2

入侵检测产品调试与部署

知识目标

- 知道入侵检测的特点及优势
- 掌握入侵检测的基本概念及分类
- 掌握入侵检测的关键技术
- 了解入侵检测的应用和发展趋势

技能目标

- 能根据用户的网络状况进行安全需求分析
- 能够根据项目需求进行方案设计
- 合理选择入侵检测产品并能够正确部署
- 能够对入侵检测产品进行调试，正确配置安全策略
- 掌握入侵检测产品和防火墙联动的方法

项目引导

项目背景

（某）市人民政府办公厅已建成基本稳定的信息系统软、硬件平台，在信息安全方面也进行了基础性的部分建设，使系统有了一定的防护能力，现有的网络拓扑如图 2-1 所示。但是，市人民政府办公厅在信息安全方面面临的形势仍然十分严峻。病毒攻击、恶意攻击泛滥，应用

软件漏洞层出不穷，木马后门传播更为普遍，特别是黑客的攻击，直接威胁市人民政府办公厅重要信息系统，并有可能进一步窃取市人民政府办公厅相关的重要信息和数据，对核心信息系统的安全运行造成很大威胁。

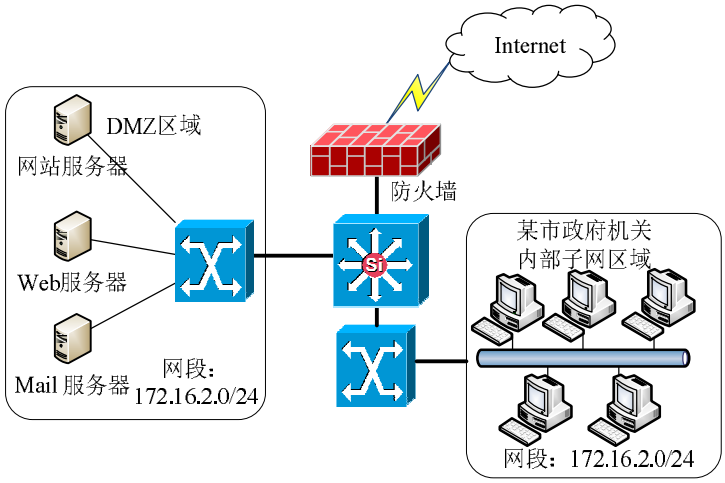

图 2-1　原有网络拓扑图

显然，仅仅部署一套防火墙系统已无法防范所有攻击，必须在现有的网络基础上添加安全设备，加固安全措施，减少安全隐患。

需求分析

现有的防火墙系统只能防范已知攻击和来自外部的攻击，且只能被动防范，无法主动防御。此外，防火墙对很多入侵方式都无能为力。例如，针对 ping 命令的攻击——ICMP 攻击；针对配置错误的攻击——IPC$攻击；针对应用漏洞的攻击——Unicode；缓冲区溢出攻击——ARP 欺骗；拒绝服务攻击——Syn Flood；针对弱口令的攻击——口令破解；社会工程学攻击等。

方案设计

为了防范来自内部和外部的攻击，入侵检测技术可以通过从计算机网络系统中若干关键节点收集信息并加以分析，监控网络中是否有违反安全策略的行为或者是否存在入侵行为，它能提供安全审计、监视、攻击识别和反攻击等多项功能，并采取相应的行动，如断开网络连接、记录攻击过程、跟踪攻击源、紧急告警等，是安全防御体系的一个重要组成部分，能与防火墙联动，增强网络防御能力。

在本方案中（市人民政府网络）部署一套入侵检测系统，该系统通过使用监控口连接交换机的镜像口来监听并分析来自重要服务器区和普通服务器区的镜像数据，负责分析网络中多个 VLAN 之间的数据交换，准确地识别来自内部和外部的各种攻击行为，实时报警和记录入侵信息，以多样化的响应方式发起告警，方便对网络情况的记录、取证工作，对网络上的可疑行为作出策略反应，及时切断入侵源，记录并通过各种途径通知网络管理员，最大幅度地保障

系统安全。安全拓扑如图 2-2 所示。

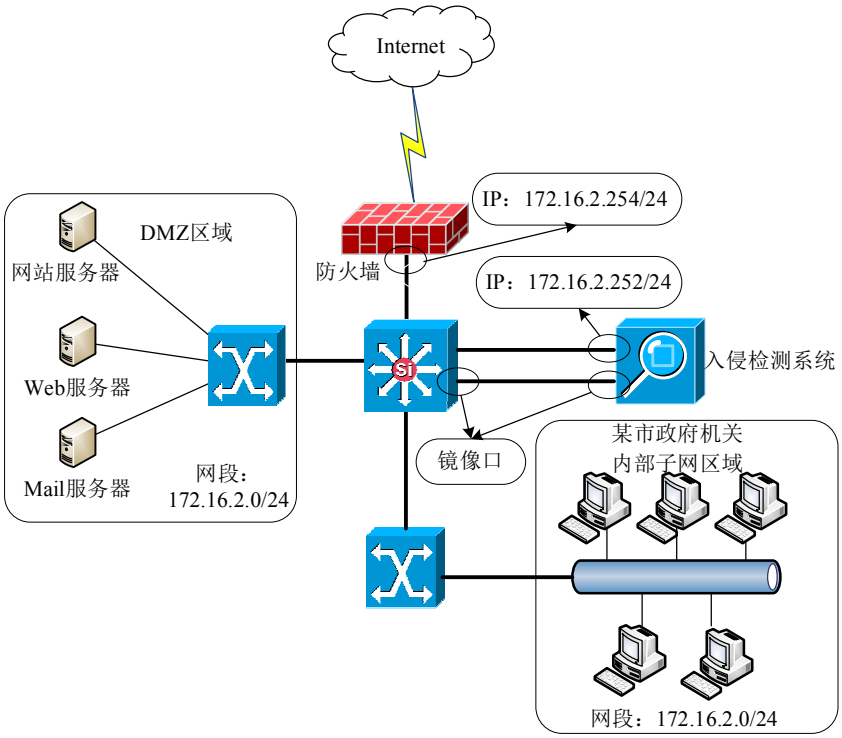

图 2-2　网络安全拓扑图

相关知识

2.1　入侵检测概述

随着信息化的应用和互联网的普及，整个世界正在迅速地融为一体，计算机网络已经成为国家的经济基础和命脉。众多的企业、组织与政府部门都在组建和发展自己的网络并连接到 Internet 上，以充分共享、利用网络的信息和资源，网络逐渐成为这些用户完成相关业务的不可或缺的手段。

与此同时，网络入侵事件也在频繁发生，入侵主要是指对信息系统资源的非授权使用，它会导致敏感信息外泄、系统数据丢失或破坏、系统拒绝服务、网络拥塞或瘫痪等。以下情况在企事业单位经常发生：

- 企业的网络系统被入侵，服务器瘫痪，但不知道什么时候被入侵的。

- 客户抱怨企业的网页无法正常打开，检查发现是服务器被攻击，但不知道遭受何种方式的攻击。
- 员工因为访问恶意站点，将后门、木马等威胁引入企业内网，造成敏感信息外泄，给企业造成巨大的损失，却无法找到问题根源。
- 企业网络拥塞，影响正常业务运转，却无法定位消耗带宽的应用类型。
- 企业网络瘫痪，检查出遭受蠕虫病毒攻击，但不知道如何清除并避免再次遭到攻击。
- 企业网络被入侵，但是在安全事件调查中缺乏证据。

……

根据调查数据显示，平均每 20 秒就发生一次入侵计算机网络的事件，超过 1/3 的互联网防火墙被攻破，这给企业网络管理带来极大的困扰，也给企业带来了巨大的安全风险。能否及时发现网络入侵，有效地检测出网络中的异常流量，成为所有网络用户面临的一个重要问题。

2.1.1 网络入侵的过程和手段

入侵技术和手段是不断发展的。从攻击者的角度说，入侵所需要的技术是复杂的，而应用的手段往往又表现得非常简单，这种特点导致攻击现象越来越普遍，对网络和计算机的威胁也越来越突出。 网络入侵的过程和手段主要有以下几点。

1. 信息探测

入侵过程一般是从信息探测开始的，攻击者开始对网络内部或外部进行有意或无意的可攻击目标的搜寻，主要应用技术包括目标路由信息探测、目标主机操作系统探测、端口探测、账户信息查询、应用服务和应用软件信息探测，以及目标系统已采取的防御措施查找等。目前，攻击者采用的手段主要是扫描工具，如操作系统指纹鉴定工具、端口扫描工具等。

2. 攻击尝试

攻击者在进行信息探测后，获取了其需要的相关信息，也就确定了在其知识范畴内比较容易实现的攻击目标尝试对象，然后开始对目标主机的技术或管理漏洞进行深入分析和验证，这就意味着攻击尝试的进行。目前，攻击者常用的手段主要是漏洞校验和口令猜解，如：专用的 CGI 漏洞扫描工具、登录口令破解等。

3. 权限提升

攻击者在进行攻击尝试以后如果成功，就意味着攻击者从原先没有权限的系统获取了一个访问权限，但这个权限可能是受限制的，于是攻击者就会采取各种措施，使得当前的权限得到提升，最理想的就是获得最高权限（如 Admin 或者 Root 权限），这样攻击者才能进行深入攻击。这个过程就是权限提升。

4. 深入攻击

攻击者通过权限提升后，一般是控制了单台主机，从而独立的入侵过程基本完成。但是，攻击者也会考虑如何将留下的入侵痕迹消除，同时开辟一条新的路径便于日后再次进行更深入的攻击，因此，作为深入攻击的主要技术手段就有日志更改或替换、木马植入以及进行跳板攻

击等。木马的种类更是多种多样，近年来，木马程序结合病毒的自动传播来进行入侵植入更是屡见不鲜。

5. 拒绝服务

如果目标主机的防范措施比较好，前面的攻击过程可能不起效果。作为部分恶意的攻击者，还会采用拒绝服务的攻击方式，模拟正常的业务请求来阻塞目标主机对外提供服务的网络带宽或消耗目标主机的系统资源，使正常的服务变得非常困难，严重的甚至导致目标主机宕机，从而达到攻击的效果。目前，拒绝服务工具已成为非常流行的攻击手段，甚至结合木马程序发展成为分布式拒绝服务攻击，其攻击威力更大。

2.1.2 入侵检测的相关定义

1. 攻击

攻击者利用工具，出于某种动机，对目标系统采取的行动，其后果是获取、破坏、篡改目标系统的数据或访问权限。

2. 事件

在攻击过程中发生的可以识别的行动或行动造成的后果，称为事件。在入侵检测系统中，事件常常具有一系列属性和详细的描述信息可供用户查看。CIDF 将入侵检测系统需要分析的数据统称为事件（Event）。

3. 入侵

入侵是指在非授权的情况下，试图存取信息、处理信息或破坏系统以使系统不可靠、不可用的故意行为。网络入侵（Hacking）通常是指具有熟练地编写和调试计算机程序的技巧，并使用这些技巧来获得非法或未授权的网络或文件访问，入侵进入内部网络的行为。

4. 入侵检测

入侵检测（Intrusion Detection）是对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。

2.1.3 入侵检测系统介绍

入侵检测系统（Intrusion Detection System，IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。在不影响网络性能的情况下能对网络进行监测，提供对内部攻击、外部攻击和误操作的实时保护，IDS 是一种积极主动的安全防护技术。系统部署如图 2-3 所示，从图中可以看到，IDS 系统通常包含探测器和控制台两部分。

防火墙为网络提供了第一道防线，IDS 被认为是防火墙之后的第二道安全闸门，弥补了防火墙的局限性和缺点，对网络进行检测，提供对内部攻击、外部攻击和误操作的实时监控，提供动态保护大大提高了网络的安全性。如图 2-4 所示，假如防火墙是一幢大楼的保安、门禁系

统，那么 IDS 就是这幢大楼里的监视系统。门锁、保安可以防止小偷进入大楼，但不能保证小偷 100%地被拒之门外，更不能防止大楼内部人员的不良企图。而一旦小偷爬窗或走后门进入大楼，或者内部人员有越界行为，门锁就没有任何作用了，这时，只有实时监视系统才能发现情况并发出警告。IDS 不仅针对外来的入侵者，同时也针对内部的入侵行为。

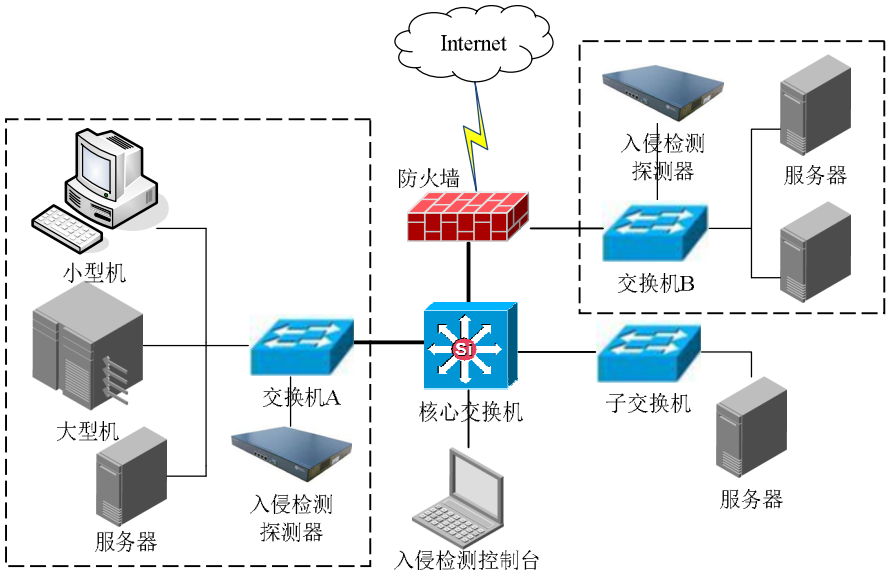

图 2-3　入侵检测系统部署

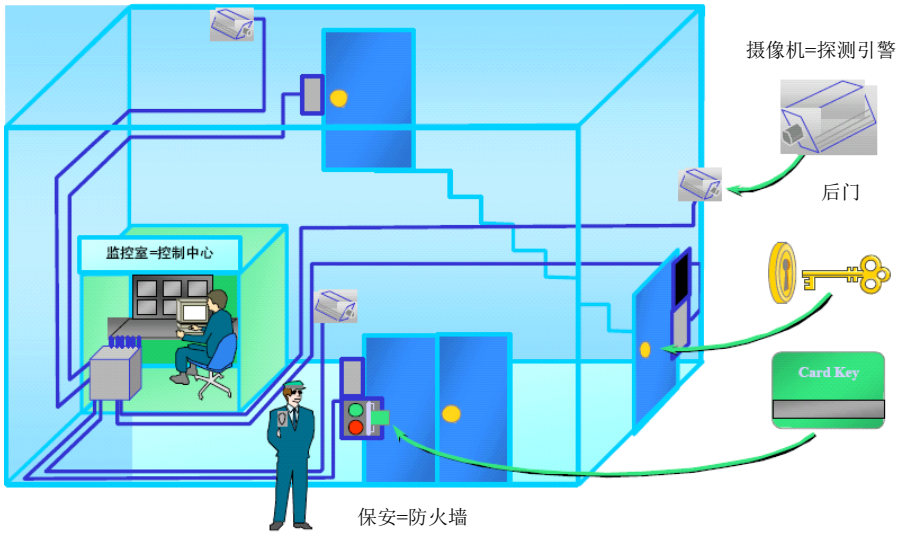

图 2-4　IDS 的功能示意图

IDS 就是网络摄像机，能够捕获并记录网络上的所有数据，同时它也是智能摄像机，能够分析网络数据并提炼出可疑的、异常的网络数据，它还是 X 光摄像机，能够穿透一些巧妙的伪装，抓住实际的内容。它不仅仅只是摄像机，还是保安员，能够对入侵行为自动地进行反击：阻断连接、关闭通路（与防火墙联动）。

IDS 通过执行以下操作来实现其功能：

（1）监视、分析用户及系统活动。

（2）系统构造和弱点的审计。

（3）识别反映已知进攻的活动模式并向相关人士报警。

（4）异常行为模式的统计分析。

（5）评估重要系统和数据文件的完整性。

（6）操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

IDS 的功能主要有三点：

（1）事前报警。IDS 能够在入侵攻击对网络系统造成危害前，及时检测到入侵攻击的发生，并进行报警。

（2）事中防御。入侵攻击发生时，IDS 可以通过与防火墙联动、TCP Killer 等方式进行报警及动态防御。

（3）事后取证。被入侵攻击后，IDS 可以提供详细攻击信息，便于取证分析。

2.1.4 入侵检测发展历史

1980 年，James P.Anderson 在给一个保密客户写的一份题为《计算机安全威胁监控与监视》的技术报告中指出，审计记录可以用于识别计算机误用，他对威胁进行了分类，第一次详细阐述了入侵检测的概念。

1984～1986 年，乔治敦大学的 Dorothy Denning 和 SRI 公司计算机科学实验室的 Peter Neumann 研究出了一个实时 IDS 模型 IDES（Intrusion Detection Expert Systems，入侵检测专家系统），是第一个在一个应用中运用了统计和基于规则两种技术的系统，是入侵检测研究中最有影响的一个系统。

1988 年，Morris 蠕虫事件导致了许多基于主机的 IDS 的开发，如 IDES、Haystack 等。

1989 年，加州大学戴维斯分校的 Todd Heberlein 写了一篇论文“A Network Security Monitor”，该监控器用于捕获 TCP/IP 分组，第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异常主机，网络入侵检测从此诞生。

1990 年，L.T.Heberlein 等人开发出了第一个基于网络的 IDS——NSM（Network Security Monitor），宣告 IDS 两大阵营正式形成：基于网络的 IDS 和基于主机的 IDS。

20 世纪 90 年代以后，不断有新的思想提出，如将信息检索、人工智能、神经网络、模糊理论、证据理论、分布计算技术等引入 IDS。

1999 年，出现商业化产品，如 Cisco Secure IDS、ISS Real Secure 等。

2000 年 2 月，对 Yahoo!、Amazon、CNN 等大型网站的 DDOS 攻击引发了对 IDS 系统的新一轮研究热潮，由此出现分布式 IDS，这是 IDS 发展史上的一个里程碑。

2.2 入侵检测的技术实现

2.2.1 入侵检测的模型

为解决入侵检测系统之间的互操作性，国际上的一些研究组织开展了标准化工作，目前对 IDS 进行标准化工作的有两个组织：IDWG（Intrusion Detection Working Group）和 CIDF（Common Intrusion Detection Framework）。CIDF 早期由美国国防部高级研究计划局赞助研究，现在由 CIDF 工作组负责，是一个开放组织。

CIDF 阐述了一个 IDS 的通用模型。它将一个 IDS 分为以下组件：事件产生器（Event Generators），用 E 盒表示；事件分析器（Event Analyzers），用 A 盒表示；响应单元（Response Units），用 R 盒表示；事件数据库（Event Databases），用 D 盒表示。如图 2-5 所示。

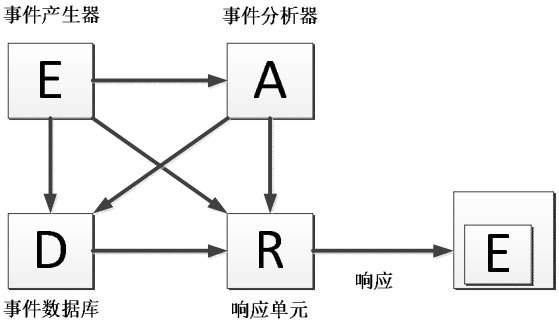

图 2-5 CIDF 模型

CIDF 模型的结构如下：E 盒通过传感器收集事件数据，并将信息传送给 A 盒，A 盒检测误用模式；D 盒存储来自 A、E 盒的数据，并为额外的分析提供信息；R 盒从 A、E 盒中提取数据，D 盒启动适当的响应。A、E、D 及 R 盒之间的通信都基于 GIDO（Generalized Intrusion Detection Objects，通用入侵检测对象）和 CISL（Common Intrusion Specification Language，通用入侵规范语言）。如果想在不同种类的 A、E、D 及 R 盒之间实现互操作，需要对 GIDO 实现标准化并使用 CISL。

2.2.2 入侵检测过程

入侵检测过程分为以下三个步骤：

（1）信息收集。入侵检测的第一步是信息收集，收集内容包括系统、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。

（2）信息分析。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，被送到检测引擎，检测引擎驻留在传感器中，一般通过三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，产生一个告警并发送给控制台。

（3）结果处理：控制台按照告警采取预先定义的响应措施，可以是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，也可以只是简单地告警。

2.2.3 入侵检测的原理

根据入侵检测模型，入侵检测系统的原理可以分为两种：异常检测和误用检测。

1. 异常检测

异常检测是根据系统或者用户的非正常行为和使用计算机资源的非正常情况来检测入侵行为。这种检测方法的基本思想是：攻击行为是异常行为的子集。将不同于正常行为的异常行为纳入攻击。

首先要总结正常操作应该具有的特征（用户轮廓），试图用定量的方式加以描述，当用户活动与正常行为有重大偏离时即被认为是入侵。某人在正常操作时的特征的集合就叫做这个用户的轮廓。例如，一个程序员的正常活动与一个打字员的正常活动肯定不同，打字员常用的是编辑文件、打印文件等命令；而程序员则用的是编辑、编译、调试、运行等命令。这样，根据各自不同的正常活动建立起来的特征，便具有用户行为特征。入侵者使用正常用户的账号，其行为并不会与正常用户的行为相吻合，因此可以检测出来。异常检测流程如图 2-6 所示，其中用户轮廓要根据正常用户的行为进行不断修正，阈值也要不断进行修正。

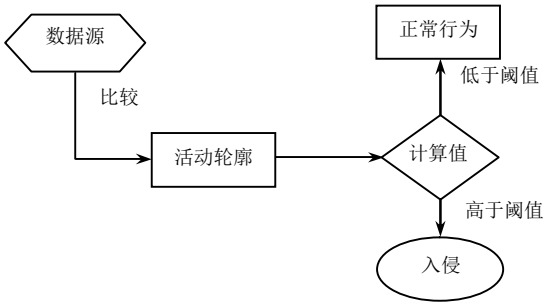

图 2-6 异常检测流程

基于异常检测原理的入侵检测方法和技术主要有以下几种方法：

（1）统计异常检测方法。根据用户对象的活动，为每个用户都建立一个特征轮廓表，通过对当前特征与以前已经建立的特征进行比较，来判断当前行为的异常性。用户特征轮廓表要根据审计记录情况不断更新，其保护可有多种衡量指标，这些指标值要根据经验值或一段时间

内的统计而得到。

（2）特征选择异常检测方法。从一组度量中挑选出能检测入侵的度量，用它来对入侵行为进行预测或分类。

（3）基于贝叶斯推理异常的检测方法。通过在任何给定的时刻测量变量值，推理判断系统是否发生入侵事件。

（4）基于贝叶斯网络异常检测方法。用图形方式表示随机变量之间的关系。通过指定的一个小的与邻接节点相关的概率集来计算随机变量的连接概率分布。按给定全部节点组合，所有根节点的先验概率和非根节点概率构成这个集。当随机变量的值变为已知时，就允许将它吸收为证据，为其他的剩余随机变量条件值判断提供计算框架。

（5）基于模式预测异常检测方法。事件序列不是随机发生的，而是遵循某种可辨别的模式，基于模式预测的异常检测法的假设条件，其特点是事件序列及相互联系被考虑到了，只关心少数相关安全事件是该检测法的最大优点。

异常检测技术的优点：无须获取攻击特征，能检测未知攻击或已知攻击的变种，且能适应用户或系统等行为的变化。

异常检测原理的缺点：一般根据经验知识选取或不断调整阈值以满足系统要求，阈值难以设定；异常不一定由攻击引起，系统易将用户或系统的特殊行为（如出错处理等）判定为入侵；系统检测的准确性受阈值的影响，在阈值选取不当时，会产生较多的检测错误，造成检测错误率高；攻击者可逐渐修改用户或系统行为的轮廓模型，因而检测系统易被攻击者训练；无法识别攻击的类型，因而难以采取适当的措施阻止攻击的继续。

2. 误用检测

误用检测也称为基于知识或基于签名的入侵检测。误用检测 IDS 根据已知攻击的知识建立攻击特征库，通过用户或系统行为与特征库中各种攻击模式的比较确定是否发生入侵。这种检测与杀毒软件依照病毒库查找病毒的过程有些类似，只是杀毒软件检测的是文件，而 IDS 检测的是通信过程（数据流）。误用检测流程如图 2-7 所示，其要点是建立攻击特征库，并不断进行更新和完善。

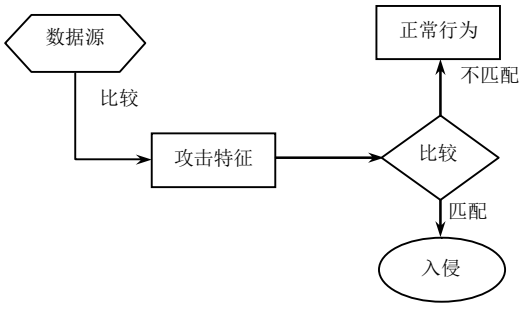

图 2-7　误用检测流程

常用的误用检测方法和技术主要有以下几种：

（1）基于专家系统的检测方法。这个方法的思想是把安全专家的知识表示成规则知识库，再用推理算法检测入侵。主要是针对有特征的入侵行为。

（2）基于状态转移分析的检测方法。该方法的基本思想是将攻击看成一个连续的、分步骤的并且各个步骤之间有一定关联的过程。在网络发生入侵时及时阻断入侵行为，防止可能还会进一步发生的攻击行为。在状态转移分析方法中，一个渗透过程可以看作是由攻击者做出的一系列的行为，而导致系统从某个初始状态变为最终某个被危害的状态。

（3）基于模型误用检测方法。它是通过把收集到的信息与网络入侵和系统误用模式数据库中的已知信息进行比较，从而发现违背安全策略的行为进行。模式匹配法可以显著地减少系统负担，有较高的检测率和准确率。

误用检测技术的关键问题是攻击签名的正确表示。误用检测是根据攻击签名来判断入侵的，如何用特定的模式语言来表示这种攻击行为是该方法的关键所在。尤其攻击签名必须能够准确地表示入侵行为及其所有可能的变种，同时又不会把非入侵行为包含进来。由于大部分的入侵行为是利用系统的漏洞和应用程序的缺陷进行攻击的，那么通过分析攻击过程的特征、条件、排列以及事件间的关系，就可以具体描述入侵行为的迹象。

3. 异常检测和误用检测技术的不同

误用检测是根据已知的攻击方法和技术总结构成特征库的，所以无法检测到新的攻击方法；而异常检测是根据假设划定系统合理的行为范围（阈值）来定义特征库，实时检测系统的状态和行为是否在合理范围内，所以这种通过表现检测的方式能检测到未知的攻击。

误用检测针对具体的行为进行推理和判断入侵攻击；而异常检测根据使用者的行为和资源的使用情况来判断。

异常检测误报率高，特别是在多用户、工作行为变动情况下，没有一个相对稳定的状态表现；而误用检测准确率较高，但对于新型的攻击漏报率也较高。

误用检测对系统依赖性高，异常检测依赖性低，移植性好。

1998 年 2 月，Secure Networks Inc.指出 IDS 有许多弱点，主要为：IDS 对数据的检测；对 IDS 自身攻击的防护。由于当代网络发展迅速，网络传输速率大大加快，这造成了 IDS 工作的很大负担，也意味着 IDS 对攻击活动检测的可靠性不高。而 IDS 在应对对自身的攻击时，对其他传输的检测也会被抑制。同时由于模式识别技术的不完善，IDS 的高误报率也是它的一大问题。

误报：实际无害的事件却被 IDS 检测为攻击事件。

漏报：一个攻击事件未被 IDS 检测到，或被分析人员认为是无害的。

2.3 入侵检测系统的分类

IDS 有多种分类方式，根据体系结构的不同可以分为集中式 IDS 和分布式 IDS；根据实

现方式的不同可以分为基于主机的 IDS（HIDS）和基于网络的 IDS（NIDS）；根据实现技术的不同，可以分为误用检测 IDS 和异常检测 IDS。这里重点介绍基于主机和基于网络的 IDS 系统。

1. 基于主机的入侵检测系统

这类 IDS 对多种来源的系统和事件日志进行监控，发现可疑活动。基于主机的入侵检测系统也叫做主机 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。许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，系统的错误就可以很快地检测出来，技术人员和安全人士都非常喜欢它。基于主机的 IDS 就是指基于服务器/工作站主机的所有类型的 IDS。其常用部署如图 2-8 所示，通常是个检测代理软件（Agent），安装于被保护的主机中，通过查询、监听当前系统的各种资源（主要包括系统运行状态信息、系统记账信息、系统事件日志、应用程序事件日志、进程、端口调用、C2 级安全审计记录、文件完整性检查等）的使用运行状态，发现系统资源被非法使用和修改的事件，并进行上报和处理，会消耗系统的一定资源。

HIDS 的主要优点有：性价比高；更加细腻，能够监视特定的系统活动；误报率较低；适用于交换和加密环境；对网络流量不敏感；能够确定攻击是否成功。

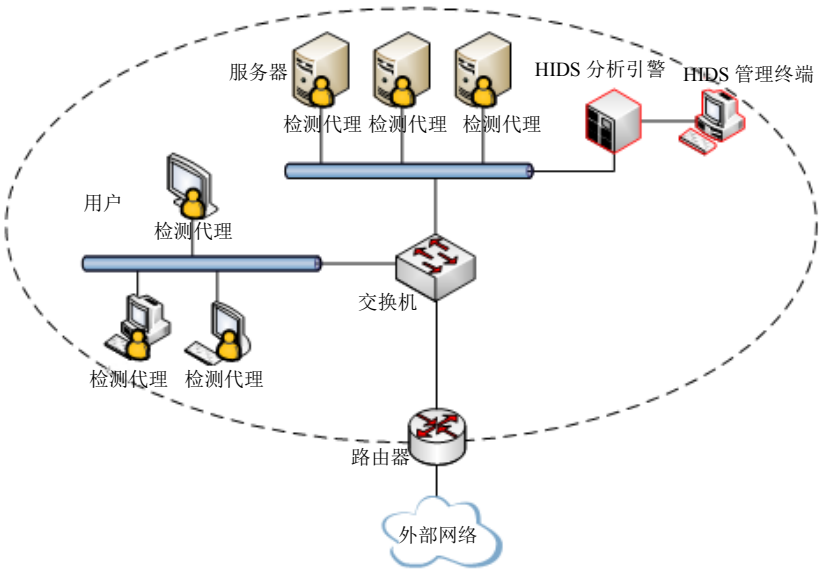

图 2-8　HIDS 典型部署

2. 基于网络的入侵检测系统

基于网络的 IDS 对所有流经监测代理的网络通信量进行监控，对可疑的异常活动和包含攻击特征的活动作出反应。在比较重要的网段安装探测器，往往是将一台机器（网络传感器）

的一个网卡设于混杂模式（Promisc Mode），监听本网段内的所有数据包并进行事件收集和分析、执行响应策略以及与控制台通信，来监测和保护整个网段，它不会增加网络中主机的负载。NIDS 存在基于应用程序的产品，只需要安装到主机上就可应用。NIDS 对每个信息包进行攻击特征的分析，但是在网络高负载下，还是要丢弃些信息包。其部署如图 2-9 所示。

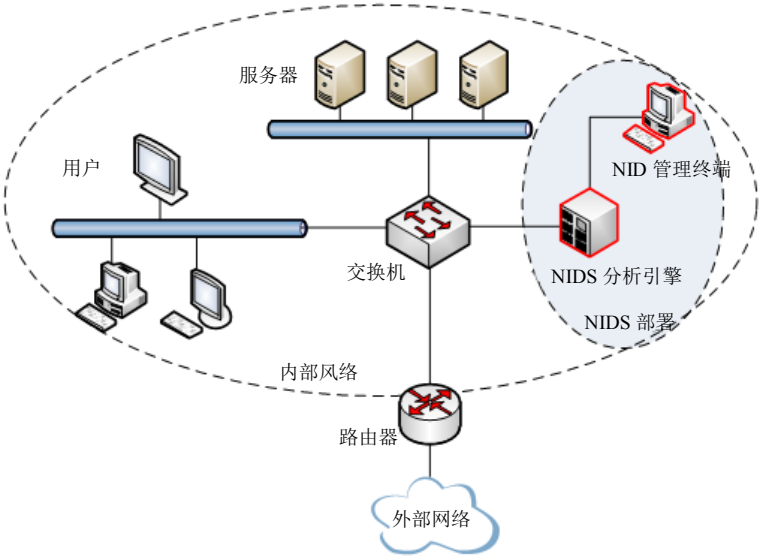

图 2-9　NIDS 典型部署

NIDS 的主要优点有：隐蔽性好；可实时检测和响应；攻击者不易转移证据；不影响业务系统；可较全面发现入侵；能够检测未成功的攻击企图。

表 2-1 比较了 HIDS 与 NIDS 的特点，以加深对两者的理解。

表 2-1　HIDS 与 NIDS 比较表

项目	HIDS	NIDS
专用硬件	不需要	需要，网络范围大时需要多个探测器
审计内容	主机内的敏感文件、目录、程序、端口的使用情况	网络数据包、检测网络攻击
判断攻击成功与否	能更准确判断	难以准确判断
未成功的攻击	较难检测	能检测
加密环境	适用	不适用
对网络的影响	无	有
安全性	受限于主机操作系统、系统日志，只检测主机不检测网络	专用操作系统，加密通信难以检测安全性、检测网络
响应方式	事后响应	实时响应

3. 混合型入侵检测系统（Hybrid IDS）

在新一代的入侵检测系统中，将把现在基于网络和基于主机这两种检测技术很好地集成起来，提供集成化的攻击签名检测报告和事件关联功能。虽然这种解决方案覆盖面极大，但同时要考虑到由此引起的巨大数据量和费用。许多网络只为非常关键的服务器保留混合 IDS。

2.4 端口镜像技术

NIDS 需要对局域网的所有网络流量进行监控，为了方便入侵检测系统，对一个或多个网络接口的流量和数据包进行分析，可以通过配置交换机来把一个或多个端口（VLAN）的数据转发到某一个端口来实现对网络的监听。

端口镜像技术（Port Mirroring）是把交换机一个或多个端口（VLAN）的数据镜像到一个或多个端口的方法。端口镜像又称端口映射，是网络通信协议的一种方式。它既可以实现一个 VLAN 中若干个源端口向一个监控端口镜像数据，也可以从若干个 VLAN 向一个监控端口镜像数据。

例如，源端口的 5 号端口（或所有端口）上流转的所有数据流均可被镜像至 10 号监控端口，而入侵检测系统通过监控 10 号端口接收了所有来自 5 号端口（或所有端口）的数据流。值得注意的是，源端口和镜像端口必须位于同一台交换机上；而且端口镜像并不会影响源端口的数据交换，它只是将源端口发送或接收的数据包副本发送到监控端口。

2.5 NIDS 系统部署

现今基于网络的 IDS 是主流，这里主要介绍 NIDS 的部署方式。从功能上看，NIDS 分为两大部分：探测引擎和控制中心。前者用于监听原始网络数据和产生事件；后者用于显示和分析事件及策略定制等工作，如图 2-10 所示。

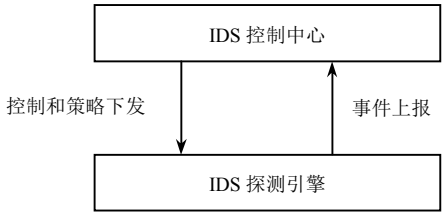

图 2-10 IDS 的组成

引擎采用旁路方式全面侦听网上信息流，实时分析，然后将分析结果与探测器上运行的策略集相匹配。执行报警、阻断、日志等功能，完成对控制中心指令的接收和响应工作。它是由策略驱动的网络监听和分析系统。

采用旁路方式不需要更改现有网络结构，不会影响业务系统运行，而且部署简单、方便；一旦系统发生断电或故障现象时，不会影响整个网络的正常运行。入侵检测旁路部署在交换机上，一般情况下，入侵检测需要配置两个口，一个口为管理口，另一个口为监控口。管理口连接在交换机的任何一个口，供网络安全管理员管理；监控口连接此交换机的镜像口，以便能及时地监控网络的数据。

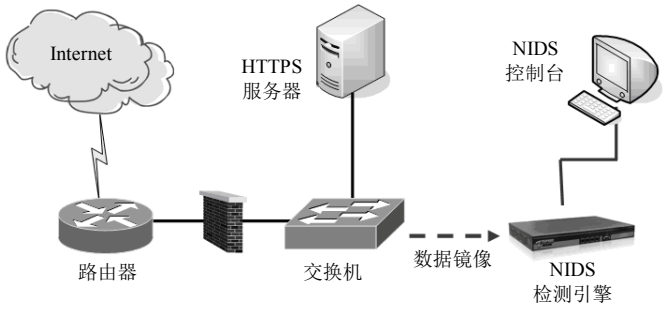

图 2-11　IDS 的部署方式

控制中心提供报警显示以及预警信息的记录和检索、统计功能制定入侵监测的策略。控制探测器系统的运行状态，收集来自多台引擎的上报事件，综合进行事件分析，以多种方式对入侵事件作出快速响应。

在部署 IDS 之前，需要对现有网络结构及网络应用作详细的了解，然后根据网络业务系统的实际需求配置相应规则库，以便能够及时检测入侵源，记录并通过各种途径通知网络安全管理员，最大幅度地保障系统安全，并且在提高网络安全的同时不影响业务系统的性能，在进行入侵检测安全策略制定的过程中，需要业务应用人员及相关的行政领导的配合和支持，同时也要注意现有网络结构环境，以防产生误报和漏报。制定一个比较实用而又合适的入侵检测策略，首先，要进行网络拓扑结构的分析，确定入侵检测的部署位置，配置被部署的交换机的镜像口；其次，开始配置入侵检测管理口、监控口和启动检测引擎服务，以便能及时检测入侵源；最后，根据实际的网络环境和安全的要求，制定相应的规则，并查看入侵日志、本身安全性管理。在入侵检测具体实施中，选择并配置好入侵检测规则。

2.6　入侵检测软件 Snort

Snort 是一个功能强大、跨平台、轻量级的网络入侵检测系统，从入侵检测分类上来看，Snort 是个基于网络和误用检测的入侵检测软件。它可以运行在 Linux、OpenBSD、FreeBSD、Solaris 以及其他 UNIX、Windows 等操作系统之上。Snort 是一个用 C 语言编写的开放源代码软件，符合 GPL（GNU General Public License，GNU 通用公共许可证）的要求，由于其是开源且免费的，许多研究和使用入侵检测系统都是从 Snort 开始，因而 Snort 在入侵检测系统方

面占有重要地位。Snort 的网站是http://www.snort.org。用户可以登录网站，下载在 Linux 和 Windows 环境下安装的可执行文件，并可以下载描述入侵特征的规则文件。在 http://www.snort.org/start/requirements 页面可以查看到在 Linux 和 Windows 两个平台所需要的所有软件及其下载链接，如图 2-12 所示。

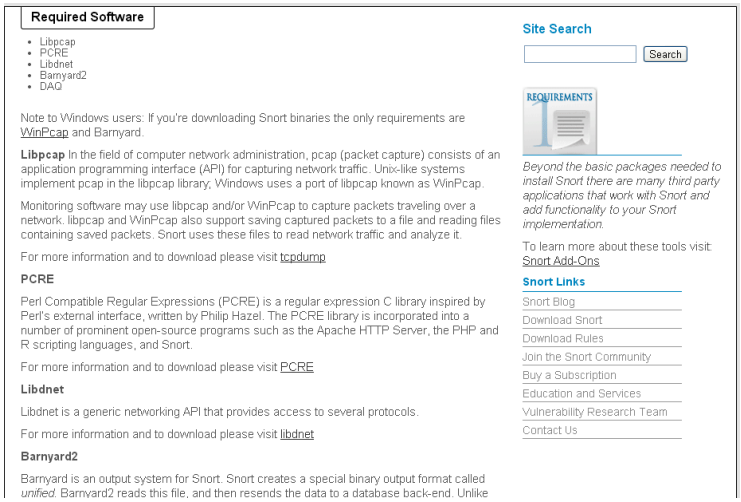

图 2-12　Snort 所需软件页面

Snort 对系统的影响小，管理员可以很轻易地将 Snort 安装到系统中去，并且能够在很短的时间内完成配置，方便地集成到网络安全的整体方案中，使其成为网络安全体系的有机组成部分。虽然 Snort 是一个轻量级的入侵检测系统，但是它的功能却非常强大。Snort 的安装和使用都很简单，这里不再赘述。

2.7　IDS 与防火墙的联动

IDS 与防火墙的联动是指 IDS 在捕捉到某一攻击事件后，按策略进行检查，如果策略中对该攻击事件设置了防火墙阻断，那么 IDS 就会发给防火墙一个相应的动态阻断策略，防火墙根据该动态策略中的设置进行相应的阻断，阻断的时间、阻断时间间隔、源端口、目的端口、源 IP 和目的 IP 等信息，完全依照 IDS 发出的动态策略来执行。一般来说，很多情况下，不少用户的防火墙与 IDS 并不是同一家的产品，因此在联动的协议上面大都遵从 OPSEC 协议（Check Point 公司）进行通信，不过也有某些厂家自己开发相应的通信规范。目前总地来说，联动有一定效果，但是稳定性不理想，特别是攻击者利用伪造的包信息，让 IDS 错误判断，进而错误指挥防火墙将合法的地址无辜屏蔽掉。

IDS 与防火墙联动的工作模型如图 2-13 所示。黑客首先穿透防火墙向主机 A 发起攻击，这时 IDS 识别到了攻击行为，IDS 会向防火墙发送通知报文；防火墙收到报文后，进行验证并

采取措施，通常是建立一条阻断或报警该链接的规则；当黑客再次发起攻击时，防火墙就会根据规则选择阻断或报警此台非法链接。

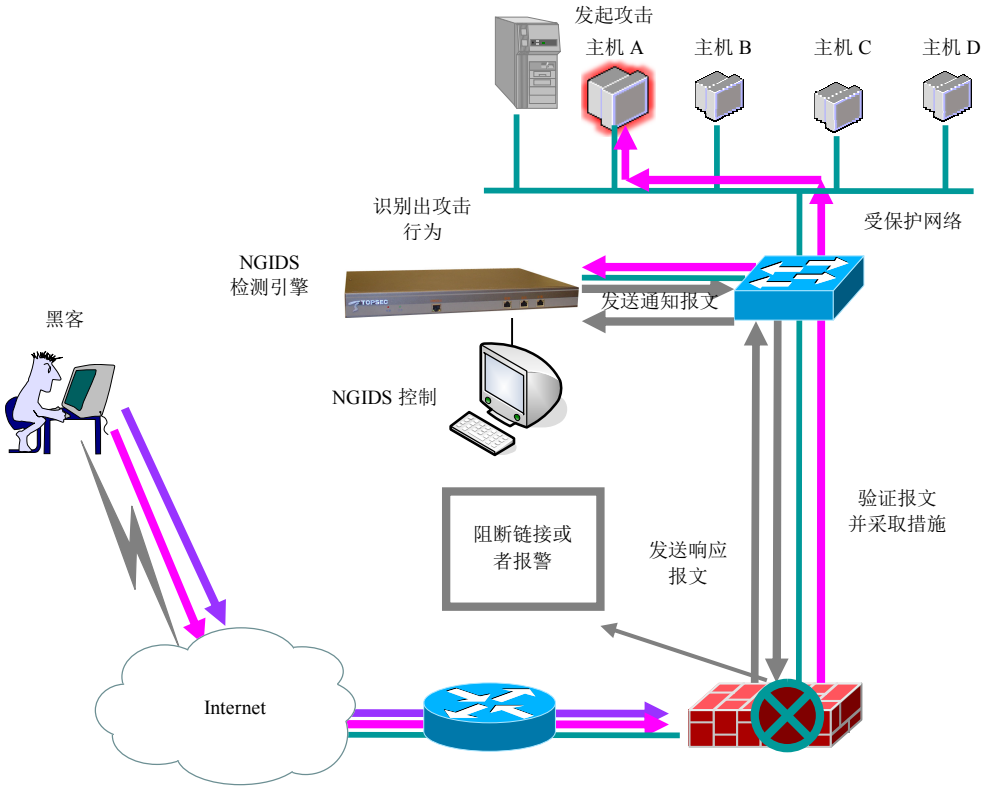

图 2-13　IDS 与防火墙联动流程

这种阻断非法链接的方式还是有很大的局限性的。整个从发现到阻断的操作需要 100 毫秒的时间，这对现代网络来说是一个巨大的时间窗口，而且它只能针对相同攻击第二次以后的链接进行阻断，第一次攻击还是会放行的。因此，比如说单个数据包的攻击就无法进行阻断，因为这种攻击方式只对同一个目的地址发送一次攻击数据包。

任务实施

2.8　项目实训

根据本章开头所述具体项目的需求分析与整体设计，现以项目中与 IDS 相关的一部分拓扑为例，进行 IDS 设备部署和调试实训，网络拓扑图如图 2-14 所示。

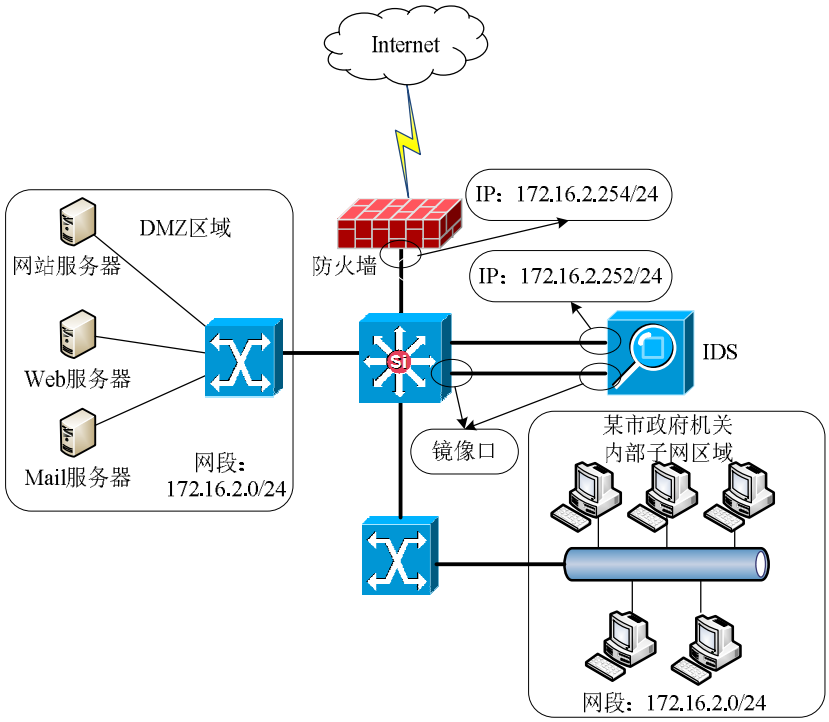

图 2-14　入侵检测部署拓扑图

如图 2-14 所示，在交换机上旁路接入一台入侵检测设备。

该设备具备 4 个标准网络接口，将其中两个口分别连接到交换机上，两个口各有用处，LAN2 作管理口，以便内部网络（主要是安全管理员）进行管理、访问；LAN3 作监控口，必须连接到交换机的镜像口。根据实际需要，在入侵检测上配置相应的规则，使之能检测到内部子网区域、DMZ 区域之间 ICMP 包攻击的数据，及时地对攻击进行处理。

配置入侵检测的规则，开启引擎服务，查看相关入侵日志。

2.8.1　任务 1：认识入侵检测系统并进行基本配置

为能更深入地结合入侵检测产品，实际学习入侵检测的配置，本章采用蓝盾 IDS 进行实践操作，通过对该设备的配置，达到前面所述的需求分析和方案设计。为此，先了解一下入侵检测设备的基本配置方法。

在一般的入侵检测的配置里，常见配置步骤为：入侵检测初步认识→入侵检测初始化配置→网络接口配置→规则配置→设备服务重启。

1. 了解 IDS 硬件

（1）了解 IDS 前面板，如图 2-15 所示，类似防火墙设备，IDS 主要包含四个网络接口、一个 CONSOLE 口和两个指示灯。

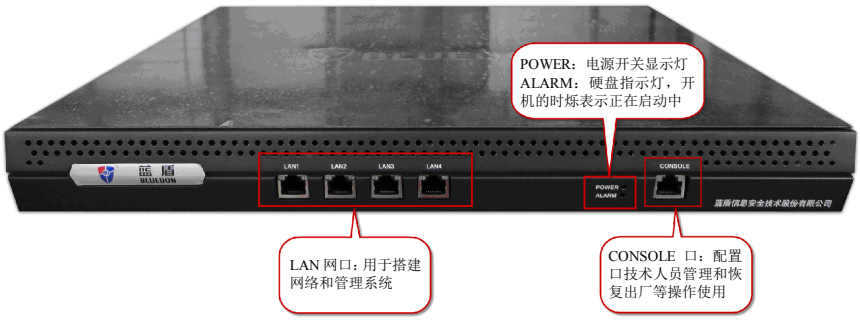

图 2-15　IDS 前面板

（2）仔细观察 IDS 后面板，如图 2-16 所示。

图 2-16　IDS 后面板

（3）了解 IDS 的初始配置参数，如表 2-2 所示为 IDS 出厂配置参数。不同厂商、不同型号的入侵检测产品，出厂参数一般都不相同，具体要参考设备手册。

表 2-2　入侵检测初始配置

网口	IP 地址	掩码	备注
LAN1	192.168.0.145	255.255.255.0	默认管理口
LAN2	无	无	可配置口
LAN3	无	无	可配置口
LAN4	无	无	可配置口

其中，LAN1 为默认管理口，默认地打开了 443 端口（HTTPS）以供管理入侵检测使用。本实验我们利用网线连接 LAN1 口与管理 PC，并设置好管理 PC 的 IP 地址。默认所有配置均为空，可在管理界面得到入侵检测详细的运行信息。

2. 利用浏览器登录 IDS 管理界面

（1）将 PC 与 IDS 的 LAN1 网口连接起来，我们将使用这条网线访问 IDS，并进行配置。

当需要连接内部子网或外线连接时，也只需要将线路连接在对应网口上，只是要根据具体情况进行 IP 地址设置。

（2）客户端 IP 设置，这里以 Windows XP 为例进行配置。打开网络连接，设置本地连接 IP 地址。这里的 IP 地址设置的是 192.168.0.100，这是因为所连端口 LAN1 的 IP 是 192.168.0.145，IP 必须设置在相同地址段上。

（3）单击“开始”→“运行”命令，输入 CMD，打开命令行窗口，使用 ping 命令测试 IDS 和管理 PC 间是否能互通。此处操作与防火墙配置时进行的连通性测试类似。

（4）打开 IE 浏览器，输入管理地址 https://192.168.0.145，进入欢迎界面。因为是通过 HTTPS 访问，会出现安全证书提示，如图 2-17 所示。

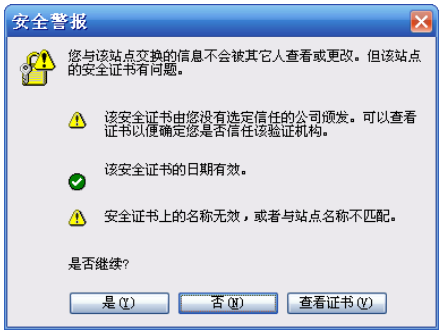

图 2-17　安全证书提示

单击“是”按钮，会出现登录入侵检测欢迎窗口，接着输入用户名和密码，默认用户名和密码分别为 admin 和 888888，单击“登录”按钮，进入入侵检测管理系统，如图 2-18 所示。

图 2-18　入侵检测主界面

3. 入侵检测的基本配置

（1）依次单击“网络设置”→“外线口设置”→“WAN 设定”命令，将 LAN2 的 IP 配置为 172.16.2.252，子网掩码为 255.255.255.0，默认网关为 172.16.2.254。单击“保存”按钮并连接（将 LAN2 口作为管理口，用于管理设备），如图 2-19 所示。

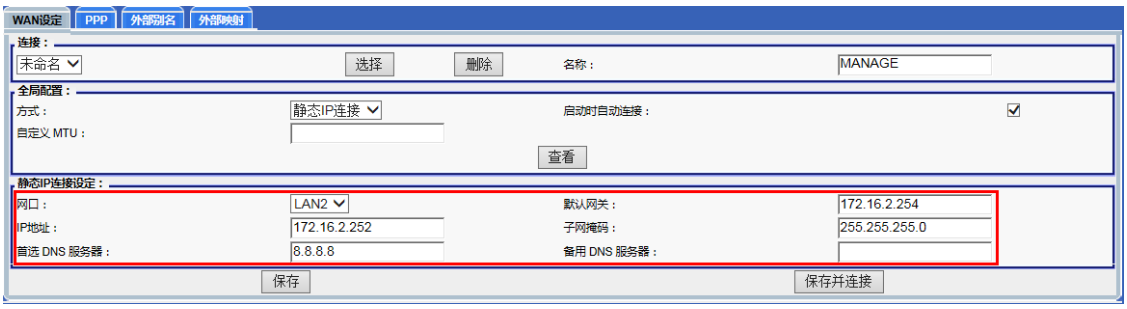

图 2-19　WAN 口配置

（2）依次点击“系统”→“管理设置”→“管理界面访问设定”命令，“网口”选择“LAN2”，其余选项保持默认，单击“添加”按钮，如图 2-20 所示。

图 2-20　管理口访问策略设定

（3）依次单击“网络设置”→“镜像口设置”→“镜像设定”命令，将 LAN3 口配置为监控口（这里又叫镜像网口），用于接收经过交换机的信息，故此必须连接到交换机的镜像口上，如图 2-21 所示。

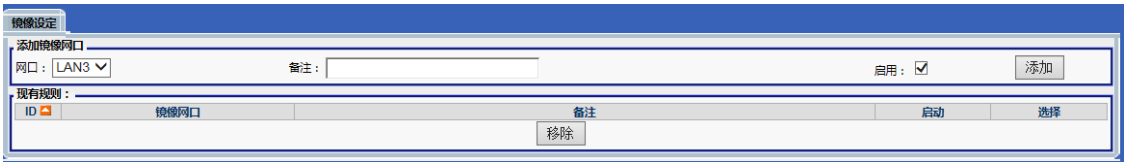

图 2-21　镜像网口设定

注意：镜像网口的选择只有 LAN3 和 LAN4，这是因为 LAN3、LAN4 口不属于内网口和 WAN 口。因此在配置镜像网口时，这个口一定要没有任何网口设定。

下面“现有规则”区域中出现了一条镜像规则，如图 2-22 所示。

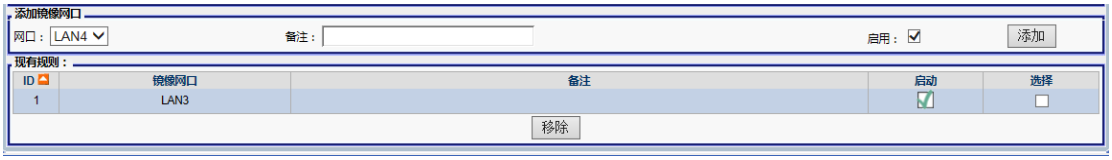

图 2-22　镜像网口配置界面

上面配置结束后，入侵检测的网口配置就暂时告一段落。但是还需根据不同管理人员配置相应的用户权限，使各管理员各司其职，互不干涉。

4. 入侵检测的设备管理配置

（1）依次单击“系统”→“管理设置”→“密码”命令，按图 2-23 所示配置管理员用户，不启用 USBKEY。

图 2-23　管理用户配置界面

下面就出现了一个超级管理员用户，如图 2-24 所示。

图 2-24　管理用户配置列表

（2）增加一个低权限用户，即只允许浏览 IDS，不允许进行操作，如图 2-25 所示。

下面添加了一个新用户 lorry，只有“查看日志”、“实时报表”的权限，一般用于让审计员等相关人员查看。

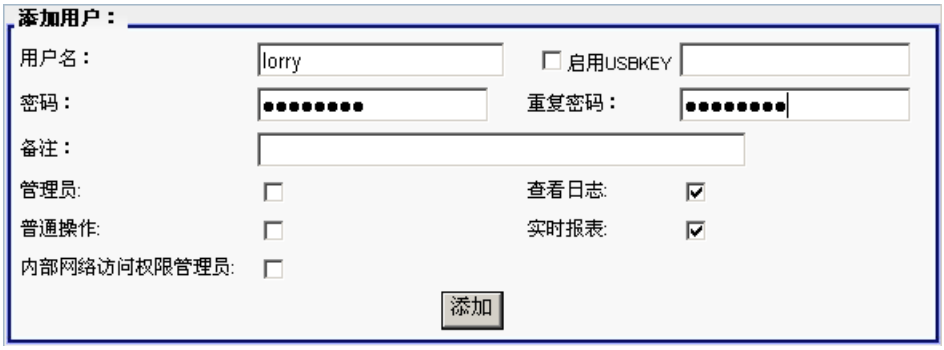

图 2-25　审计用户配置界面

（3）依次单击“系统”→“管理设置”→“用户安全设置”命令，进行用户安全设置，如图 2-26 所示。

图 2-26　用户安全设置界面

在设置密码时，如果密码长度没有达到要求位数时将出现提示，如图 2-27 所示。

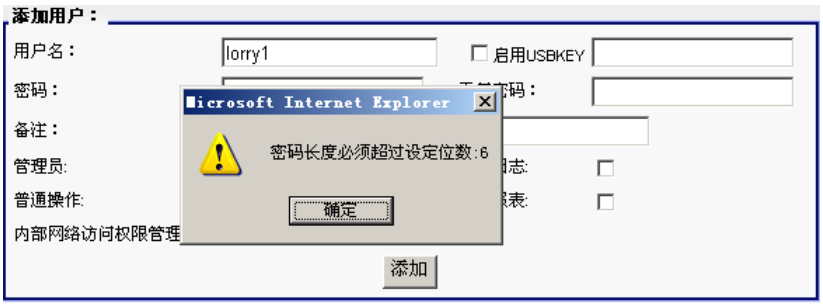

图 2-27　密码长度设定错误界面

输入密码时一定要提高密码的强度，需要“数字+字符”的形式。

登录超过限制次数，系统会将用户锁定，1 分钟后用户才能重新登录，如图 2-28 所示。

2.8.2　任务 2：入侵检测规则配置

（1）将入侵检测按照部署拓扑（见图 2-14）所示接入市人民政府办公厅当前网络，入侵检

测设备的 LAN2 口接入内网核心交换机，入侵检测设备的 LAN3 口接内网核心交换机的镜像口。

图 2-28　密码复杂度设定错误界面

（2）系统自带检测规则。选择“入侵检测”→“检测规则”命令，该页面显示所有 IDS 自带检测规则，用户可以查看已经勾选的规则库，或进行规则库的选择。系统会定时自动下载更新规则库，以使用户得到及时的保护。用户也可上传自定义补丁更新规则库，如图 2-29 所示。

图 2-29　规则库界面

根据市人民政府办公厅的需求，常发现 ICMP 攻击，这里要对 ICMP 规则库进行勾选，下面也以 ICMP 攻击为例进行实训，如图 2-30 和图 2-31 所示。

最后单击“保存”按钮，使规则策略生效。

注意：建议用户只勾选必要的选择，以提高检测的速率和性能。例如，如果内部网络中没有数据库服务器，则不必勾选数据库选项下的规则库。一般情况下，勾选的规则越多，对进出数据包的检测匹配耗时越长，降低 IDS 设备处理性能。

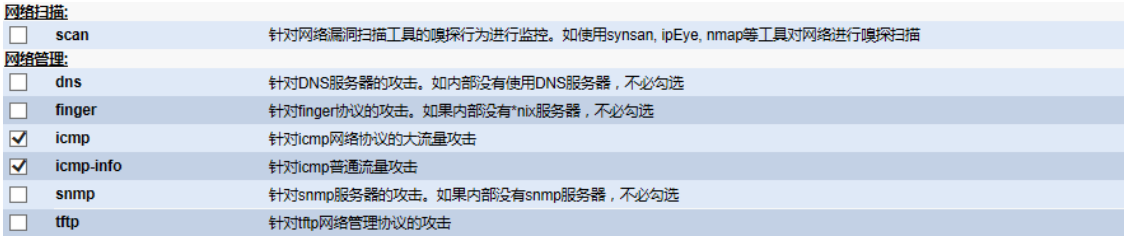

图 2-30　规则库勾选界面

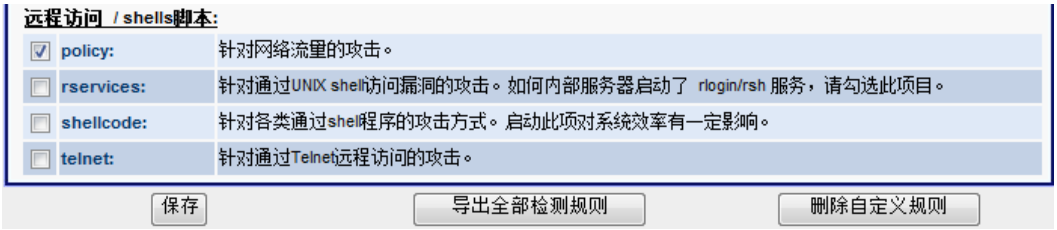

图 2-31　规则库保存

（3）选择“入侵检测”→“启动控制”命令，在该页面上选择 IDS 的“启动入侵检测”复选框来启动引擎服务，网口选择之前配置的监控口（即入侵检测系统的镜像网口），最后单击“重启”按钮，使服务启动，如图 2-32 所示。

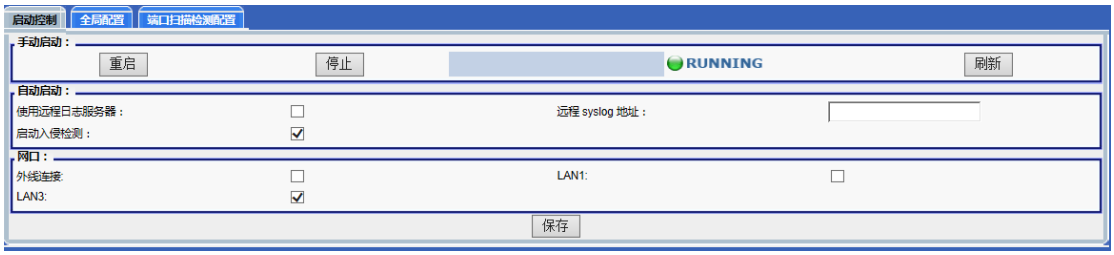

图 2-32　启动入侵服务

2.8.3　任务 3：入侵检测测试

（1）市政府内部子网区域 PC 机（172.16.2.200/24），访问 DMZ 区域中 Web 服务器（IP：172.16.2.168），如图 2-33 所示。

图 2-33　ICMP 测试

（2）查看入侵日志。

进入蓝盾入侵检测系统管理界面，选择“报表日志”→“系统日志”→“入侵检测日志查询”命令，然后单击“查看”按钮，效果如图 2-34 所示。

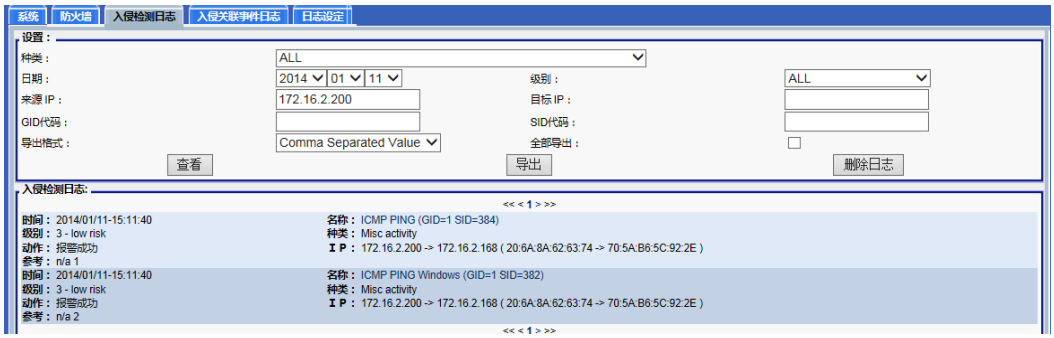

图 2-34　查看日志

2.9　项目实施与测试

2.9.1　任务 1：入侵检测系统规划

根据项目建设的要求，对 IDS 进行物理连接、接口和 IP 地址分配、路由表及 IDS 策略规划。

1. 接口规划

根据现有网络结构，对该市政府网络 IDS 的物理接口做如表 2-3、表 2-4 所示的设计。

表 2-3　IDS 物理连接表

本端设备名称	本端端口号	对端设备名称	互联线缆	对端端口号
ZZGLYYNIDS-xx	LAN2	三层交换机	6 类双绞线	E1/0/1
	LAN3	三层交换机	6 类双绞线	E1/0/2

注：因实施环境不具备而无法实施，以后可以按照客户的需求进行配置。

表 2-4　接口和 IP 地址分配表

设备名称	端口	IP 地址	掩码	管理
ZZGLYYNIDS-xx	LAN1	192.168.0.145	255.255.255.0	Ssh/telnet/ http/https
	LAN2	172.16.2.252	255.255.255.0	
	LAN3	无	无	

注：目前环境因素不具备具体配置实施条件，整体配置在后期建设中规划，本阶段对设备仅进行加电处理。

2. 路由规划

根据该市政府网络的情况，现对 IDS 路由规划，如表 2-5 所示。

表 2-5 IDS 路由表

设备	目的网段	下一跳地址
ZZGLYYNIDS-xx	172.16.2.0	172.16.2.254
	0.0.0.0	172.16.2.254

2.9.2 任务 2：网络割接与 IDS 实施

在项目实施过程中根据如下时间序列进行项目实施，在项目实施之前确保已经做好 IDS 配置。

1. 前期准备

（1）确认当前政府机关网络运行正常。

（2）确认 IDS 状态正常。

（3）确认 IDS 配置正常。

（4）进行割接前业务测试，且记录测试状态。

2. 产品上架

具体步骤如下：

（1）产品上架前策略配置检查和交换机测试。

（2）选择在市政府网络业务较为空闲时实施产品安装。

（3）根据方案设计的部署 IDS 及相关接口的连接与策略配置，如表 2-3 所示。

3. 测试

（1）测试终端 PC 到 IDS 的连通性（可 ping IDS 接口地址）。

（2）对预订好的业务进行测试，且对比之前的网络状态，查看网络是否异常。

（3）进行 IDS 策略测试。

4. 实施时间表

根据项目计划，由整个项目实施过程到完成入侵检测规则的配置及测试，尽可能不影响网络的负担，并且在不中断网络及业务的情况下完成，一般的实施过程和时间如表 2-6 所示。

表 2-6 IDS 实施时间表

步骤	动作	详细	业务中断时间（分钟）	耗时（分钟）
1	设备上架前检查	IDS 加电检查 IDS 软件检查 IDS 配置检查	0	20

续表

步骤	动作	详细	业务中断时间（分钟）	耗时（分钟）
2	实施条件检查确认	IDS 机架空间/挡板准备检查 网线部署检查 电源供应检查	0	10
3	设备上架	根据项目规划将设备上架 接通电源，并确认设备正常启动完成	0	30/延长
4	IDS 上线	上线 IDS	0	5/延长
		IDS 状态检查	0	10/延长
		业务检查及测试	0	15/延长

5. 回退

如经测试发现未成功，则执行回退。回退步骤如下：

（1）拔出 IDS 上所接所有线路。

（2）将汇聚交换机与内部交换机之间的线路进行连接，所有线路还原。

（3）业务连接测试。

综合训练

一、判断题

1. 入侵是指任何企图破坏资源的完整性、保密性和有效性的行为。（　　）

2. 入侵检测的直接目的是阻止入侵事件的发生。（　　）

3. 基于主机的入侵检测和基于网络的入侵检测是按照信息数据来源的不同分类的。（　　）

4. 目前入侵检测存在误报率和漏报率高的问题。（　　）

5. 异常入侵检测是以分析各种类型的攻击手段为基础的。（　　）

6. 误用入侵检测用来检测未知的入侵行为。（　　）

7. 入侵检测中的漏报是指异常而非入侵的活动被标记为入侵。（　　）

8. 基于网络的入侵检测系统，利用工作在混杂模式下的网卡监视分析网络数据。（　　）

9. 任何单位和个人在从计算机信息网络上下载程序、数据或者购置、维修、借入计算机设备时，不必进行计算机病毒检测。（　　）

二、单项选择题

1. 按照入侵检测分析的方法，可将 IDS 分为（　　）。

A．基于主机的 IDS 和基于网络的 IDS
B．异常入侵检测系统和误用入侵检测系统
C．集中式入侵检测系统和分布式入侵检测系统
D．基于浏览器的 IDS 和基于服务器的 IDS

2．一般来说，IDS 由三部分组成，分别是事件产生器、事件分析器和（　　）
A．控制单元　　B．检测单元
C．解释单元　　D．响应单元

3．入侵检测的基础是（　　），入侵检测的核心是（　　）。
A．信息收集　信息分析　　B．信息收集　告警与响应
C．信息分析　入侵防御　　D．信息收集　检测方法

4．信息分析有模式匹配、统计分析和完整性分析了种技术手段，其中（　　）用于事后分析。
A．模式匹配　　B．统计分析
C．信息收集　　D．完整性分析

5．（　　）系统是一种自动检测远程和本地主机安全性弱点的程序，通过远程检测目标主机上 TCP/IP 不同端口的服务，记录目标给予的回答。
A．入侵检测　　B．漏洞扫描
C．信息安全管理与审计　　D．入侵防御

6．异常入侵检测以（　　）作为比较的参考基准。
A．异常的行为特征轮廓　　B．正常的行为特征轮廓
C．日志记录　　D．审计记录

7．误用入侵检测依靠的一个假定是（　　）。
A．所有的入侵行为都是异常的
B．只有异常行为才有可能是入侵攻击行为
C．所有可能的入侵行为和手段都能够表达为一种模式或特征
D．正常行为和异常行为可以根据一定的阈值来加以区分

8．基于网络的 IDS 利用（　　）作为数据源。
A．审计记录　　B．日志记录
C．网络数据包　　D．加密数据

9．对网络层数据包进行过滤和控制的信息安全技术机制是（　　）。
A．防火墙　　B．IDS
C．漏洞扫描　　D．VPN

三、思考题

1．IDS 的工作模式可以分为几个步骤？分别是什么？

2．基于主机的 IDS 和基于网络的 IDS 的区别是什么？

3．简述防火墙对部署 IDS 的影响。

技能拓展

某企业的网络安装防火墙后，其拓扑结构如图 2-35 所示，按照各题要求填充空白区。

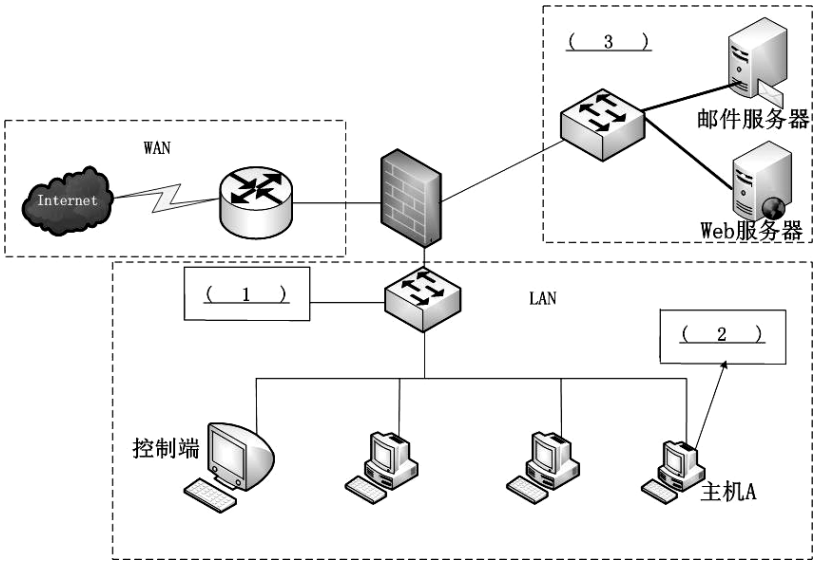

图 2-35　网络拓扑图

1．为图中标识的 3 中选择合适的名称（　　）。

A．DMZ 区　　B．堡垒区　　C．服务区　　D．安全区

2．为了实时检测安全威胁，图中标识的 1 可选择一种合适的安全设备（　　）。

A．防火墙　　B．基于网络的 IDS

C．防病毒网关　　D．基于主机的 IDS

3．LAN 区中主机 A 为 Windows Server 2003 操作系统，为了保证图中标识的 2 中能够正常、安全地运行，除了可以配置 Windows Server 2003 操作系统的注册表以外，为了整体提高主机 A 的安全性，还可以进行哪些方面的系统安全加固？（至少列举 5 点）