第3章 入侵检测设备基础知识

随着网络安全风险系数不断提高，曾经作为最主要的安全防范手段的防火墙，已经不能满足人们对网络安全的需求。仅仅使用防火墙来保护网络的安全还远远不够，原因在于：

- 网络的入侵者可寻找防火墙的漏洞；
- 网络的入侵者可能就在防火墙内；
- 由于性能的限制，防火墙通常不能提供实时的入侵检测能力。

作为对防火墙的有益补充，入侵检测系统 IDS 能够帮助网络系统快速发现网络攻击的发生，从而扩展系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。IDS 被认为是防火墙之后的第二道安全闸门，它能在不影响网络性能的情况下，对网络进行监听，从而提供对来自内部攻击、外部攻击和误操作的实时保护。

IDS 这一概念最先由 James P. Anderson 在 1980 年 4 月为美国空军做的一份题为《计算机安全威胁监控与监视》的技术报告中提出。此后，经历 20 余年的发展，IDS 终于发展成熟，发展成为基于网络的 IDS 和基于主机的 IDS 两大阵营，并且随着入侵事件的愈演愈烈而逐渐成为安全市场主角。有人将 IDS 产品比作为继杀毒和防火墙产品之后安全领域的第三战场。前两个战场已处于酣战之中，IDS 领域将成为今后一段时期安全厂商角力的主战场。

3.1 什么是入侵检测系统

IDS 是英文“Intrusion Detection Systems”的缩写，中文意思是“入侵检测系统”。专业上讲就是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。做一个形象的比喻：假如防火墙是一幢大楼的门锁，那么 IDS 就是这幢大楼里的监视系统。一旦小偷爬窗进入大楼或内部人员有越界行为，只有实时监视系统才能发现情况并发出警告，IDS 设备如图 3-1 所示。

通过在网络中安装防火墙，可以阻挡一般性的网络攻击行为，采用 IDS 入侵防护系统，则可以对越过防火墙的攻击行为，以及来自网络内部的违规操作进行监测和响应，相当于为网络提供第二套保护机制。入侵检测系统多安置在防火墙之后，对网络活动进行实时检测。在很多情况下，由于可以记录和禁止网络活动，所以入侵检测系统是防火墙

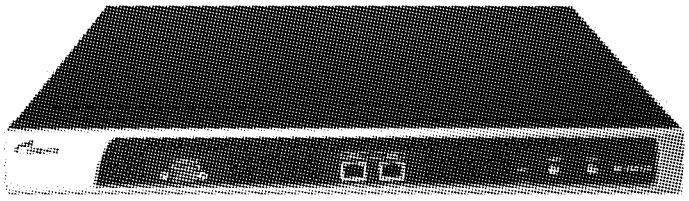

图 3-1　入侵检测系统硬件设备

的延续。它们可以和防火墙以及路由器配合工作。如 IDS 可以通过配置来禁止从防火墙外部进入的恶意流量，独立于防火墙而开展工作的。

入侵检测系统 IDS 与系统扫描器 system scanner 不同。系统扫描器是根据攻击特征数据库来扫描系统漏洞的，它更关注配置上的漏洞而不是当前进出主机的流量。在遭受攻击的主机上，即使正在运行扫描程序，也无法识别这种攻击。IDS 扫描当前网络的活动、监视和记录网络的流量，根据定义好的规则来过滤从主机网卡到网线上的流量，提供实时报警。网络扫描器只检测主机上先前设置的漏洞，而 IDS 监视和记录网络流量。如果在同一台主机上运行 IDS 和扫描器，配置合理的 IDS 会发出许多报警。

不同于防火墙，IDS 入侵检测系统是一个监听设备，没有跨接在任何链路上，无须网络流量流经它便可以工作。因此，对 IDS 的部署，唯一的要求是：IDS 应当挂接在所有所关注流量都必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。在如今的网络拓扑中，已经很难找到以前的 Hub 式的共享介质冲突域的网络，绝大部分的网络区域都已经全面升级到交换式的网络结构。因此，IDS 在交换式网络中的位置一般选择为：(1)尽可能靠近攻击源；(2)尽可能靠近受保护资源。

这些位置通常是：在服务器区域交换机上，或者在 Internet 接入路由器之后第一台交换机上，或者在重点保护网段局域网交换机上，经典的入侵检测系统部署方式如图 3-2 所示。

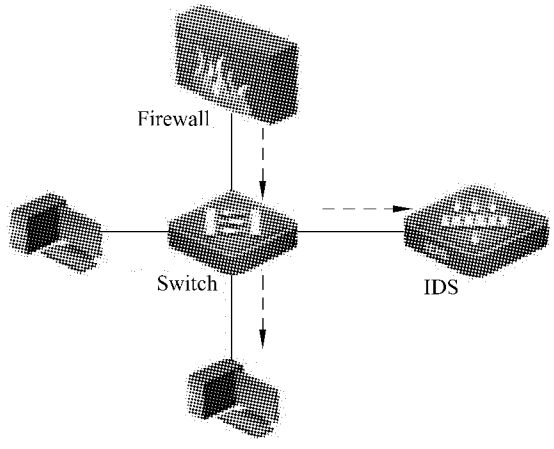

图 3-2　IDS 的部署网络拓扑图

3.2 入侵检测系统功能

大多数的入侵检测系统 IDS 可以提供关于网络流量非常详尽的分析，它们可以监视任何定义好的流量，如对 FTP、HTTP 和 Telnet 流量都有默认的设置，对其他的流量如 NetBus、本地和远程登录等，可以自己定制策略。

常见的入侵检测系统检测功能如下：

1. 网络流量管理

大多数的入侵检测系统 IDS 允许记录、报告和禁止几乎所有形式的网络访问。还可以用它监视某一台主机上通过的所有网络流量。如定义了策略和规则，在设备上获得 FTP、SMTP、Telnet 和任何其他的流量，这种策略和规则有助于追查该连接和确定网络上发生过什么，或现在正在发生什么。这在需要确定网络中策略实施的一致性时是非常有效的工具。

虽然入侵检测系统 IDS 是网络中安全管理人员或审计人员非常有价值的工具，但公司内网中的用户同样可以安装像 eTrust Intrusion Detection 或 Intrude Alert 这样的程序来访问重要的信息。攻击者不仅可以读取未加密的邮件，还可以嗅探密码和收集重要的协议方面的信息。所以实施整网安全工作还要检查在网络中是否有类似的程序在运行。

2. 系统扫描

入侵检测系统 IDS 设备可以在网络中对不同的应用实施控制，从操作系统到扫描器、IDS 程序和防火墙。许多安全专家将这些应用和 IDS 结合起来。

3. 追踪

入侵检测系统 IDS 设备所能做的不仅仅是记录安全事件，它还可以确定安全事件发生的位置。通过追踪来源，可以更多地了解攻击者。IDS 检测设备记录下的日志不仅可以记录攻击过程，同时也有助于确定解决方案。

3.3 入侵检测系统工作原理

早期的 IDS 设备仅仅是一个监听系统，IDS 可以将位于与 IDS 连接在同一网络中的交换机/Hub 和服务器的访问、操作全部记录下来以供分析使用。跟常用的 Windows 操作系统的事件查看器类似，本质上入侵检测系统 IDS 是一个典型的“窥探设备”，它不跨接多个物理网段（通常只有一个监听端口），无须转发任何流量，只在网络上被动地、无声息地收集它所关心的报文，如图 3-3 所示。

IDS 就像交通灯、摄像头一样，对攻击者常规的入侵行为做很好的监测，对网络安全有一定的保护作用。入侵检测系统具有的作用主要表现在以下几方面：

- 通过检测和记录网络中的安全违规行为，防止网络入侵事件的发生；
- 检测其他安全措施未能阻止的攻击或安全违规行为；

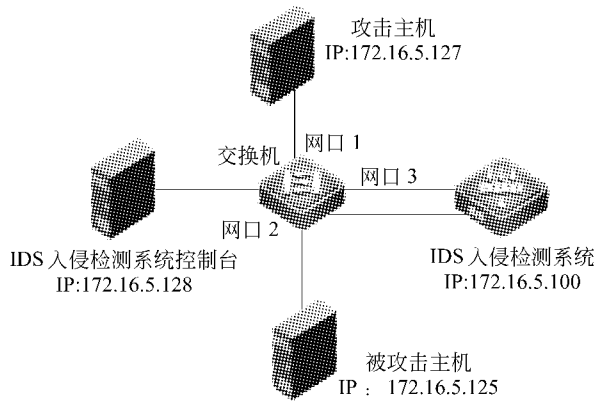

图 3-3 IDS 监听系统模型

- 检测黑客在攻击前的探测行为，预先给管理员发出警报；
- 报告计算机系统或网络中存在的安全威胁；
- 提供攻击的信息，帮助管理员诊断网络中存在的安全弱点，利于修补；
- 在大型、复杂网络中布置入侵检测系统，提高网络安全管理质量。

IDS 的运行方式有两种：一种是在目标主机上运行以监测其本身的通信信息；另一种是在一台单独的机器上运行以监测所有网络设备的通信信息，例如 Hub、路由器。当有某个事件与一个已知攻击的信号相匹配时，多数 IDS 都会警报。一个基于异常的 IDS 会构造一个当时活动的主机或网络的大致轮廓，当有一个在这个轮廓以外的事件发生时，IDS 就会告警。在 IDS 运行过程中，和以下几个关键字有关。

- 攻击(attacks)

攻击可以定义为试图渗透系统或者绕过系统安全策略而获取信息、更改信息、中断目标网络或者系统的正常运行的活动。

- 警报(alerts)

警报是 IDS 向系统操作员发出的有入侵正在发生或者正在尝试的消息。一旦侦测到入侵，IDS 会以各种方式向分析员发出警报。如果控制台在本地，IDS 警报通常会显示在监视器上。IDS 还可以通过声音报警(但在繁忙的 IDS 上建议关闭声音)。通过厂商的通信手段可以将警报发送到远程控制台，除此之外，还可以利用 SNMP 协议(安全性有待考虑)、E-mail、SMS/Pager 或者这几种方式的组合进行报警。

- 异常(anomaly)

大多 IDS 在检测到与已知攻击特征匹配的事件时就会发出警报，而基于异常的 IDS 会用一段时间建立一个主机或者网络活动的轮廓。在这个轮廓之外的事件也会发出 IDS 警报，也就是说，当有人进行以前从没有过的活动，IDS 就会发出警报。例如一个用户突然获得管理员权限(或者 root 权限)。一些厂商把这种方法称为启发式 IDS，但是真正的启发式 IDS 比这种方法有更高的智能性。

IDS 处理网络上数据信息的过程分为数据采集阶段、数据处理及过滤阶段、入侵分析及检测阶段、报告以及响应阶段 4 个阶段。

数据采集阶段是数据审核阶段，在入侵检测系统收集目标系统中，引擎提供主机通信数据包和系统使用等数据信息。入侵检测的第一步是数据信息收集，收集数据内容包括系统、网络、数据及用户活动的状态和行为。由放置在不同网段的传感器或不同主机的代理来收集信息，包括系统和网络日志文件、网络流量、非正常的目录和文件改变、非正常的程序执行。

而数据处理及过滤阶段则是对采集到的数据进行分析和处理，收集到的有关系统、网络、数据及用户活动的状态和行为等信息，送到检测引擎，检测引擎驻留在传感器中，一般通过 3 种技术手段进行分析：模式匹配、统计分析和完整性分析。当检测到某种误用模式时，产生一个警告并发送给控制台。

最后是报告以及响应阶段，通过控制台按照警告产生预先定义的响应而采取相应措施，可以重新配置路由器或防火墙、终止进程、切断连接、改变文件属性，也可以只是简单的警告。

通过分析上一阶段提供的数据、分析及检测入侵阶段来判断是否发生入侵，这一阶段是整个入侵检测系统的核心执行阶段。最后到了报告及响应阶段，针对上一个阶段进行的判断做出响应。如果通过数据来分析，判断网络中可能发生了入侵行为，系统将根据网络管理员事先配置的安全措施，对其采取相应的响应手段。此外也可以通过提示信息，通知网络管理人员网络发生了入侵，以便于采取措施。

3.4　入侵检测系统类型

入侵检测系统是从计算机网络系统中的若干关键点来收集信息，并分析这些信息，检查网络中是否有违反安全策略的行为或遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门。入侵检测通过对入侵行为的过程与特征进行研究，使安全系统对入侵事件和入侵过程做出实时响应。一般来讲，入侵检测系统按其输入数据的来源来看，可以分为 3 类：

1. 基于主机的入侵检测系统(HIDS)

基于主机的入侵检测系统输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。基于主机的入侵检测产品通常是安装在被重点检测的主机之上，主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果主体活动十分可疑(特征或违反统计规律)，入侵检测系统就会采取相应的措施。

基于主机的 IDS 对多种来源的系统和事件日志进行监控，将会发现可疑活动。基于主机的 IDS 也叫做主机 IDS，最适合于检测那些可以信赖的内部人员的误用以及已经避开了传统的检测方法而渗透到网络中的活动。除了完成类似事件日志阅读器的功能，主机 IDS 还对“事件/日志/时间”进行签名分析。在很多产品中还包含了启发式功能。因为主机 IDS 几乎是实时工作的，系统的错误可以很快地检测出来，技术人员和安全人士都非常喜欢它。现在，基于主机的 IDS 指基于服务器/工作站主机的所有类型的入侵检测系统。

基于主机的入侵检测系统的优点如下：

- 主机入侵检测系统对分析“可能的攻击行为”非常有用。
- 主机入侵检测系统在通常情况下比网络入侵检测系统误报率要低。
- 主机入侵检测系统可以部署在那些不需要广泛的入侵检测、传感器与控制台之间。

基于主机的入侵检测系统的弱点如下：

- 主机入侵检测系统安装在需要保护的设备上。
- 主机入侵检测系统的另一个问题是它依赖于服务器固有的日志与监视能力。
- 全面部署主机入侵检测系统代价较大，在企业中很难将所有主机用主机入侵检测系统保护，只能选择部分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，入侵者可利用这些机器达到攻击目标。
- 主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。

2. 基于网络的入侵检测系统(NIDS)

基于网络的入侵检测系统放置在比较重要的网段内，不停地监视网段中的各种数据包，输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。基于网络的入侵检测产品(NIDS)放置在比较重要的网段内，不停地监视网段中的各种数据包。

网络入侵检测系统的优点如下：

- 网络入侵检测系统能够检测来自网络的攻击，能够检测到未授权的非法访问。
- 网络入侵检测系统不需要改变服务器等主机配置，不需要在系统主机中安装额外软件，从而不影响这些主机的 CPU、I/O 盘等资源使用，也不会影响系统的性能。
- 由于网络入侵检测系统不像路由器、防火墙等关键设备那样工作，它不会成为系统中关键路径。网络入侵检测系统发生故障不会影响正常业务运行。部署一个网络入侵检测系统风险比主机入侵检测系统风险少得多。
- 网络入侵检测系统近年有向专业设备发展的趋势，安装这样的入侵检测系统非常方便，只需将定制设备接上电源，做一些配置，再将其连到网络上即可。

网络入侵检测系统的弱点如下：

- 网络入侵检测系统只检查它直接连接网段的通信，不能检测在不同网段的网络包。
- 网络入侵检测系统为了性能目标通常采用特征检测的方法，检测出普通的一些攻击，而很难实现一些复杂、需要大量计算与分析时间的攻击检测。
- 网络入侵检测系统可能会将大量的数据传回分析系统中。
- 网络入侵检测系统处理加密的会话过程比较困难，目前通过加密通道的攻击还不多，但随着 IPv6 的普及，这个问题会越来越突出。

3. 分布式入侵检测系统

采用上述两种数据来源的分布式入侵检测系统，能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，一般为分布式结构，由多个部件组成。

3.5 入侵检测系统设备介绍

IDS 产品有软件和硬件两种，下面介绍的是 IDS 的硬件产品。

现在的 IDS 做成了硬件放到机架上，而不是安装在现有的操作系统中，这样很容易就可以把 IDS 嵌入网络。一个入侵检测产品通常由两部分组成：传感器(Sensor)和控制台(Console)。传感器负责采集数据(如网络包、系统日志等)、分析数据并生成安全事件。控制台主要起到中央管理的作用，商品化的产品通常提供图形界面的控制台，这些控制台基本上都支持 Windows NT 平台。

IDS 设备的控制端口通常为 Console 端口，IDS 的初始配置也是通过控制端口(Console)与 PC(通常是便于移动的笔记本电脑)的串口(RS-232)连接，再通过 Windows 系统自带的超级终端(HyperTerminal)程序进行选项配置，如图 3-4 所示。

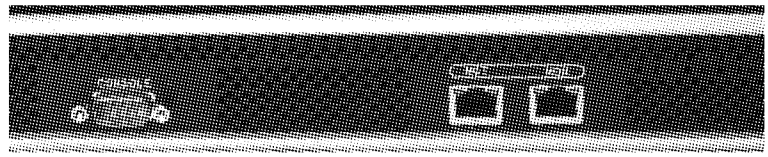

图 3-4　IDS 设备配置端口

3.6 入侵检测系统设备性能指标

对于 IDS，用户会关注每秒能处理的网络数据流量、每秒能监控的网络连接数等指标。但除了基本的硬件性质指标外，其实还有一些不为一般用户了解的指标也很重要，例如每秒抓包数、每秒能够处理的事件数等。

1. 每秒数据流量(Mbps 或 Gbps)

每秒数据流量是指网络上每秒通过某节点的数据量。这个指标是反映网络入侵检测系统性能的重要指标，一般由 Mbps 来衡量。例如 10Mbps、100Mbps 和 1Gbps。

网络入侵检测系统的基本工作原理是嗅探(Sniffer)，它通过将网卡设置为混杂模式，使得网卡可以接收网络接口上的所有数据。如果每秒数据流量超过网络传感器的处理能力，基于网络的入侵检测系统 NIDS 就可能会丢包，从而不能正常检测攻击。但是 NIDS 是否会丢包，不仅取决于每秒数据流量，还取决于每秒抓包数。

2. 每秒抓包数(pps)

每秒抓包数是反映网络入侵检测系统性能的最重要的指标。因为系统不停地从网络上抓包，对数据包作分析和处理，查找其中的入侵和误用模式。所以，每秒所能处理的数据包的多少，反映了系统的性能。业界不熟悉入侵检测系统的人往往把每秒网络流量作为判断网络入侵检测系统的决定性指标，这种想法是错误的。

每秒网络流量等于每秒抓包数乘以网络数据包的平均大小。网络数据包的平均大小差异很大，因此在相同抓包率的情况下，每秒网络流量的差异也会很大。例如，网络数据包的平均大小为 1024 字节左右，系统的性能能够支持 10 000pps 的每秒抓包数，那么系统每秒能够处理的数据流量可达到 78Mbps，当数据流量超过 78Mbps 时，会因为系统处理不过来而出现丢包现象；如果网络数据包的平均大小为 512 字节左右，在10 000pps的每秒抓包数的性能情况下，系统每秒能够处理的数据流量可达到 40Mbps，当数据流量超过 40Mbps 时，就会因为系统处理不过来而出现丢包现象。

在相同的流量情况下，数据包越小，处理的难度越大。小包处理能力，也是反映防火墙性能的主要指标。

3. 每秒能监控的网络连接数

网络入侵检测系统不仅要对单个的数据包进行检测，还要将相同网络连接的数据包组合起来进行分析。网络连接的跟踪能力和数据包的重组能力是网络入侵检测系统进行协议分析、应用层入侵分析的基础。这种分析延伸出很多网络入侵检测系统的功能，例如，检测利用 HTTP 协议的攻击、敏感内容检测、邮件检测、Telnet 会话的记录与回放、硬盘共享的监控等。

4. 每秒能够处理的事件数

网络入侵检测系统检测到网络攻击和可疑事件后，会生成安全事件或称报警事件，并将事件记录在事件日志中。每秒能够处理的事件数，反映了检测分析引擎的处理能力和事件日志记录的后端处理能力。有的厂商将反映这两种处理能力的指标分开，称为事件处理引擎的性能参数和报警事件记录的性能参数。

大多数网络入侵检测系统报警事件记录的性能参数小于事件处理引擎的性能参数，主要是 Client/Server 结构的网络入侵检测系统，引入了网络通信的性能瓶颈。这种情况将导致事件的丢失，或者控制台响应缓慢。

3.7 入侵检测产品选择要点

防火墙看起来好像可以满足系统管理员的一切需求。然而，随着攻击行为和产品自身问题的增多，IDS 由于能够在防火墙内部监测非法的活动变得越来越重要。新的技术同样给防火墙带来了严重的威胁。

当组建安全网络需要选择入侵检测系统时，要考虑的要点如下：

1. 系统的价格

当然，价格是必须考虑的要点，不过，性能价格比，以及要保护系统的价值是更重要的因素。

2. 特征库升级与维护的费用

像反病毒软件一样，入侵检测的特征库需要不断更新才能检测出新出现的攻击方法。

3. 网络入侵检测系统的最大可处理流量

要分析网络入侵检测系统所部署的网络环境，如果在 512K 或 2M 专线上部署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。

4. 该产品容易被躲避

有一些常用的躲开入侵检测的方法，如分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等。

5. 产品的可伸缩性

系统支持的传感器数目、最大数据库大小、传感器与控制台之间通信带宽和对审计日志溢出的处理。

6. 运行与维护系统的开销

产品报表结构、处理误报的方便程度、事件与日志查询的方便程度以及使用该系统所需的技术人员的数量。

7. 产品支持的入侵特征数

不同厂商对检测特征库大小的计算方法不一样。

8. 产品有哪些响应方法

要从本地、远程等多个角度考察。自动更改防火墙配置是一个很“酷”的功能，但是自动配置防火墙是一个极为危险的举动。

9. 是否通过了国家权威机构的评测

主要的权威测评机构有：国家信息安全测评认证中心、公安部计算机信息系统安全产品质量监督检验中心。