模块包括数据的收集与分析以及响应都集中在一台主机上运行，这种方式适用于网络环境比较简单的情况。CIDS 也可以有多个分布于不同主机上的审计程序，但只有一个中央入侵检测服务器，审计程序将当地收集到的数据踪迹发送给中央服务器进行分析处理。CIDS 在系统的可伸缩性、可配置性方面存在致命缺陷。随着网络规模的增大，主机审计程序和服务器之间传输的数据量就会骤增，必将导致网络性能的降低。而且一旦中央服务器出现故障，整个系统将会陷入瘫痪。

2）分布式入侵检测系统(Distributed Intrusion Detection System，DIDS)

相对于 CIDS，DIDS 的各个模块分布在网络中不同的计算机、设备上，其分布性主要体现在数据收集模块上，如果网络环境比较复杂、数据量比较大，那么数据分析模块也会分布在网络的不同计算机和设备上，通常是按照层次性的原则进行组织。DIDS 根据各组件间的关系还可细分为层次式 DIDS 和协作式 DIDS。其中层次式 DIDS 是一种部分分布控制形式，而协作式 DIDS 是全分布式控制形式。

(1) 层次式 DIDS：为解决 CIDS 的缺陷，在监视大规模网络时，需将网络进行分层管理。在层次式 DIDS 中，定义了若干个分等级的监测区域，每一个区域有一个专门负责分析数据的 IDS，每一级 IDS 只负责所监测区域的数据分析，然后将结果传输给上一级 IDS。层次式 DIDS 通过分层分析很好地解决了集中式 IDS 的不可扩展的问题，但同时也存在下列

问题：当网络的拓扑结构改变时，区域分析结果的汇总机制也需要做相应的调整；一旦位于最高层的 IDS 受到攻击后，其他那些从网络多路发起的协同攻击就容易逃过检测，造成漏检。

(2) 协作式 DIDS：协作式 DIDS 将中央检测服务器的任务分配给若干个互相合作的 HIDS，这些 HIDS 不分等级，各司其职，负责监控本地主机的某些活动，所有的 HIDS 并发执行并相互协作。协作式 DIDS 的特点就在于它的各个节点都是平等的，一个局部 DIDS 的失效不会导致整个系统的瘫痪，也不会导致协同攻击检测的失败。因而，系统的可扩展性、安全性都得到了显著提高。但同时它的维护成本也很高，并且增加了所监控主机的工作负荷，例如通信机制、审计开销、踪迹分析等。而且主机之间的通信、审计以及审计数据分析机制的优劣直接影响了协作式 DIDS 的效率。

5.2.4　入侵检测系统的局限性及发展趋势

1. 当前的入侵检测产品存在的问题

虽然入侵检测系统的重大作用不言而喻，但是它作为一项比较新的技术，还存在一些技术上的困难，不是所有厂商都有研发入侵检测产品的实力。目前的入侵检测产品大多存在这样一些问题。

1) 误报和漏报的矛盾

入侵检测系统对网络上所有的数据进行分析，如果攻击者对系统进行攻击尝试，而系统相应服务开放，只是漏洞已经修补，那么这一次攻击是否需要报警？这就是一个需要管理员判断的问题，因为这也代表了一种攻击的企图。但大量的报警事件会分散管理员的精力，反而无法对真正的攻击做出正确反映。和误报相对应的是漏报，随着攻击的方法不断更新，入侵检测系统是否能报出网络中所有的攻击也是一个问题。

2) 隐私和安全的矛盾

入侵检测系统可以收到网络的所有数据，同时可以对其进行分析和记录，这对网络安全极其重要，但难免会对用户的隐私构成一定风险，这就要看具体的入侵检测产品是否能提供相应功能以供管理员进行取舍。

3) 被动分析与主动发现的矛盾

入侵检测系统采取被动监听的方式发现网络问题，无法主动发现网络中的安全隐患和故障。如何解决这个问题也是入侵检测产品面临的问题。

4) 海量信息与分析代价的矛盾

随着网路数据流量的不断增加，能否高效处理网路中的数据也是衡量入侵检测产品的重要依据。

5) 功能性和管理性的矛盾

随着入侵检测产品功能的增加，可否在功能增加的同时尽可能地降低管理难度？例如，入侵检测系统的所有信息都存储在数据库中，此数据库能否自动维护和备份而不需管理员的干预？另外，入侵检测系统自身安全性如何？是否易于部署？采用何种报警方式？这些都是需要考虑的因素。

6) 单一的产品与复杂的网络应用的矛盾

入侵检测产品最初的目的是为了检测网络的攻击，但仅仅检测网络中的攻击远远无法

满足目前复杂的网络应用需求。通常，管理员难以分清网络问题是由于攻击引起的还是网络故障引起的。入侵检测系统检测出的攻击事件又如何处理？可否和目前网络中的其他安全产品进行配合？

2. 入侵检测系统的发展趋势

未来 DIDS 技术的发展将着重于以下几个方面。

1）分析技术的改进

入侵检测误报和漏报的解决将最终依靠分析技术的改进。目前入侵检测分析方法主要有统计分析、模式匹配、数据重组、协议分析和行为分析等。

统计分析是统计网络中相关事件发生的次数，达到判别攻击的目的。模式匹配利用对攻击的特征字符进行匹配完成对攻击的检测。数据重组是对网络连接的数据流进行重组再加以分析，而不仅仅分析单个数据包。

协议分析技术是在对网络数据流进行重组的基础上，理解应用协议，再利用模式匹配和统计分析技术来判明攻击。例如某个基于 HTTP 协议的攻击含有 ABC 特征，如果此数据分散在若干个数据包中，假如一个数据包包含 A，另外一个包含 B，还有一个包含 C，则单纯的模式匹配就无法检测，只有基于数据流重组才能完整检测。而利用协议分析则只在符合的协议（例如 HTTP）检测到此事件才会报警。假设此特征出现在 E-mail 里，因为不符合协议，就不会报警。利用此技术有效地降低了误报和漏报。

行为分析技术不仅简单分析单次攻击事件，还根据前后发生的事件确认是否确有攻击发生，攻击行为是否生效，这是入侵检测分析技术的最高境界。但目前由于算法处理和规则制定的难度很大，目前还不是非常成熟，但这是入侵检测技术未来发展的趋势。目前最好综合使用多种检测技术，而不只是依靠传统的统计分析和模式匹配技术。另外，规则库是否及时更新也和检测的准确程度相关。

2）内容恢复和网络审计功能的引入

前面已经提到，入侵检测的最高境界是行为分析。但行为分析目前还不是很成熟，因此个别优秀的入侵检测产品引入了内容恢复和网络审计功能。内容恢复即在协议分析的基础上，对网络中发生的行为加以完整的重组和记录，网络中发生的任何行为都逃不过它的监视。网络审计即对网络中所有的连接事件进行记录。入侵检测的接入方式决定入侵检测系统中的网络审计不仅类似防火墙可以记录网络进出信息，还可以记录网络内部连接状况，此功能对内容无法恢复的加密连接尤其有用。

内容恢复和网络审计让网络管理员看到网络的真正运行状况，其实就是调动网络管理员参与行为分析的过程。此功能不仅能使网络管理员看到孤立的攻击事件的报警，还可以看到整个攻击过程，了解攻击确实发生与否，查看攻击者的操作过程，了解攻击造成的危害，不但发现已知攻击，同时发现未知攻击，不但发现外部攻击者的攻击，也发现内部用户的恶意行为。毕竟网络管理员是最了解其网络的，他们通过此功能的使用，很好地达到了行为分析的目的。但使用此功能的同时需注意对用户隐私的保护。

3）集成网络分析和管理功能

入侵检测不仅可以对网络攻击进行检测，同时还可以收到网络中的所有数据，对网络的故障分析和健康管理也可起到重大作用。当网络管理员发现某台主机有问题时，也希望能马上对其进行管理。入侵检测也不应只采用被动分析方法，最好能和主动分析相结合。所以，

入侵检测产品集成网管功能、扫描器(Scanner)及嗅探器(Sniffer)等功能是以后发展的方向。

4) 安全性和易用性的提高

入侵检测系统是个安全产品,其自身安全极为重要。因此,目前的入侵检测产品大多采用硬件结构透明式接入来免除自身安全问题。同时,对易用性的要求也日益增强,例如,全中文的图形界面,自动的数据库维护,多样的报表输出。这些都是优秀入侵检测产品的特性和以后继续发展细化的趋势。

5) 改进对大数据量的网络的处理方法

随着对大数据量处理的要求,入侵检测产品的性能要求也逐步提高,出现了千兆入侵检测等产品。但如果入侵检测产品不仅具备攻击分析,同时具备内容恢复和网络审计功能,则其存储系统也很难完全工作在千兆环境下。这种情况下,网络数据分流也是一个很好的解决方案,性价比也较好。这也是国际上较通用的一种作法。

6) 防火墙联动功能

入侵检测系统发现攻击,自动发送给防火墙,防火墙加载动态规则拦截入侵,称为防火墙联动功能。目前此功能还没有到完全实用的阶段,主要是一种概念,随便使用会导致很多问题。目前主要的应用对象是自动传播的攻击,例如 Nimda 等,联动只在这种场合有一定的作用。无限制地使用联动,若未经充分测试,对防火墙的稳定性和网络应用会造成负面影响。但随着入侵检测产品检测准确度的提高,联动功能日益趋向实用化。

思　考　题

(1) 计算机网络有哪些漏洞?

(2) 什么样的网络是安全的? 网络安全的重要性有哪些?

(3) 简述网络安全所涉及的主要技术。

(4) 简述防火墙在网络安全中的地位,它可以分为几种类型?

(5) 典型的防火墙有哪些方面的基本特征?

(6) 防火墙有哪些不足?

(7) 入侵检测技术弥补了防火墙的哪些不足?

(8) 试描述通用的入侵检测系统的基本结构。

(9) 简述基于主机的入侵检测系统的特点。

(10) 简述基于网络的入侵检测系统的优缺点。

(11) 根据检测原理入侵检测系统可以分为几种? 它们的原理分别是什么?

(12) 简述入侵检测技术的发展方向。

参 考 文 献

[1] 袁艺,张晓燕,卫红. 网络战在平时悄然打响. 保密工作,2010,(10): 52～54.

[2] 柯科峰,邵世煌. 企业入侵检测系统的研究与实现. 计算机应用研究,2004,(1): 154～158.

[3] 周秋霞,梁启文.校园网络入侵检测系统的设计与实现.重庆工学院学报(自然科学版),2007,(12):58～60.
[4] 宿洁,袁军鹏.防火墙技术及其进展.计算机工程与应用,2004,(9):147.
[5] 刘学波,孟丽荣.高速网络环境下的入侵检测系统的研究.计算机工程与设计,2005,(5):6～38.
[6] 潘永刚.浅谈入侵检测系统的应用与趋势.鄂州大学学报,2008,(52):25～27.
[7] 孙雷.入侵检测系统在计算机网络安全上的应用.应用能源技术,2009,(8):45～46.
[8] 张国华,肖频.一种基于网络的入侵检测系统设计.微计算机信息,2009,(2):70～72.
[9] 王文奇,郑秋生,吴婷.高速入侵检测研究.计算机工程与设计,2008,(14):3616～3620.
[10] 宋劲松.网络入侵检测——分析、发现报告攻击.北京:国防工业出版社,2004.
[11] 杨琼,杨建华,王习平,马斌.基于防火墙与入侵检测互动技术的系统设计.武汉理工大学学报,2005,(7):113～115.
[12] 曹天杰.计算机系统安全.北京:高等教育出版社,2003.
[13] 朱林平,万郡.浅谈入侵检测系统.计算机与现代化,2006,(12):121～123.
[14] Pacek TH,Newsham TN. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. Se2cureNetworks,Inc,January,1998.
[15] 丁志芳,徐孟春,汪淼,殷石仓.关于入侵检测系统与入侵防御系统的探讨.光盘技术,2006,(1):21～23.
[16] Stephen Northcutt.网络入侵检测分析员手册.北京:人民邮电出版社,2000.
[17] 张丽红,赵俊忠.计算机网络入侵检测系统发展趋势.计算机测量与控制,2004,(4):301～305.
[18] 杜彦辉.利用蜜罐技术实现对互联网非法活动进行监控.中国人民公安大学 47 参考文献学报(自然科学版),2007,(4):48～50.
[19] 樊雷.校园网入侵检测系统的研究和设计.福建电脑,2008,5:117～118.
[20] Julia Allen,Alan Christie,William Fithen. State of the Practice of Intrusion Detection Technologies. Networked Systems Survivability Program,2000.
[21] John Chrirllo. Hack Attacks Revealed. America Copyright China Machine Press,2003.
[22] 祝晓光.网络安全设备与技术.北京:清华大学出版社,2004.
[23] 汪静,王能.入侵检测系统设计方案的改进.计算机应用研究,2004,(7):208～210.
[24] 王永波,梅波.浅谈计算机网络入侵检测系统.黑龙江科技信息,2008,(12):95～97.