Snort
轻量级入侵检测系统
全攻略

陈 伟 周继军 许德武 编著

SNORT
QINGLIANGJI RUQIN
JIANCE XITONG
QUANGONGLUE

北京邮电大学出版社
www.buptpress.com

Snort 轻量级入侵检测系统全攻略

陈　伟　周继军　许德武　编著

北京邮电大学出版社
·北京·

内 容 简 介

全书共 11 章，主要内容包括四个方面，较为全面地介绍了 Snort 入侵检测系统的安装部署、配置、调整及使用，基本涵盖了 Snort 有关的方方面面。

本书的特点是实用性非常强，概念准确、实例丰富，能够培养读者建立一套实用 IDS 的实际动手能力。另外，本书深入到 Snort 的具体技术细节中，是一本不可多得的全面掌握 Snort 的技术图书。

本书面向的对象为具有基本网络技术知识的读者，即使读者以前从未接触过 IDS，书中穿插的实例也能帮助读者成为 IDS 高手。对于资深网管，本书能提供一种性价比高的安全解决方案。同时，对于已学习过网络课程的大中专在校生，本书也可作为入侵检测或信息安全课程的授课辅助材料。

图书在版编目(CIP)数据

Snort 轻量级入侵检测系统全攻略/陈伟，周继军，许德武编著．—北京：北京邮电大学出版社，2009
ISBN 978-7-5635-1966-8

Ⅰ．S… Ⅱ．①陈…②周…③许… 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(2009)第 063248 号

书　　名：Snort 轻量级入侵检测系统全攻略
作　　者：陈　伟　周继军　许德武
责任编辑：李欣一
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：62282185　传真：62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京忠信诚胶印厂
开　　本：787 mm×1 092 mm　1/16
印　　张：20.5
字　　数：509 千字
印　　数：1—3 000 册
版　　次：2009 年 7 月第 1 版　2009 年 7 月第 1 次印刷

ISBN 978-7-5635-1966-8　　定　价：39.00 元

前　言

随着互联网的飞速发展，攻击和入侵等安全问题与日俱增，给很多网络管理员带来了巨大的压力。考虑到网络数据的巨大价值，安全业务已持续成为各大公司和研究机构关注的重点。

面对这些挑战，国内外很多公司近年来相继开发出了各种专用入侵检测系统（IDS，Intrusion Detection System），其价值动辄数万元甚至数十万元人民币。厂商的宣传往往让用户眼花缭乱，在面对形形色色价格昂贵的商用产品时难以适从。大部分技术人员往往更关心如何判断产品的好坏，如何在网络中部署IDS，如何在使用中配置和调试IDS等问题，而这些从厂商的宣传材料中是得不到的。

其实，人们还有更好的选择，这就是著名的骨灰级开源IDS软件系统——Snort。它在业内的重要地位可称“一直被模仿，从未被超越”，在国内的安全行业甚至成为IDS系统的代名词，其规则语法更成为了事实上的业界标准。

Snort设计简洁，功能强大，无论对小的家庭用户还是繁忙的公司网络，它都有能力实时分析和记录通信流，其基于规则的检测引擎能够检测多种变种攻击。Snort几乎能兼容所有硬件平台和操作系统，并提供丰富的报警记录信息以供选择。它还能帮助用户确定网络中一些莫名其妙的服务的作用，其可扩展的体系结构和开源模式更使得用户群不断增长。

上述优点来自Snort开发小组的紧密努力：构造一个卓越的IDS系统内核。“量身订做”的特性是如此灵活，以至于新手们往往无所适从。对此，全世界的程序员们围绕着Snort开发了大量适用于各种需求和各种应用环境的应用程序、工具和脚本，极大地降低了Snort配置使用所要求的技术门槛。因此，管理员们所需做的不是强忍不适磕磕绊绊地使用Snort，而是发现Snort的奇妙之处，找到称手的Snort应用工具，将它们和Snort内核DIY成一款强大的IDS。

本书致力于带领读者由浅入深循序渐进地进入Snort这个奇妙的世界，一

砖一瓦地教会读者如何搭建自己的互联网城堡。本书面向的对象为具有基本网络技术知识的读者，即使读者以前从未接触过IDS，书中穿插的实例也能带领您成为IDS高手。当然，如果您是一位资深网管，正在为自己的网络寻找一种性价比高的安全解决方案，相信本书将会是通往它的捷径。同时，对于已学习过网络课程的大中专在校生，本书也可作为入侵检测课程的专业教材或信息安全课程的授课辅助材料。

全书共11章，主要内容包括四个方面。

第1章和第2章是理论基础。第1章介绍了入侵检测系统的基本概念，重要的是澄清了人们对于漏报和误报可能存在的一些日常错误观念，并阐述了IDS在网络中的部署问题，第2章对于有关Snort的原理性知识、优缺点、工作流程和内部组件作了概要介绍。所谓“兵马未动，粮草先行”，在动手部署系统之前，首先我们需要具备一些最基本的指引，因此，第2章后半部分详细说明了如何从自己的网络结构和安全策略出发制定系统部署方案，对小型网络到大中型网络结构中如何一步步部署Snort系统作了深入剖析。即使您对IDS已非常熟悉，仍建议仔细阅读该部分。

在读者已经具备了IDS和Snort的基本知识后，第3章和第4章带领读者进入系统部署实施阶段，这部分内容主要介绍在集成式和分离式两种部署策略下，如何在Windows和Linux平台上部署Snort IDS。

安装好Snort系统后，我们就该学习如何使用了。第5章到第9章的内容涉及系统调整、测试和使用，包括命令行参数介绍、规则、预处理器和数据分析工具等方面，其中，第5章具有总括性地位。Snort在分析和定位恶意的网络流量方面功能强大的秘诀就在于它能让使用者完全定制自己的规则，并按照自己的意愿调整预处理器设置，前提是使用者拥有关于Snort规则和预处理器的相关知识。这一点上本书能提供较为全面的帮助。

第10章涉及Snort升级维护和IDS评测标准等方面，这些内容可供想要进一步了解Snort系统的读者参考。

第11章给出了几个Snort的使用实例，以供参考。

计算机是一门年轻的学科，知识更新很快。而网络安全在计算机领域内的知识更新程度又是最快的。本书总结了作者多年来在使用Snort方面积累的大量经验教训，同时也参考了国内外众多Snort方面的权威书籍和大量的网络资源，网络资源未能一一列出，敬请原谅。书内一些章节附有一些重要网络资源和参考资料的说明。读者可以通过查阅网址得到进一步帮助。

本书只是提供一个 Snort 轻量级入侵检测系统的指引，如果您面对的是大型主干网的话，本书能起到一定辅助作用，帮助读者科学地决策，避免一味追求高端产品。同时我们需要强调的就是，对于需要高性能 IDS 的大型主干网，或者追求 IPS 甚或 IRS 的用户，付出更多成本是必需的。

在此，我们对书中参考的各类资料的作者表示衷心感谢。在本书的撰写过程中，胡星、肖志文、谭文元等研究生付出了很大的努力，另外，中国人民解放军信息工程大学通信工程系通信与信息系统专业的硕士研究生王颖同志在攻读硕士学位期间也为此书的撰写洒下了许多汗水，在此对他们的辛勤劳动表示感谢。特别要感谢的是中国民航信息网络股份有限公司网络部的蔡毅同志，他为本书提供了很多实践指导。

由于时间仓促，加上我们水平有限，书中难免还存在一些缺点甚至错误，恳请广大读者和专家批评指正。读者在本书及课件等相关资源的使用中遇到任何问题或有何建议，请发邮件至：cyberella2000@163.com。欢迎读者与我们进行交流，帮助我们提高质量。

作　者

第1章 DIYIZHANG

入侵检测基础概念

1.1 入侵检测系统的作用

谈到网络安全，人们首先想到的就是防火墙。入侵检测系统(Intrusion Detection System，IDS)相当于防火墙之后的第二道安全闸门。如果说防火墙相当于门卫的话，入侵检测就相当于内部监控系统。入侵检测由传感器和管理员控制台组成，前者相当于密布各个关键处的摄像头，而后者就相当于一排排监视画面，管理员则是端坐于监视画面之前的安保人员。显然，一个只设置了门卫的机构，其安全保卫工作基本是不可靠的。

IDS广泛采用了与反病毒软件查杀病毒相类似的机制。所不同的是，杀毒软件分析的是文件内容，而IDS则通过分析数据包内容，检测来自网络的未经许可的访问、资源请求等可疑活动，从已知的攻击类型中发现是否有人正在试图攻击网络或者主机，并成功捕获攻击。利用入侵监测系统收集的信息，网管或者安全管理人员能够采取有效措施加固自己的系统，从而避免造成更多损失。除了检测攻击外，IDS还能记录下网络入侵者的罪证，以便采取进一步的法律措施。这些可以通过执行以下任务实现：

- 监视、分析用户和系统活动；
- 审计系统的配置和弱点；
- 识别已知进攻模式；
- 异常活动的统计分析；
- 评估关键系统和数据文件的完整性；
- 对操作系统和其他应用程序的日志进行审计，识别用户违反安全策略的行为；
- 实时报警和主动响应。

与防火墙类似，市场上的IDS同时存在硬件系统、软件系统或二者结合的产品。一般，IDS软件与防火墙、代理服务或其他边界服务可以运行于同一台硬件设备或服务器。

1.2 IDS的标准结构

根据目前国际通行的方法，可以将IDS的内部结构分为如下几个部分：事件产生器(Event Generators)、事件分析器(Event Analyzers)、响应单元(Response Units)和事件数据库(Event Databases)。

事件产生器又称为传感器，是入侵检测的第一步，它的目的是从整个网络环境中采集数据，并提供给系统的其他部分。采集内容可能包括：系统日志、应用程序日志、系统调用、网络数据、用户行为和其他IDS的信息。从技术上来说，传感器实际就是一个嗅探器(Sniffer)。

事件分析器分析得到的数据，并产生分析结果。它是整个IDS的核心，效率高低直接决定整个IDS性能。

响应单元则是对分析结果作出反应的功能单元，功能包括：

- 报警和事件报告；
- 终止进程，强制用户退出；
- 切断网络连接，修改防火墙设置；
- 灾难评估，自动恢复；
- 查找定位攻击者。

事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。通常，规则库、行为模式库等也归于此。

此外，一套完整的IDS还应包括管理器，它负责定位、控制等常规的管理功能，包括管理员控制台和日志输出模块。管理员控制台可以采用命令行或Web方式。

1.3 如何检测入侵

要判定是否发生了入侵，首要的是依据。IDS判定入侵的依据从何而来？这就涉及检测技术的问题。IDS检测技术基本可以分为两大类：基于特征(规则)的入侵检测和基于异常的入侵检测。

现有的攻击大多数是针对网络的攻击，因此捕获和分析数据包已成为检测入侵和攻击的最主要方法，现有的入侵检测方法多数是针对网络数据包的。入侵者所发出的网络数据包常具有用软件可以检测到的特征。例如，如果截获数据包中包含一段明文“GET /script/root.exe”就表明出现了尼姆达蠕虫的特征。IDS系统包含一系列已知入侵行为特征的规则集。正基于此，入侵检测系统才能发现可疑行为。这类简单的字符串匹配技术虽然古老但却快速有效，一直被IDS和反病毒软件使用。每当IDS匹配到一条入侵规则时，都会触发一条警报。当然，为提高准确率，避免受骗，IDS还需在特征比对之前对数据包进行一些预处理。

检测已经成为所有IDS的通用技术，这一点和反病毒软件一样。大部分恶意流量都能被唯一的一种特征所鉴别。当然，它也存在一定的局限性。一方面，特征检测仅仅是机械地匹配字符串，因此有时即使是正常流量也可能触发警报。这往往导致误报，也就是没有入侵

误以为有，称之为第一类错误。另一方面，字符串匹配的智能化程度极低。有时候，仅仅修改一个比特就能避开 IDS 的检测。对于一些明显反常的行为，例如多次错误登录、午夜登录、异地登录等，因为没有可供匹配的特征串，特征检测无法识别这类异常，对于未知攻击更是如此。这些都会导致漏报，也就是有入侵误以为没有，称之为第二类错误。

检测的另一个问题是，随着特征库的增长，IDS 内核负担越来越沉重，而随着网络带宽的增长，计算代价也越来越大。一旦带宽超出 IDS 承受力，随着丢包的产生，漏报就会变得很严重。

虽然有上述缺点，但是因其技术简单、可靠性高，特征检测 IDS 还是性能最突出、最可靠的。

基于异常的入侵检测不使用入侵特征库，而是通过识别出“异常”行为来进行检测。它需要预先定义什么是“正常”，一些 IDS 允许用户定义一个正常行为的基准(Baseline)，例如登录时间、登录地点、击键频次等，然后它可以用采样统计、神经网络等方法构造“用户正常行为基准”。异常检测 IDS 从用户的系统行为中收集一组数据，检查其是否偏离该基准。异常检测这种方式有时要比特征检测系统更好一些。特别是检测未知入侵时，异常 IDS 系统往往更管用，而特征 IDS 系统则完全无用。关于这一点，只要想一想依靠升级病毒特征码来识别病毒的杀毒软件在来势汹汹的新病毒前束手无策的情况便一目了然。

显然，异常检测可以检测提升权限攻击。如果一个正常用户无权访问某一重要系统文件，但该用户却可以随意访问该文件，异常检测就能及时发现。异常检测的不利之处也很多。它需要使用复杂的算法，计算代价比简单的字符串匹配大得多，这也就意味着它比特征检测更容易丢包和漏报。如果一种异常行为发生在 IDS 收集用户正常行为建模时，IDS 就会将它当成正常，不会发出警报；相反，一些没有被收集到正常行为基准中的非恶意流量反而会产生警报。一个类似的例子是，很多人都有这样的经验，如果平时只在家中登录 QQ，偶尔旅行时在外地登录 QQ 就会触发 QQ 软件的“异常登录”提示。

特征检测和异常检测的关系可以用图 1-1 作一类比。图中左侧纯黑色区域代表已知正常，黑色箭头代表 IDS 判定的正常，右侧灰色区域代表已知入侵，较粗箭头代表 IDS 判定的入侵，中间区域为未知地带。特征检测长于发现已知入侵，准确度极高，短于理解未知，所以会将一部分没有特征串的攻击当成正常，错误主要体现在漏报率上；异常检测则试图发现未知入侵行为，会将一些正常用户行为当成入侵，特别是在一些用户较多或工作行为经常改变的环境中，误报率较高。

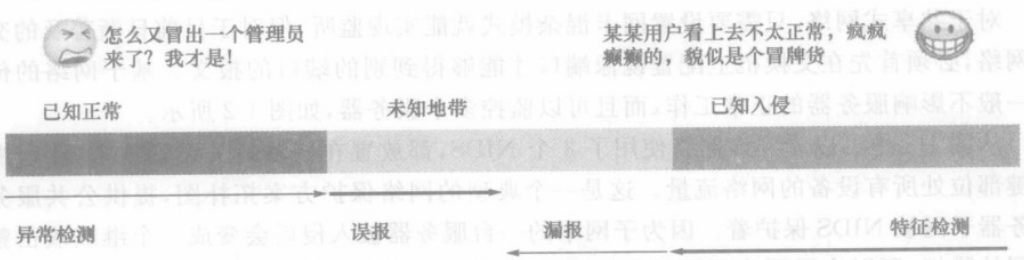

图 1-1 特征检测和异常检测的关系

需要提醒读者特别注意的是，虽然误报和漏报互为反面，但它们在 IDS 性能中所处的地位是不一样的。误报只是一些虚假警报，令人心烦却还不致命，漏报则性质完全不同。漏

报标志发生了IDS没有察觉的入侵，目前还没有好的办法检测，只有当系统产生了实质损害后才能察觉，而这就意味着IDS的彻底失败。因此，IDS应当产生一定量的误报。如果IDS不产生误报，就必然有漏报。一套迟钝而麻木的IDS就失去了其存在的意义。所以，很多IDS产品都会在测试出厂参数时故意将误报与漏报的比例最大化，留待用户逐步调谐至最佳状态。虽然通过调整，IDS可以将误报降低到可接受的水平，但是最佳状态并非是零误报，出于谨慎的考虑，最好还是保持一些误报。

当IDS检测到入侵者，它将用报警来通知安全管理员。报警的形式可以是弹出窗口、终端显示及发送电子邮件等。报警同时也以日志信息的形式存储到日志文件或者数据库中，以供安全专家查看。

1.4 IDS的分类

IDS系统的分类标准很多。解释这些分类标准有助于我们根据自己的需要选择合适的IDS系统。

大多数的入侵检测系统都可以被归入到基于网络、基于主机和分布式3类。根据IDS工作的特点，我们可以看出IDS是分布式的结构。以监控系统作比喻，装在各个地方的摄像头称为“传感器”，作用是收集信息并分析，发现异常。根据安装位置的不同，传感器可以分为基于主机的和基于网络的。基于主机的传感器安装在被监控的服务器上，通过收集服务器的信息来进行分析报警。基于网络的传感器安装在被监控的服务器的同一个集线器或交换机上，通过监听网络上到达服务器的报文来分析报警。基于主机的传感器就像装在各个房间的摄像头，基于网络的传感器就像装在各个走廊的摄像头。两个位置不同，互为补充。

1.4.1 NIDS

顾名思义，NIDS是站在整个网络高度的IDS。正常情况下，计算机网卡工作在非混杂模式，只有数据包的目的地址是网卡的MAC(Media Access Control)地址时，网卡才会接收该数据包并处理。在混杂模式中，网卡接收所有流经本机的数据包，不论其最终接收地址是什么。在混杂模式下，NIDS可以监视不流向自己的MAC地址的网络流量。这部分的技术原理和Sniffer完全相同。

对于共享式网络，只需要设置网卡混杂模式就能实现监听，但对于目前日渐普及的交换式网络，必须首先在交换机上配置镜像端口才能够得到别的端口的报文。基于网络的传感器一般不影响服务器的正常工作，而且可以监控多个服务器，如图1-2所示。

从图1-2中可以看到该网络使用了3个NIDS，都放置在网络最关键的地方，能监视到关键部位处所有设备的网络流量。这是一个典型的网络保护方案拓扑图，提供公共服务的服务器子网被NIDS保护着。因为子网中的一台服务器被入侵后会变成一个继续攻击整个子网的跳板，所以为了预防更深层次的危险，必须监视整个子网。

内网中的主机被其他的NIDS保护着，这样可以减少内网主机被入侵的危险，在网络中布置多个NIDS是深层安全防护的一个很好例子。

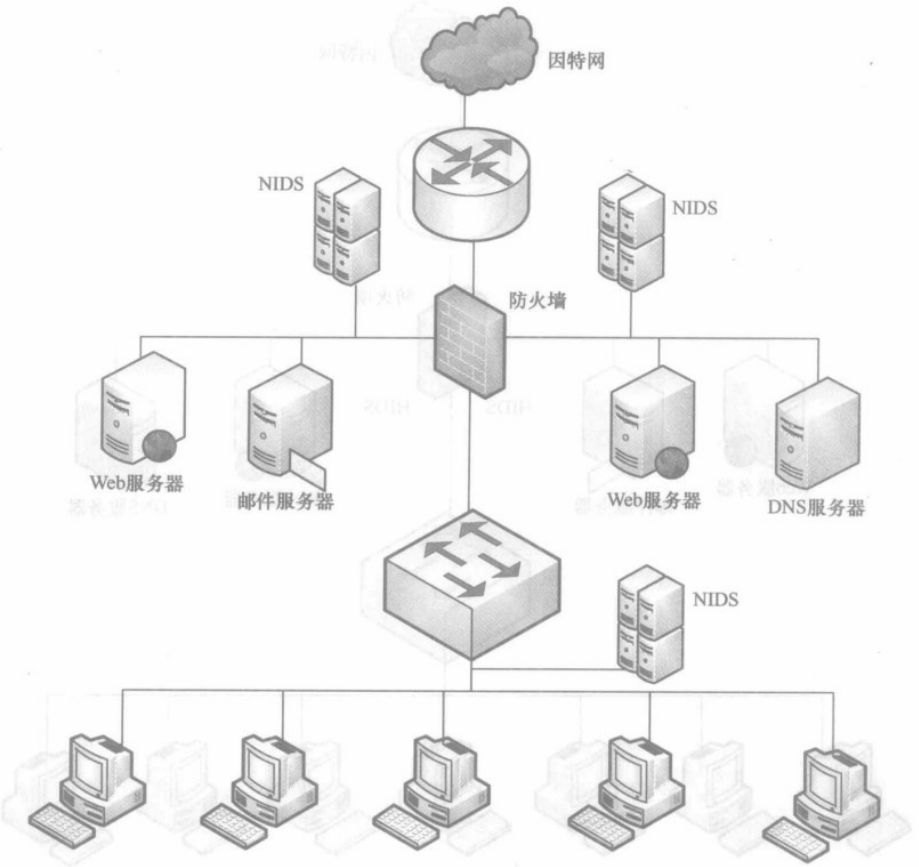

图 1-2　NIDS 网络

1.4.2　HIDS

HIDS 和 NIDS 有两点不同：HIDS 只能保护它所在的计算机，计算机网卡设置的是“非混杂模式”，不像 NIDS 需要将网卡设置为混杂模式，在 HIDS 中，网卡只在正常的“非混杂模式”下工作，因为不是所有的网卡都能设置成混杂模式的。另外，对配置低的计算机来说，混杂模式对 CPU 的占用会很明显地体现出来。

HIDS 的另一个好处是可以精确地根据自己的需要定制规则。例如，如果运行 HIDS 的计算机上没有运行域名服务(DNS)，就不需要加上那些检测 DNS 攻击的规则集。减少了不相关的规则可以提高检测效率和降低处理器的负荷。

图 1-3 描述了一个在一些服务器和个人计算机上安装了 HIDS 的网络。如前所述，安装在邮件服务器上的 HIDS 主要设置和邮件服务器相关的规则，使其免受入侵，而安装在 Web 服务器上的 IDS 主要设置和 Web 服务相关的规则，检测对 Web 服务器的攻击。在安装的时候，零散的计算机可以使用常用的规则集，当有新的漏洞公布后，规则要及时和定期地更新以检测新漏洞。

基于主机的传感器收集的信息准确，但是占用服务器资源，尤其在繁忙的服务器上会降低服务器性能。而且，基于主机的传感器是与操作系统相关的，如果使用了 IDS 产品不支持的操作系统就不能安装 HIDS。

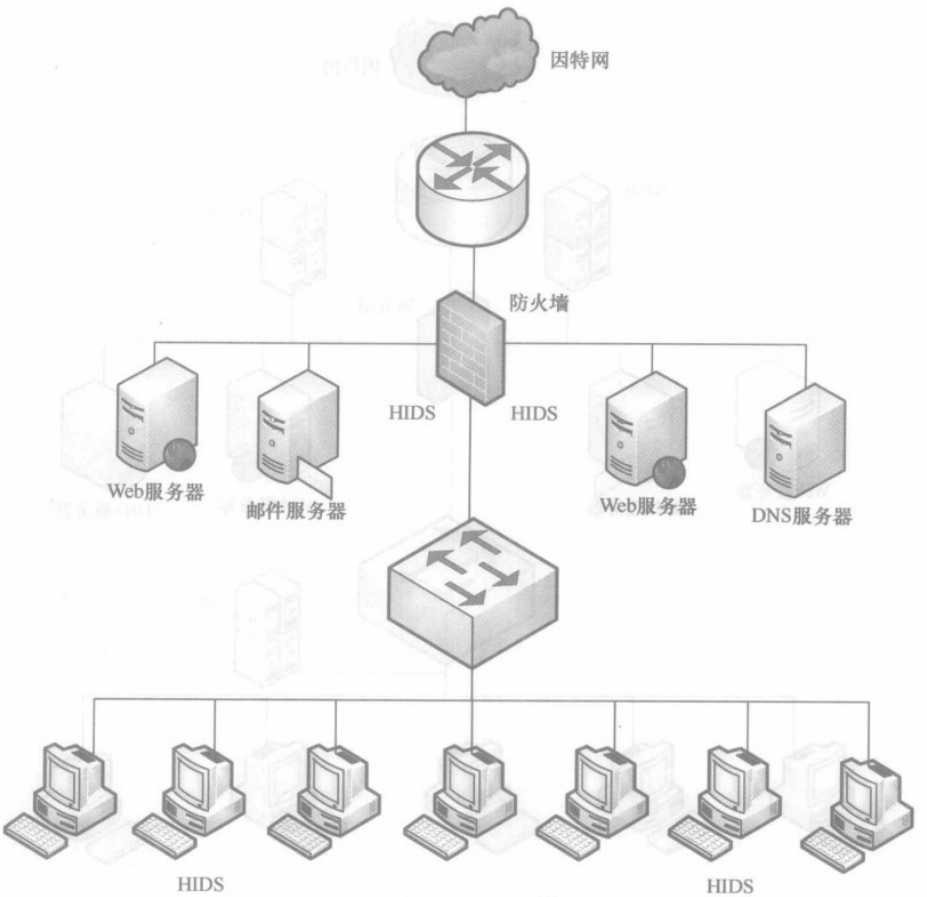

图 1-3　HIDS 网络

1.4.3　DIDS

典型的 DIDS 是管理端/传感器结构。NIDS 作为传感器放置在网络的各个地方，并向中央管理平台汇报情况。攻击日志定时地传送到管理平台并保存在中央数据库中，新的攻击特征库能发送到各个传感器上。每个传感器能根据所在网络的实际需要配置不同的规则集。报警信息能发到管理平台的消息系统，用各种方式通知 IDS 管理员。

在图 1-4 中，我们可以看到 DIDS 包含了 4 个传感器和 1 个中央管理平台。传感器 1 和传感器 2 工作在隐蔽的混杂模式，保护提供公共服务的服务器。传感器 3 和传感器 4 在可信任的网络区域中保护里面的计算机。

传感器和管理端之间的网络传输可以在搭建的专用网络中进行，也可以使用现有的网络结构。当使用现有的网络结构管理数据时，强烈建议使用 VPN、加密等方式保障数据传输的安全。

对 DIDS 来说，不同厂商的产品的功能和特性差别很大，因此要对 DIDS 做一个准确的定义很困难。在 DIDS 中，传感器可以使用 NIDS、HIDS，或两者都用。传感器有的工作在混杂模式，有的工作在非混杂模式，然而，无论在什么情况下，DIDS 都有一个显著的特征，

即分布在网络不同位置的传感器都向中央管理平台传送报警和日志信息。

目前，NIDS 和 HIDS 结合，异常和特征 IDS 结合，IDS 和防火墙结合是一种趋势。

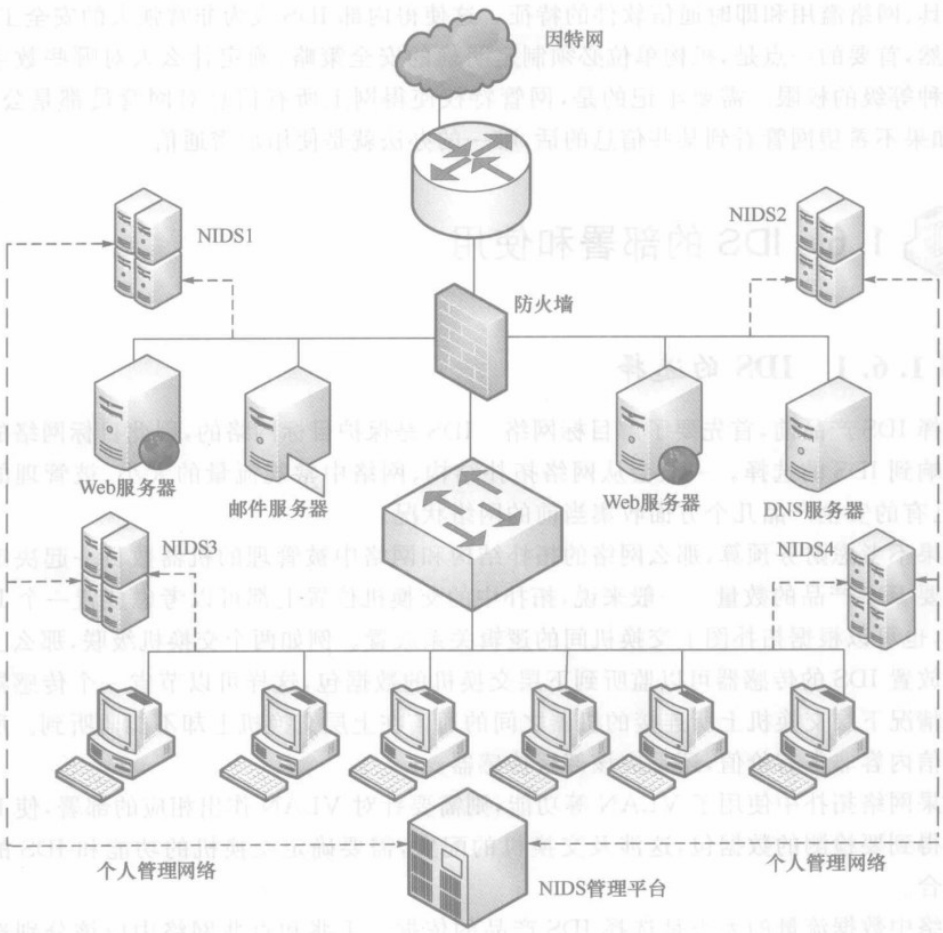

图 1-4　DIDS 网络

1.5　攻击的来源

一般来说，安全威胁通常来自两个方向：外部和内部。

很多组织和个人觉得自己的地位并不那么重要，不会吸引黑客注意，计算机中的数据也并无太大保护价值，因此对保护系统采取无所谓的态度。实际上，入侵和病毒一样，常常并不针对具体而特定的目标展开，而是漫无目标地扫描因特网，寻找那些有漏洞的机器。黑客的目的可能是学习入侵技术、测试入侵代码或寻找攻击跳板。因此，在网络安全问题上，个人计算机未必就比公司网络更安稳。

据统计，80％单位防御的重点都是外向型的。确实，大部分攻击尝试来自外部，而且都以失败告终。但常言道“堡垒最容易从内部攻破”，大部分成功的攻击却来自内部。内部攻

击破坏性很强而且难以发现。尤其在今天，NAT、P2P、防火墙穿透技术已经让防火墙安全性受到考验，大部分内网用户可能压根没有想到他们的日常行为会产生内网安全漏洞。此时，部署于内网的 IDS 能检测出内部攻击和违反公司规定的访问行为。它能检测出大部分 P2P 工具、网络滥用和即时通信软件的特征。这使得内部 IDS 成为非常强大的安全工具。

当然，首要的一点是，机构单位必须制定明确的安全策略，确定什么人对哪些数字资源拥有何种等级的权限。需要牢记的是，网管特权使得网上所有信息对网管员都是公开的。所以，如果不希望网管看到某些信息的话，唯一的办法就是使用加密通信。

1.6 IDS 的部署和使用

1.6.1 IDS 的选择

选择 IDS 产品前，首先要了解目标网络。IDS 是保护目标网络的，因此目标网络的情况直接影响到 IDS 的选择。一般会从网络拓扑结构、网络中常规流量的大小、被管理的机器数目、已有的安全产品几个方面收集当前的网络状况。

如果不考虑财务预算，那么网络的拓扑结构和网络中被管理的机器数目一起决定了网络中需要 IDS 产品的数量。一般来说，拓扑中的交换机位置上都可以考虑放置一个 IDS 的传感器，也可以根据拓扑图上交换机间的逻辑关系放置。例如两个交换机级联，那么上层交换机上放置 IDS 的传感器可以监听到下层交换机的数据包，这样可以节省一个传感器。但是这种情况下层交换机上所连接的机器之间的通信在上层交换机上却不能监听到。所以如果该通信内容非常有价值，还是应该部署传感器。

如果网络拓扑中使用了 VLAN 等功能，则需要针对 VLAN 作出相应的部署，使 IDS 传感器能得到要检测的数据包，这涉及交换机的配置，需要确定交换机的功能和 IDS 的功能是否配合。

网络中数据流量的大小是选择 IDS 产品的依据。千兆和百兆网络中应该分别选择千兆和百兆的 IDS 产品。现在主流的产品在百兆上基本都分成高端和低端两大类。两类产品的区别主要在于抓包方式：低端 IDS 产品使用 Libpcap 函数库抓包，高端 IDS 产品使用零复制等方式把数据包从网卡快速送到检测引擎。

网络流量其实比人们想象的要小得多。如果网络中有提供网络服务的服务器，那么流量很大，常见的大企业的中心机房百兆网络的流量平均在 20～30 Mbit/s。如果是办公网络，流量平均只有几十至几百千比特。因此可以根据网络流量的实际情况，为不同位置配置不同档次的 IDS 传感器，节约开支。

作为网络安全解决方案中的一环，IDS 的存在价值更多地体现在能否融入到网络安全解决方案中去，而不是作为单独的安全产品发挥作用。这种系统整合需求主要体现在两个方面：产品间的联动；可管理性和报警日志的综合分析。

提到联动，很多人会被这种方便的功能所吸引，而了解 IDS 技术现状的人考虑更多的是 IDS 的误报率过高，会因为联动引起正常的网络连接被屏蔽。其实联动还是能发挥很大作用的，最明显的例子就是对病毒爆发的抑制。现在像冲击波这样的病毒，对本机的危害还

在其次，最令管理员头疼的是大量的垃圾数据包阻塞了网络，影响到所有人，而管理员查找感染病毒的机器非常麻烦，速度也慢，结果是遭到抱怨。如果管理员把冲击波病毒这样的攻击联动，则中招的机器会被防火墙屏蔽，不能上网，而其他人可以正常使用网络。中招的机器病毒杀干净了才能重新上网。下面列出的是在选择入侵检测系统时最经常考虑的因素：

- 实时性；
- 与其他安全产品联动，自动反应能力；
- 能检测所有事件，不会发生漏报警；
- 能适应多种操作系统平台。

此外，管理员控制台的好坏也是一个关键因素。一些单位虽然采购了IDS，但是因为管理员控制台不好用，所以虽然IDS还连着网，但是形同废弃。人们总是在使用几个月后，才发现所需要的IDS应提供何种特点：

- 能提供报警优先级供管理员选择的快速控制台；
- 良好的误报警管理：对报警不仅显示常规信息，还提示相关附加信息，以供管理员快速判别；
- 标志已被分析过的事件；
- 层层探究的能力：管理员通过控制台就能够深入探究触发报警的数据包头以及相关连接；
- 提供好的报告：有两类报告，即事件检测报告和日/周/月度总结报告。IDS收集信息产生报告所耗费的时间和报告的详细程度是重要的性能指标。

1.6.2 IDS的部署

1. 部署原则

关于IDS的部署原则，现在各种解决方案中标准的做法是把传感器放在能监听需要监视的网络对象的地方，通常每个交换机上放一个。最简单的是在网关处的交换机上放一个，但如果希望有的放矢地考虑传感器应该放置的位置，则要确定网络拓扑中安全保护的重点，然后根据希望保护的程度部署传感器。

确定安全重点主要基于两点考虑：控制不同的访问者对网络和设备的访问，划分并隔离不同的安全域；防止内部访问者对无权访问区域的访问和误操作。根据以上考虑，可以按照网络区域安全级别把网络划分成两大安全区域，即关键服务器区域和外部接入网络区域。

对IDS的部署，唯一的要求是IDS应当挂接在所有关键流量都必须流经的链路上。关键流量的定义是所有可能对网络、主机造成损害的流量。包括：

- 所有从外网进入内网的流量；
- 所有访问核心服务器区域的流量。

因此，IDS在交换式网络中的位置一般选择在：

- 尽可能靠近攻击源的地方；
- 尽可能靠近受保护资源的地方。

具体到安放设备，通常选择以下设备：

- 服务器区域的交换机；
- 因特网接入路由器/防火墙之后的第一台交换机；

- 重点保护网段的局域网交换机。

2. 部署环境

目前共享式网络和交换式网络并存，它们部署传感器的方式很不一样，所以有必要在此作一概略介绍。共享式网络上传感器的部署最简单，如图 1-5 所示。

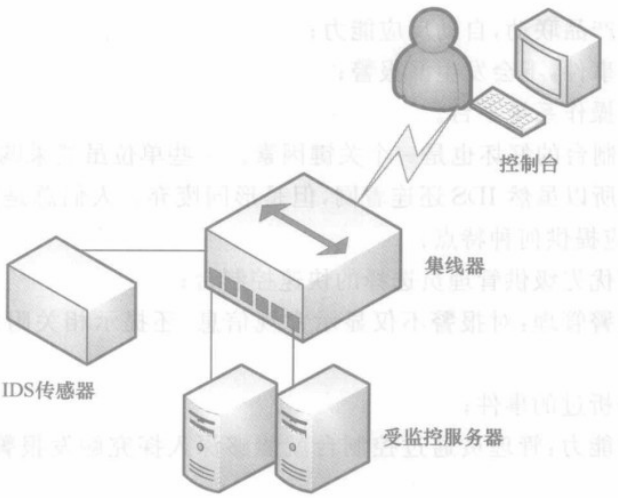

图 1-5　共享式网络的 IDS 部署

而对于交换式网络，IDS 要求交换机设备能够支持端口镜像功能，即将某一到多个端口的流量复制到镜像端口中去，如图 1-6 所示。

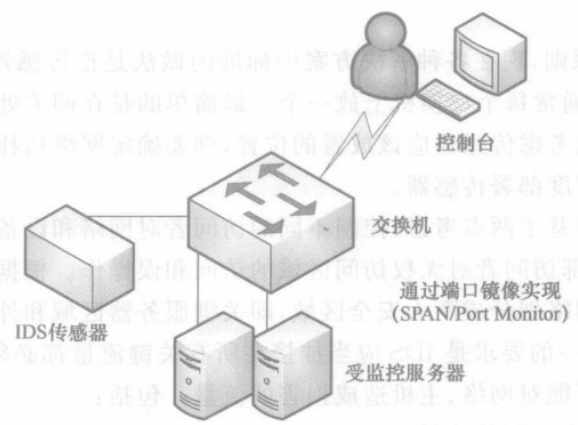

图 1-6　交换式网络的 IDS 部署

对于有些单位来说，也许更愿意采用 IDS 的隐蔽部署，这样做的好处是 IDS 不容易被发觉，对网络的影响小，同时也更不容易受到攻击，如图 1-7 所示。

3. 部署位置

要建造一个安全的企业网络，首先要保证企业网络边界的安全，企业网的边界直接与公网打交道，是企业网络安全的第一道防线。利用防火墙技术，经过仔细的配置，通常能够在内外网之间提供安全的网络保护，降低网络安全风险。但是，仅仅使用防火墙还远远不够，

通过部署IDS，能够发现透过防火墙的攻击，也可以发现防火墙内部的入侵者，并提供实时的入侵检测能力。

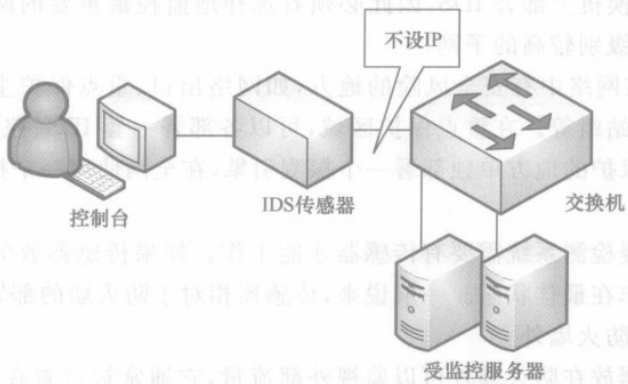

图 1-7　隐蔽模式下 IDS 的部署

IDS的安装位置取决于要探测的入侵行为类型，是检测内部入侵还是外部入侵，或者两个都要检测。例如，如果只想检测外部入侵活动，并且只有一个路由器接到因特网，那么放置IDS的最佳位置就是紧靠着路由器或者防火墙的内部网络接口。如果有多条路接入因特网的接口，也许用户希望在每个入口处放置一台IDS。有时用户也希望能够检测来自内部的威胁，那么可以在每个网段都放置一台IDS。在很多情况下，并不需要在所有网段都实施入侵检测，可以仅仅在敏感区域放置IDS。要知道，越多的IDS就意味着越多的工作量和维护费用。因此IDS的部署要取决于安全策略，也就是想防范什么样的入侵。唯一的要求是IDS应当挂接在所有关键流量都必须流经的链路上。图1-8是一种IDS安装的典型位置，IDS安装在防火墙和路由器后，起到监控子网的作用。

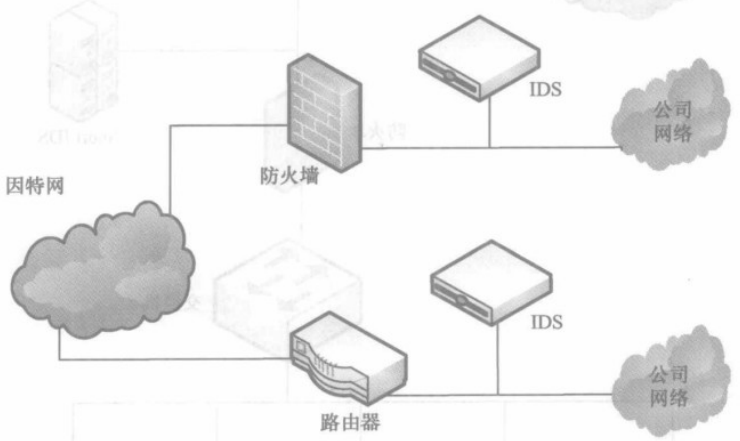

图 1-8　IDS 的一种部署

实际应用中，应该根据网络出口情况、要保护的服务器区域等确定IDS的部署方式，然后根据各IDS的实际物理位置、网络拓扑等选择IDS的管理方式，力争做到管理方便、高效。

(1)IDS部署于安全级别高的子网

关键网络设备、关键服务器区域是用户的业务核心所在，提供业务系统80%以上的功