第7章　网络防御

罗文坚

主要内容

- 7.1 概述
- 7.2 防火墙
- 7.3 入侵检测系统
  - 7.3.1 入侵检测概述
  - 7.3.2 入侵检测系统分类
  - 7.3.3 入侵检测技术
  - 7.3.4 Snort系统
- 7.4 网络防御的新技术

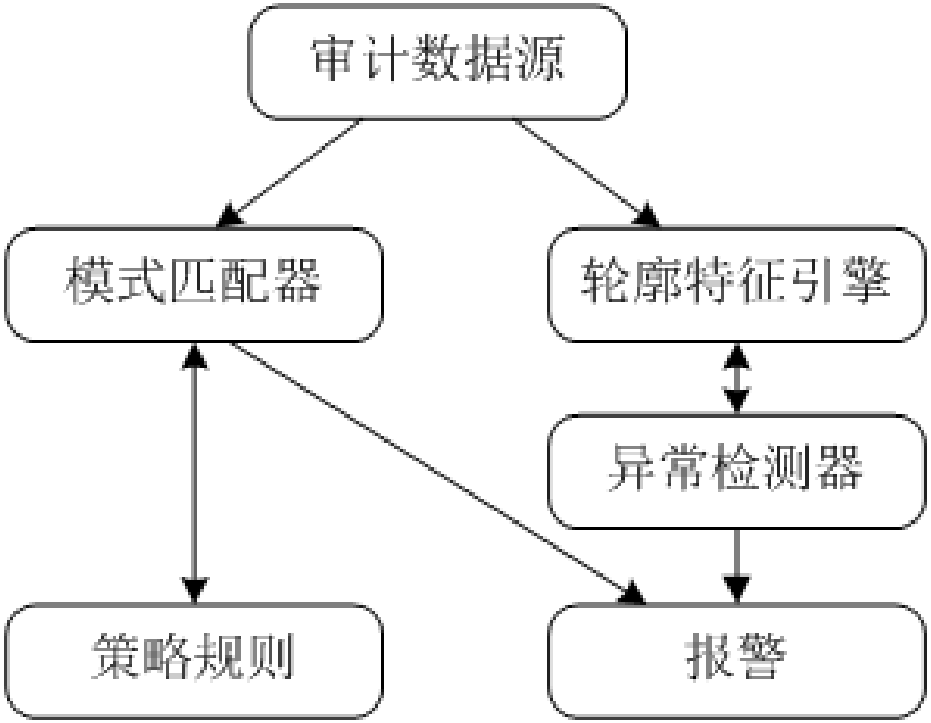
入侵检测系统

- IDS（Intrusion Detection System，入侵检测系统）
  - 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系统。

- 一般认为，防火墙属于静态防范措施，而入侵检测系统为动态防范措施，是对防火墙的有效补充。
  - 假如防火墙是一幢大楼的门禁，那么IDS就是这幢大楼里的监视系统。

入侵检测概述

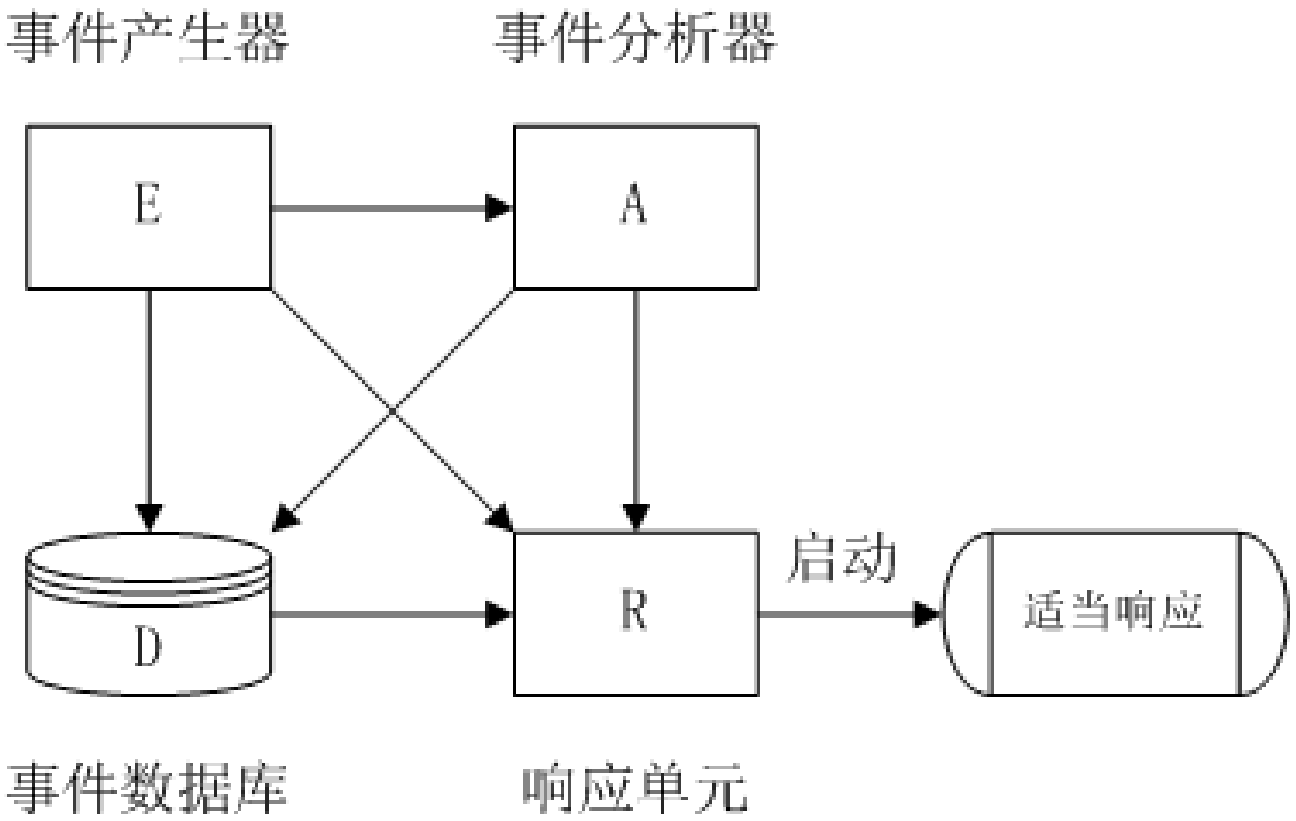
- 1980年， James P. Anderson，《Computer Security Threat Monitoring and Surveillance》，此技术报告被公认是开山之作。
- 1984-1986年，Dorothy Denning和 Peter Neumann，实时入侵检测系统模型，IDES (Intrusion Detection Expert System)。



CIDF通用模型

- IDWG（Intrusion Detection Working Group，IETF下属的研究机构）和CIDF（Common Intrusion Detection Framework，一个美国国防部赞助的开放组织）负责组织开展对IDS进行标准化和研究工作。

➢ CIDF模型：



IDS有关的重要概念

- 事件：当网络或主机遭到入侵或出现较重大变化时，称为发生安全事件，简称事件。
- 报警：当发生事件时，IDS通过某种方式及时通知管理员事件情况称为报警。
- 响应：当IDS报警后，网络管理员对事件及时作出处理称为响应。
- 误用：误用是指不正当使用计算机或网络，并构成对计算机安全或网络安全威胁的一类行为。
- 异常：对网络或主机的正常行为进行采样、分析，描述出正常的行为轮廓，建立行为模型，当网络或主机上出现偏离行为模型的事件时，称为异常。

IDS有关的重要概念

- 入侵特征：也称为攻击签名（Attack Signature）或攻击模式（Attack Patterns）。
  - 一般指对网络或主机的某种入侵攻击行为（误用行为）的事件过程进行分析提炼，形成可以分辨出该入侵攻击事件的特征关键字，这些特征关键字被称为入侵特征。

- 感应器：
  - 布置在网络或主机中用于收集网络信息或用户行为信息的软硬件，称为感应器。
  - 感应器应该布置在可以及时取得全面数据的关键点上，其性能直接决定IDS检测的准确率。

入侵检测系统的工作过程

- 信息收集：
  - 入侵检测的第一步是信息收集，收集内容包括系统和网络的数据及用户活动的状态和行为。信息收集工作一般由由放置在不同网段的感应器来收集网络中的数据信息（主要是数据包）和主机内感应器来收集该主机的信息。
- 信息分析：
  - 将收集到的有关系统和网络的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。当检测到某种入侵特征时，会通知控制台出现了安全事件。
- 结果处理：
  - 当控制台接到发生安全事件的通知，将产生报警，也可依据预先定义的相应措施进行联动响应。例如，重新配置路由器或防火墙、终止进程、切断连接、改变文件属性等。

IDS主要功能

1. 监测并分析用户、系统和网络的活动变化；
2. 核查系统配置和漏洞；
3. 评估系统关键资源和数据文件的完整性；
4. 识别已知的攻击行为；
5. 统计分析异常行为；
6. 操作系统日志管理，并识别违反安全策略的用户活动。

主要内容

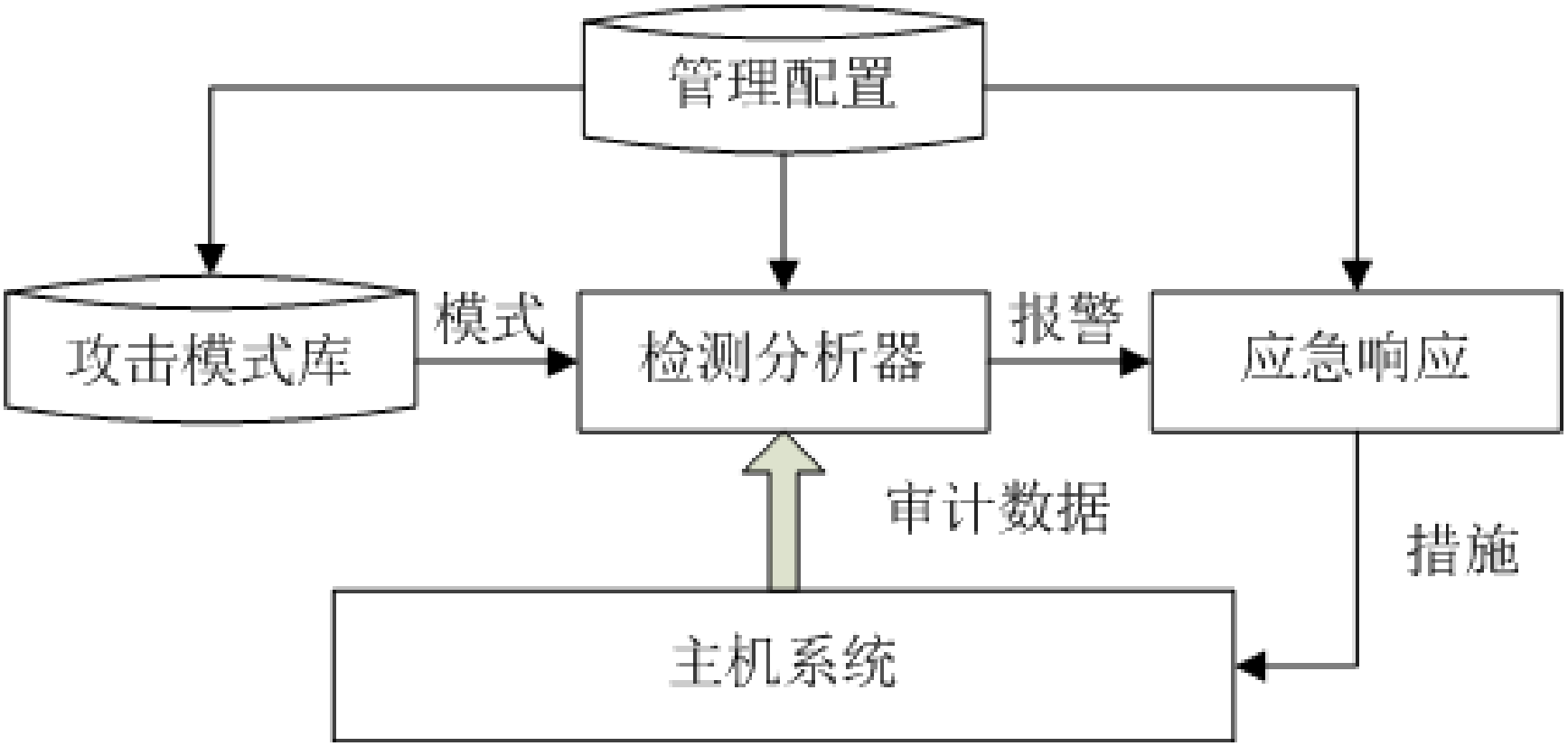
- 7.1 概述
- 7.2 防火墙
- 7.3 入侵检测系统
  - 7.3.1 入侵检测概述
  - 7.3.2 入侵检测系统分类
  - 7.3.3 入侵检测技术
  - 7.3.4 Snort系统
- 7.4 网络防御的新技术

入侵检测系统分类

- 以数据源为分类标准
  - 主机型入侵检测系统HIDS（Host-based Intrusion Detection System）
  - 网络型入侵检测系统NIDS（Network-based Intrusion Detection System）。

主机型入侵检测系统

- 数据来源主要是操作系统的事件日志、应用程序的事件日志、系统调用、端口调用和安全审计记录等。



主机型入侵检测系统

- HIDS只能用来检测该主机上发生的入侵行为，主要检测内部授权人员的误用以及成功避开传统的系统保护方法而渗透到网络内部的入侵活动，检测准确性高。

- 在检测到入侵行为后，可及时与操作系统协同阻止入侵行为的继续。

- HIDS的缺点：
  1. 与操作系统平台相关，可移植性差；
  2. 需要在每个被检测主机上安装入侵检测系统，维护较复杂；
  3. 难以检测针对网络的攻击，如消耗网络资源的DoS攻击、端口扫描等。

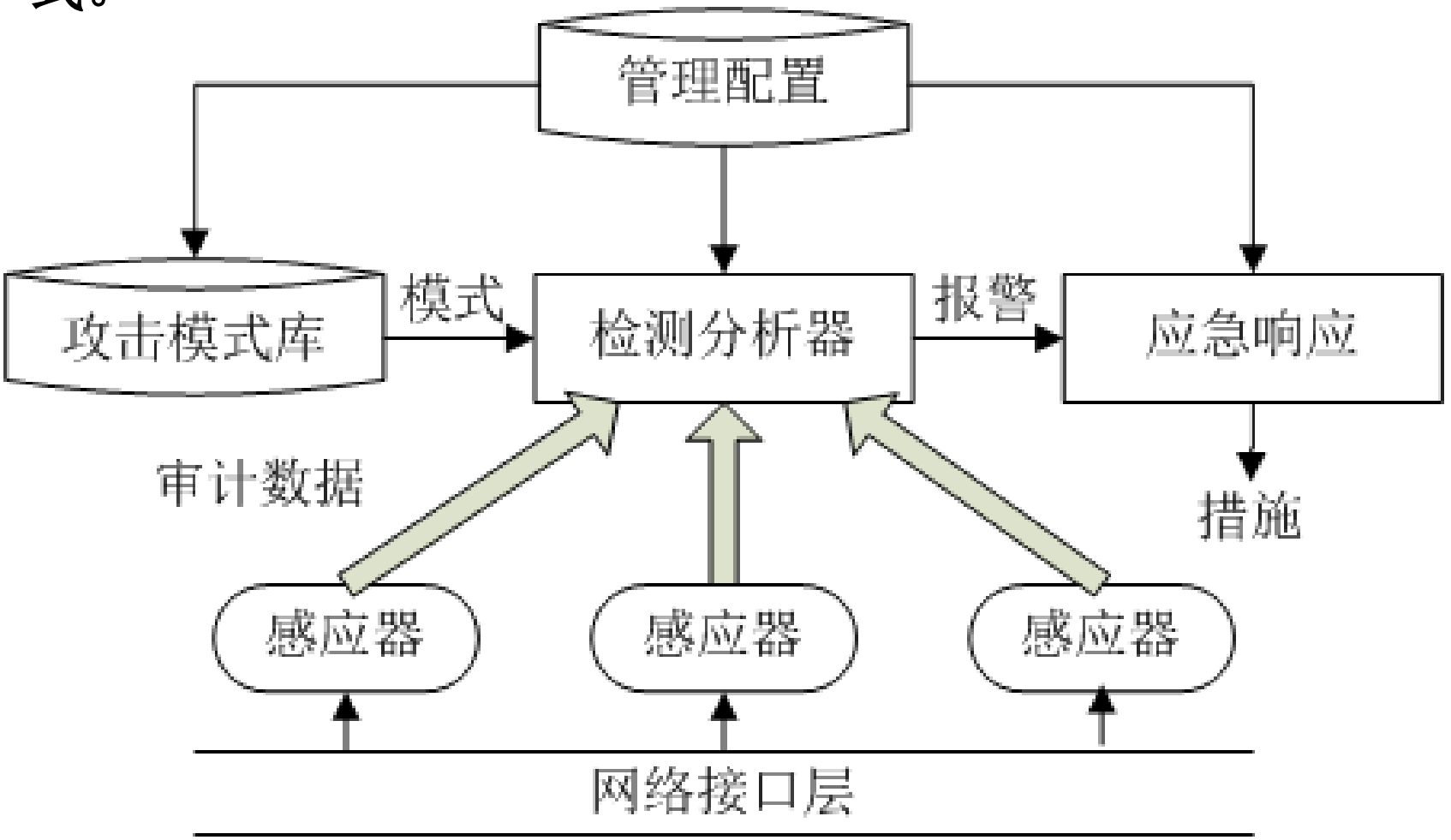
主机型入侵检测系统

- 随着针对应用层的攻击手段增多以及加密环境应用的普及，HIDS的优势逐渐明显。

- HIDS优点主要包括：
  1. 性价比较高，不需要增加专门的硬件平台，当主机数量较少时性价比尤其突出；
  2. 准确率高，HIDS主要监测用户在系统中的行为活动，如对敏感文件、目录、程序或端口的访问，这些行为能够准确地反映系统实时的状态，便于区分正常的行为和非法的行为；
  3. 对流量不敏感，不会因为网络流量的增加而丢掉对网络行为的监视；
  4. 适合加密环境下的入侵检测。

网络型入侵检测系统

- NIDS主要通过部署在网络关键位置上的感应器（多数为计算机）捕获网上的数据包，分析其是否具有已知的入侵特征模式。



网络型入侵检测系统

- **NIDS的优点主要包括：**
  1. 对用户透明，隐蔽性好，使用简便，不容易遭受来自网络上的攻击；
  2. 与被检测的系统平台无关；
  3. 利用独立的计算机完成检测工作，不会给运行关键业务的主机带来负载上的增加；
  4. 攻击者不易转移证据。
- **NIDS的缺点主要包括：**
  1. 无法检测到来自网络内部的攻击，以及内部合法用户的误用行为；
  2. 无法分析加密的数据报文；
  3. 需要对所有的网络报文进行采集分析，主机的负荷较大，且易受DoS攻击。

HIDS和NIDS

- HIDS和NIDS具有互补性。
  - HIDS能够更加精确地监视主机中的各种活动，适应特殊环境，如加密环境。
  - NIDS能够客观地反映网络活动，特别是能够监视到主机系统审计的盲区。

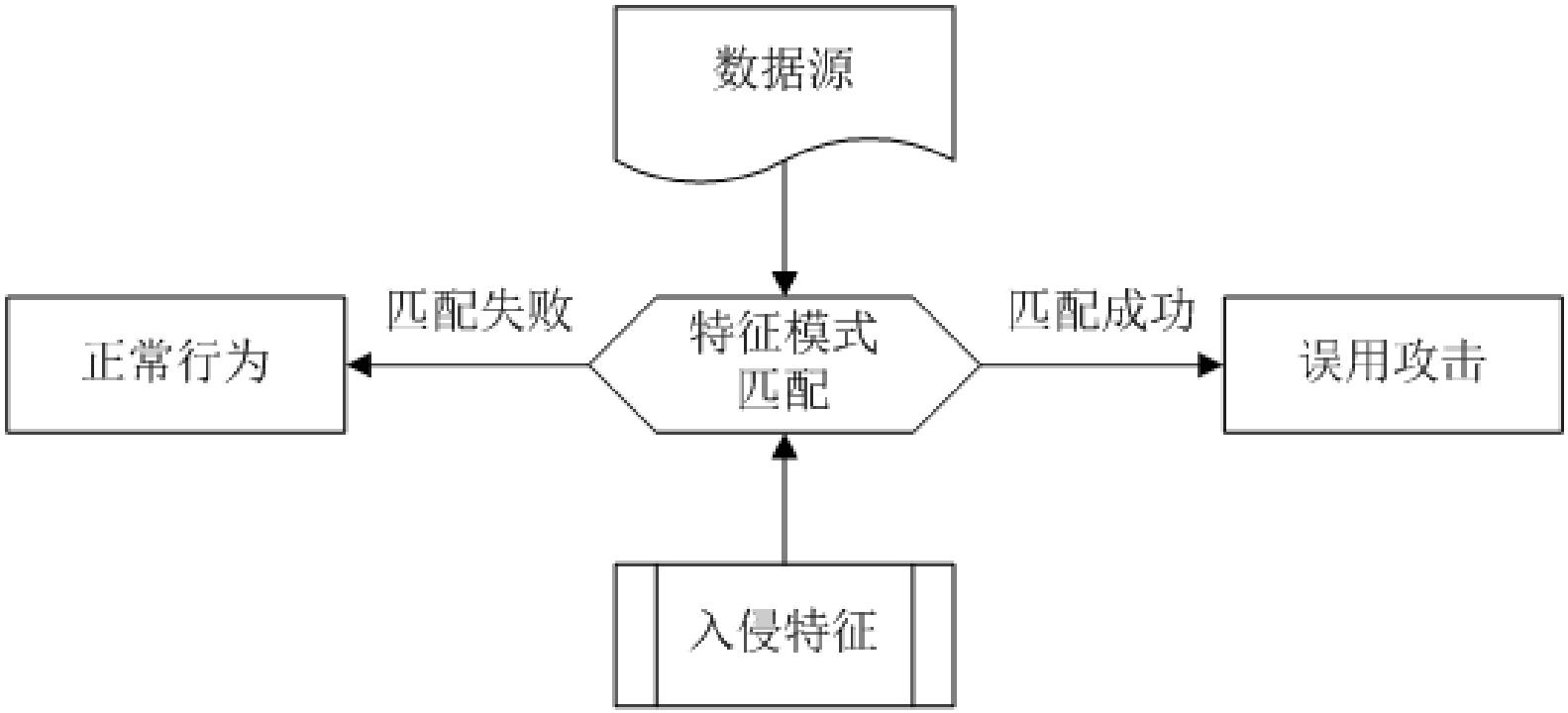
- 因此，一些入侵检测系统采用了NIDS和HIDS的混合形式，来提高对内部网络的保护力度。

入侵检测系统分类

- 以检测技术为分类标准
  - 基于误用检测（Misuse Detection）的IDS
  - 基于异常检测（Anomaly Detection）的IDS

基于误用检测的IDS

- 误用检测是事先定义出已知的入侵行为的入侵特征，将实际环境中的数据与之匹配，根据匹配程度来判断是否发生了入侵攻击行为。



误用检测模型

基于误用检测的IDS

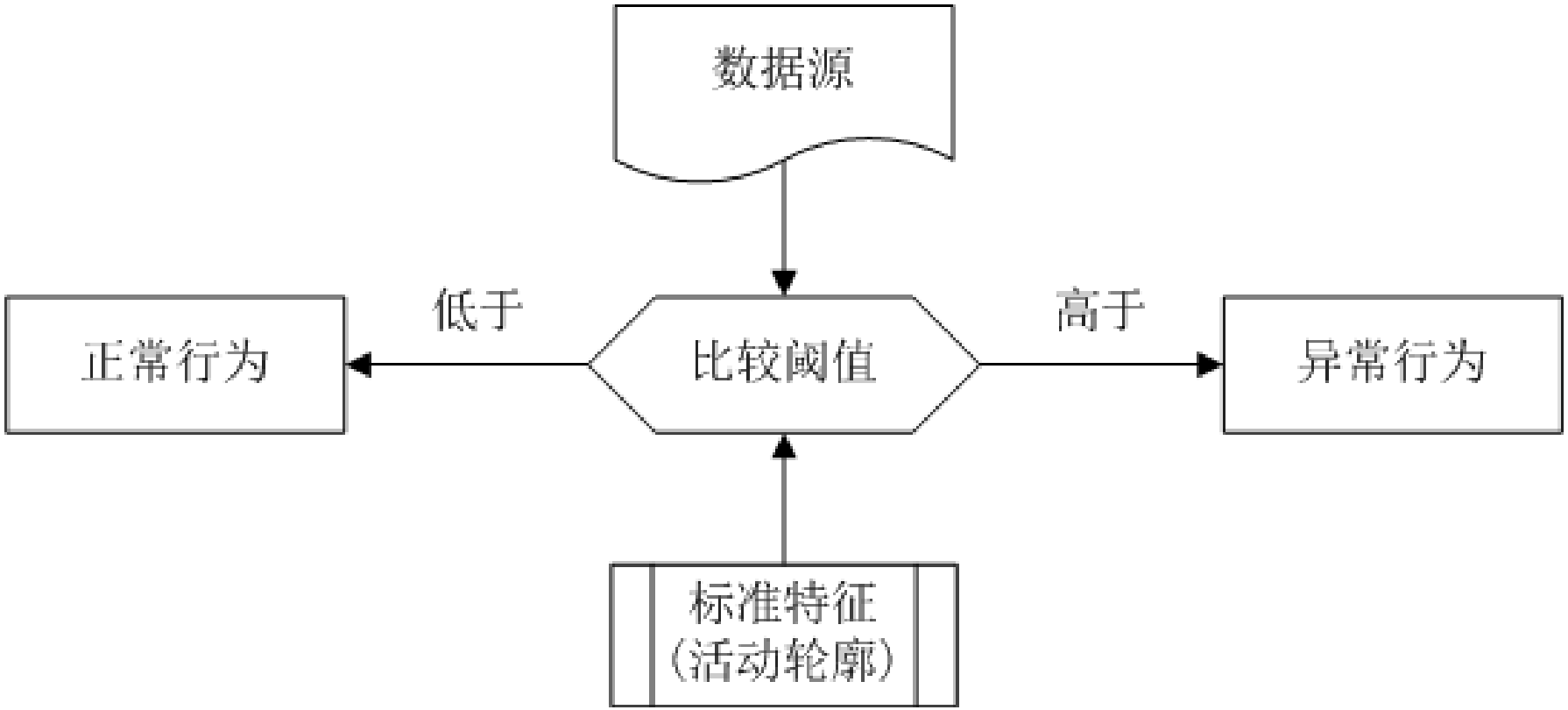
- 大部分入侵行为都是利用已知的系统脆弱性。通过分析入侵过程的特征、条件、顺序以及事件间的关系，可以具体描述入侵行为的特征信息。
  - 由于依据具体特征库进行判断，所以检测准确率很高。

- 误用检测有时也被称为特征分析（Signature Analysis）或基于知识的检测（Knowledge-based Detection）。

- 误用检测的主要缺陷：
  - 首先，检测范围受已有知识的局限，无法检测未知的攻击类型；
  - 其次，将具体入侵手段抽象成知识具有一定困难，而且建立的入侵特征库需要不断更新维护。

基于异常检测的IDS

- 异常检测是根据使用者的行为或资源使用状况的程度与正常状态下的标准特征（活动轮廓）之间的偏差来判断是否遭到入侵。如果偏差高于阈值，则发生异常。



基于异常检测的IDS

- 异常检测不依赖于某个具体行为是否出现，通用性较强。
- 但是，对基于异常检测的IDS来说，得到正常行为或状态的标准特征以及确定阈值具有较大的难度。
  - 首先，不可能对整个系统内的所有用户行为进行全面的描述，而且每个用户的行为是经常改变的。
  - 其次，资源使用情况也可能由于某种特定因素发生较大的变化。
- 因此，基于异常检测的IDS往往漏报率低，但误报率高。
- 在实际应用中，往往将误用检测和异常检测项结合，以达到更好的效果。

主要内容

- 7.1 概述
- 7.2 防火墙
- 7.3 入侵检测系统
  - 7.3.1 入侵检测概述
  - 7.3.2 入侵检测系统分类
  - 7.3.3 入侵检测技术
  - 7.3.4 Snort系统
- 7.4 网络防御的新技术

入侵检测技术

- 入侵检测技术研究具有综合性、多领域性的特点，技术种类繁多，涉及到许多相关学科。

- 从以下四个方面介绍入侵检测的主要技术方法。
  - 误用检测
  - 异常检测
  - 诱骗
  - 响应

误用检测技术

- 误用检测是一直比较成熟的入侵检测技术，目前大多数入侵检测系统都是基于误用检测的思想来设计实现的。

- 实现误用检测的方法主要包括：
  1. 专家系统；
  2. 特征分析；
  3. 模型推理；
  4. 状态转换分析；
  5. 完整性校验等。

误用检测技术

1. 专家系统：

- 安全专家将入侵检测方面的知识，以规则结构的形式表示出来，形成专家知识库。
- 规则结构一般采用条件判断形式，即if-then结构，if部分是构成入侵所要求的条件，then部分是发现入侵后采取的相应措施。
- 专家系统的主要问题是全面性问题和效率问题。
- 全面性问题是指难以取得专家的全部知识，同时专家的知识也很难具有充分的全面性。
- 效率问题是所需处理的数据量可能很大，逐一判断效率低。

误用检测技术

2. 特征分析：

- 目前商业软件主要采用的方法，也称为模式匹配。
- 模式匹配，就是将收集到的信息与已知的误用模式数据库进行比较，从而发现违背安全策略的行为。
- 该过程可以很简单（如通过字符串匹配以寻找一个简单的条目），也可以很复杂（如利用正规的数学表达式来表示安全状态的变化）。
- 该方法的优点是只需收集相关的数据集合，显著减少系统负担，技术成熟。
- 该方法的缺点是，需要不断地升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

误用检测技术

3. 状态转换分析
   - 将入侵过程看做一个行为序列，该行为序列导致系统从初始状态转入被入侵状态。
   - 需要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。

4. 模型推理
   - 通过建立误用脚本模型，根据样本来推理以判断是否发生了误用行为。

5. 完整性分析
   - 主要关注某些特定对象是否被更改，如重要的日志、文件以及目录等内容。
   - 完整性分析利用消息摘要函数等方法，能够识别特定对象极其微小的变化。

异常检测技术

- 异常检测是一种与系统相对无关、通用性较强的入侵检测技术。异常检测的思想最早由Denning在IDES系统中提出，即通过监视系统审计记录上系统使用的异常情况，可以检测出违反安全政策的事件。

- 通常异常检测都与一些数学分析方法相结合，但存在着误报率较高的问题。

- 异常检测主要针对用户行为数据、系统资源使用情况进行分析判断。

- 常见的异常检测方法主要包括统计分析、预测模型、系统调用监测以及基于人工智能的异常检测技术等。

异常检测技术

- 统计分析
  - 检测系统维护一个由行为模式组成的规则知识库，每个模式采用一系列系统度量来表示特定用户的正常行为。
- 预测模型
  - 使用动态规则集合来检测入侵，这些规则根据所观察事件的序列关系和局部特性归纳产生序列模式。
- 系统调用监测
  - 监视由特权程序进行系统调用的方法来进行异常检测。
- 基于人工智能的异常检测技术
  - 这些人工智能技术主要包括数据挖掘、神经网络/深度学习、模糊证据理论等。

入侵诱骗技术

- 入侵诱骗是指用通过伪装成具有吸引力的网络主机来吸引攻击者，同时对攻击者的各种攻击行为进行分析，进而找到有效的应对方法。
- 入侵诱骗也具有通过吸引攻击者，从而保护重要的网络服务系统的目的。

- 常见的入侵诱骗技术主要有蜜罐（Honeypot）技术和蜜网（Honeynet）技术等。
  - 蜜罐是一种安全资源，其价值在于被扫描、攻击和攻陷。所有流入或流出蜜罐的网络流量都可能预示了扫描、攻击和攻陷。
  - 蜜网是蜜罐技术上发展起来的一个新概念，又称为诱捕网络。

入侵诱骗技术

- 蜜罐的核心价值在于对这些攻击活动进行监视、检测和分析。

- 蜜罐有两种形式：
  - 一种是真实系统蜜罐，实际上就是一个真实运行的系统，并带有可入侵的漏洞，它所记录下的入侵信息往往是最真实的。
  - 另一种是伪装系统蜜罐，它是运行于真实系统基础上的仿真程序，它可以伪造出各种“系统漏洞”。入侵这样的“漏洞”，只能是在一个程序框架了打转。即使成功“渗透”，对系统本身也没有损害。

- 利用蜜罐技术可以迷惑入侵者，从而保护真实的服务器；同时，也可以诱捕网络罪犯。

入侵诱骗技术

- 蜜网技术实质上是一类高交互蜜罐技术，其主要目的是收集黑客的攻击信息。

- 与传统蜜罐技术的差异：蜜网构成了一个黑客诱捕网络体系架构，该架构包含了一个或多个蜜罐，同时保证了网络的高度可控性，并提供多种工具来完成对攻击信息的采集和分析。

- 蜜网可以通过采用虚拟操作系统软件来实现，如VMWare等，这样可以在单一主机上实现蜜网的体系架构，即虚拟蜜网。
  - 虚拟蜜网的引入使得架设蜜网的代价大幅降低，较容易部署和管理，但同时也带来了更大的风险。
  - 黑客有可能识别出虚拟操作系统软件，并可能攻破虚拟操作系统，从而获得对整个虚拟蜜网甚至真实主机的控制权。

响应技术

- 入侵检测系统的响应技术可以分为主动响应和被动响应。
- 主动响应是系统自动阻断攻击过程或以其他方式影响攻击过程。
- 被动响应是报告和记录发生的事件。
  - 被动响应无法阻止入侵行为，只起到缩短系统管理人员反应时间的作用。

响应技术

- 主动响应的一种表现形式就是采取反击行动。
  - 但是，一直以来没有成为常用的响应形式，主要是有客观原因。
  - 因为入侵者的常用攻击方法是利用一个被黑掉的系统作为攻击的平台，而且反击行动也可能会涉及法律法规等问题。
  - 因此，当检测到入侵时，一般是利用防火墙和网关阻止来自入侵IP地址的数据包，也可以采用网络对话的方式阻断网络连接，即向入侵者的计算机发送TCP的RESET包，或发送ICMP的Destination Unreachable数据包，或者求助于被入侵主机的网络管理员。

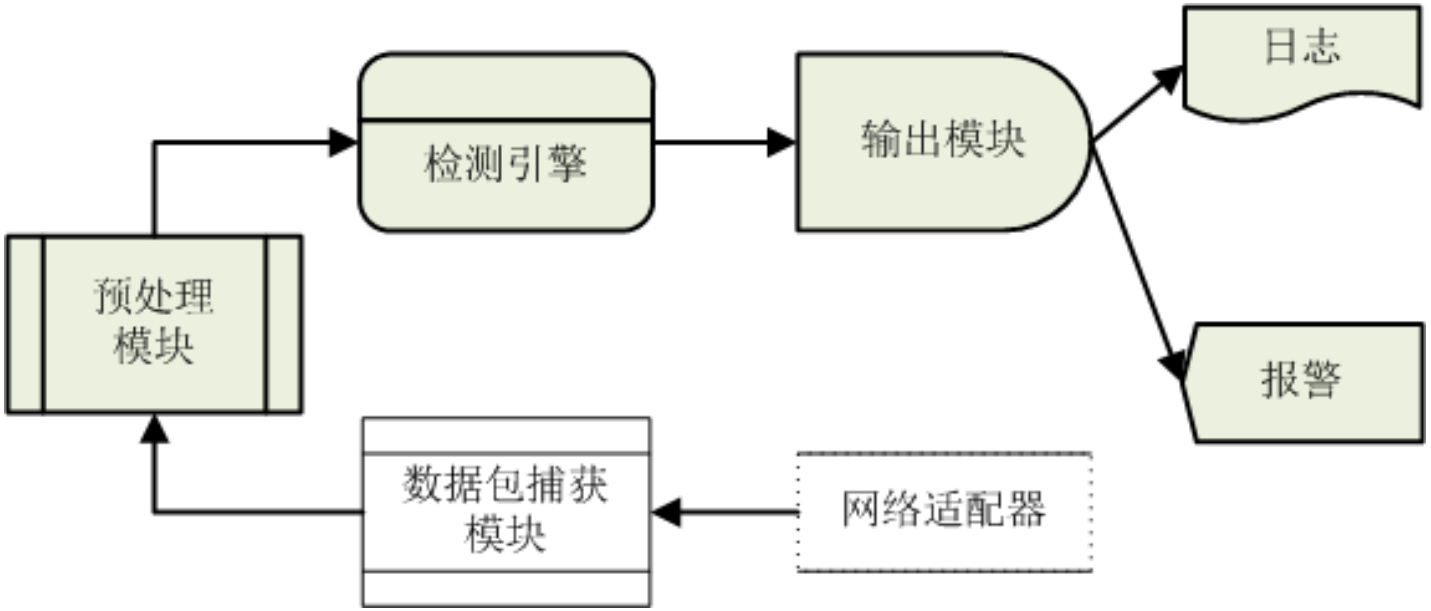
- 修正系统环境也是主动响应的一种手段，主要是提高分析引擎对特定模式的敏感度，增加监视范围，更好地收集信息，以便堵住导致入侵发生的漏洞，目前被广泛应用。

主要内容

- 7.1 概述
- 7.2 防火墙
- 7.3 入侵检测系统
  - 7.3.1 入侵检测概述
  - 7.3.2 入侵检测系统分类
  - 7.3.3 入侵检测技术
  - 7.3.4 Snort系统
- 7.4 网络防御的新技术

Snort系统

- Snort入侵检测系统是一个开放源代码的轻量级网络入侵检测系统。
- Snort遵循CIDF模型，使用误用检测的方法来识别发现违反系统和网络安全策略的网络行为。
- Snort系统包括数据包捕获模块、预处理模块、检测引擎和输出模块四部分组。



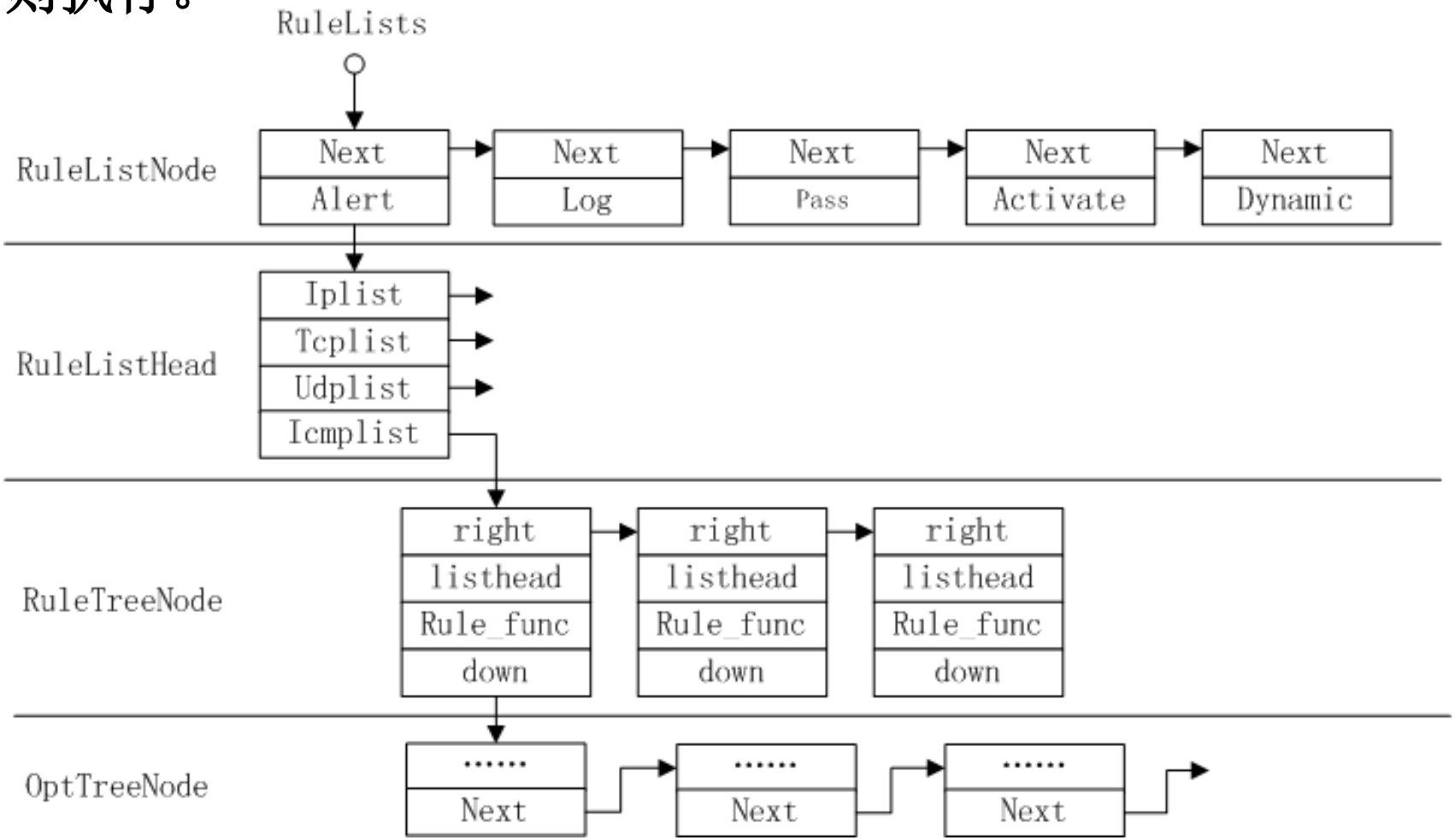
Snort检测引擎模块

- 检测引擎是Snort的核心部件，主要功能是规则分析和特征检测。
  - 当数据包从预处理送过来后，检测引擎依据预先设置的规则检查数据包，一旦发现数据包中的内容和某条规则相匹配，就通知输出模块进行报警。

- Snort将所有已知的入侵行为以规则的形式存放在规则库中，并以三维链表结构进行组织。
- 每一条规则由规则头和规则选项两部分组成。
  - 规则头对应于规则树节点（Rule Tree Node，RTN），包含规则动作选项、数据包类型、源地址、源端口、目的地址、目的端口、数据流动方向等内容。
  - 规则选项对应于规则选项节点（Optional Tree Node, OTN），包含报警信息和匹配内容等选项。

Snort规则库

- **Activate：** 报警并且激活另一条dynamic规则。**Dynamic：** 保持空闲直到被一条activate规则激活，被激活后就作为一条log规则执行。



Snort规则例子

- **Alert tcp any any->10.1.1.0/24 80(content:"/cgi-bin/phf" ; msg:"PHF probe!";)**
- 在这个规则中，括号左面为规则头，括号中间的部分为规则选项，规则选项中冒号前的部分为选项关键字**(Option Keyword)**。
- 规则头由规则行为、协议字段、地址和端口信息**3**部分组成。

- 选项关键字**content**是在数据包负载中搜索的模式；**msg**表示打印一条警告信息到警告或日志中；

- 这条规则的含义是：当在任何发往**10.1.1.0/24**子网主机**80**端口的**tcp**数据包负载中，如果发现子串“**/cgi-bin/phf**”，则此数据包为攻击数据包，**Snort**将报警并输出“**PHF probe!**”，表示此数据包为对本地网络**Web**服务器的**PHF**服务的探测攻击。

主要内容

- 7.1 概述
- 7.2 防火墙
- 7.3 入侵检测系统
- 7.4 网络防御的新技术

网络防御的新技术

- 主要介绍：
  - VLAN技术
  - IPS（入侵防御系统）
  - IMS（入侵管理系统）
  - 云安全

VLAN技术

- VLAN（Virtual Local Area Network）的中文名为虚拟局域网。
- 1999年IEEE颁布了用于实现VLAN标准化的802.1Q协议标准草案。将VLAN定义为：
  - VLAN是由一些局域网网段构成的与物理位置无关的逻辑组，而每个逻辑组中的成员具有某些相同的需求。
- VLAN是用户和网络资源的逻辑组合，是局域网给用户提供的一种服务，而并不是一种新型局域网。

- 每一个VLAN的帧都有一个明确的标识符，指明发送这个帧的工作站属于哪一个VLAN。

- 由于VLAN是从逻辑上划分，所以同一个VLAN内的各个工作站可以在不同物理LAN网段。

VLAN的划分方式

- VLAN的划分可依据不同原则，常见的方式：
  - 基于端口、基于MAC地址和基于IP子网等几种方法。

- 基于端口的VLAN划分
  - 这种划分是把一个或多个交换机上的几个端口划分一个逻辑组，这是最简单、最有效的划分方法。
- 基于MAC地址的VLAN划分
  - 按MAC地址把一些节点划分为一个逻辑子网，使得网络节点不会因为地理位置的变化而改变其所属的网络，从而解决了网络节点的变更问题。
- 基于IP子网的VLAN划分
  - 基于子网的VLAN，则是通过所连计算机的IP地址，来决定其所属的VLAN。

VLAN的安全性

- 广播风暴防范
  - VLAN逻辑分段和物理网络分段不同，同一VLAN处于相同的广播域，通过VLAN的划分可以有效地阻隔网络广播，缩小广播域，控制广播风暴。
- 信息隔离
  - 同一个VLAN内的计算机之间可以直接通信，不同VLAN间的通信则要通过路由器进行路由选择、转发，这样就能隔离基于广播的信息，防止非法访问。
- 控制IP地址盗用
  - 该VLAN内任何一台计算机的IP地址都必须在分配给该VLAN的IP地址范围内，否则将无法通过路由器的审核，也就不能进行通信。

VLAN存在的问题

- VLAN容易遭受欺骗攻击和硬件依赖性问题。
- 欺骗攻击主要包括MAC地址欺骗、ARP欺骗以及IP盗用转网等问题；
- 硬件依赖是指VLAN的组建要使用交换机，并且不同主机之间的信息交换要经过交换机。
  - 因此，VLAN的安全性在很大程度上依赖于所使用的交换机，以及对交换机的配置。

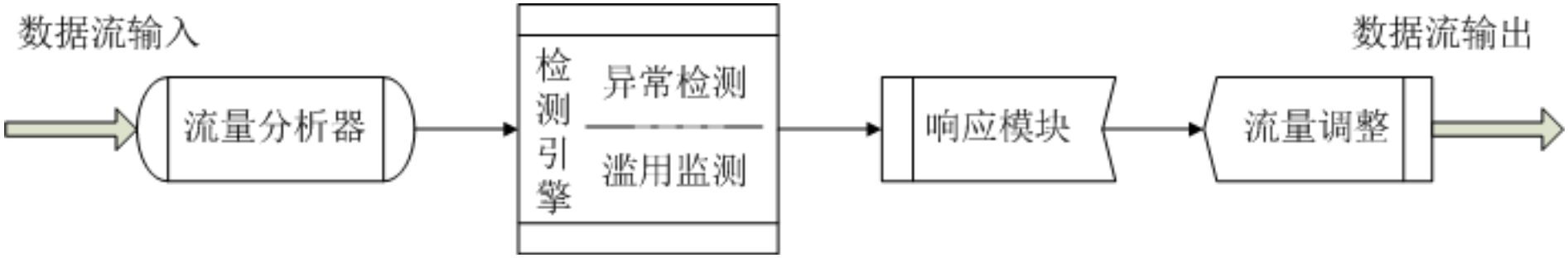
IPS

- 入侵防御系统IPS（Intrusion Prevention System）是在防火墙和IDS基础上发展起来的，但不是IDS的升级产品。

- IPS采用串联的方式部署在内、外网络之间的关键路径上，其工作方式是采用基于包过滤的存储转发机制。

- IPS技术可以深度感知并检查流经的网络流量，对恶意数据包进行丢弃以阻断攻击，保护网络带宽资源。

IPS结构



- **流量分析器：**截获数据包并处理异常情况，执行类似于防火墙的访问控制。
- **检测引擎：**一般基于异常检测模型和误用检测模型，识别不同属性的攻击。
- **响应模块：**丢弃数据包、中止会话、修改防火墙规则、报警、日志等。
- **流量调整器：**流量分类和流量优化，设置不同优先级。

IPS与IDS相比的优势

1. 具备检测和防御功能：IDS只是检测和报警，IPS可以做到检测和防御兼顾。

2. 可检测到IDS检测不到的攻击行为：IPS是在应用层的内容检测基础上，加上主动响应和过滤功能，填补了网络安全产品线的基于内容的安全检查的空白。

3. 黑客较难破坏入侵攻击数据：IPS在检测攻击行为时具有实时性，因此可在入侵时予以检测防御，避免入侵攻击行为记录被破坏。

4. 具有双向检测防御功能：IPS可以对内网和外网之间的两个方向的攻击入侵行为做到检测和防御。

IPS面临的问题

- 作为串联接入网络的IPS所面临的最大问题是处理速度必须与数千兆或者更大容量的网络流量保持同步，否则成为网络瓶颈。

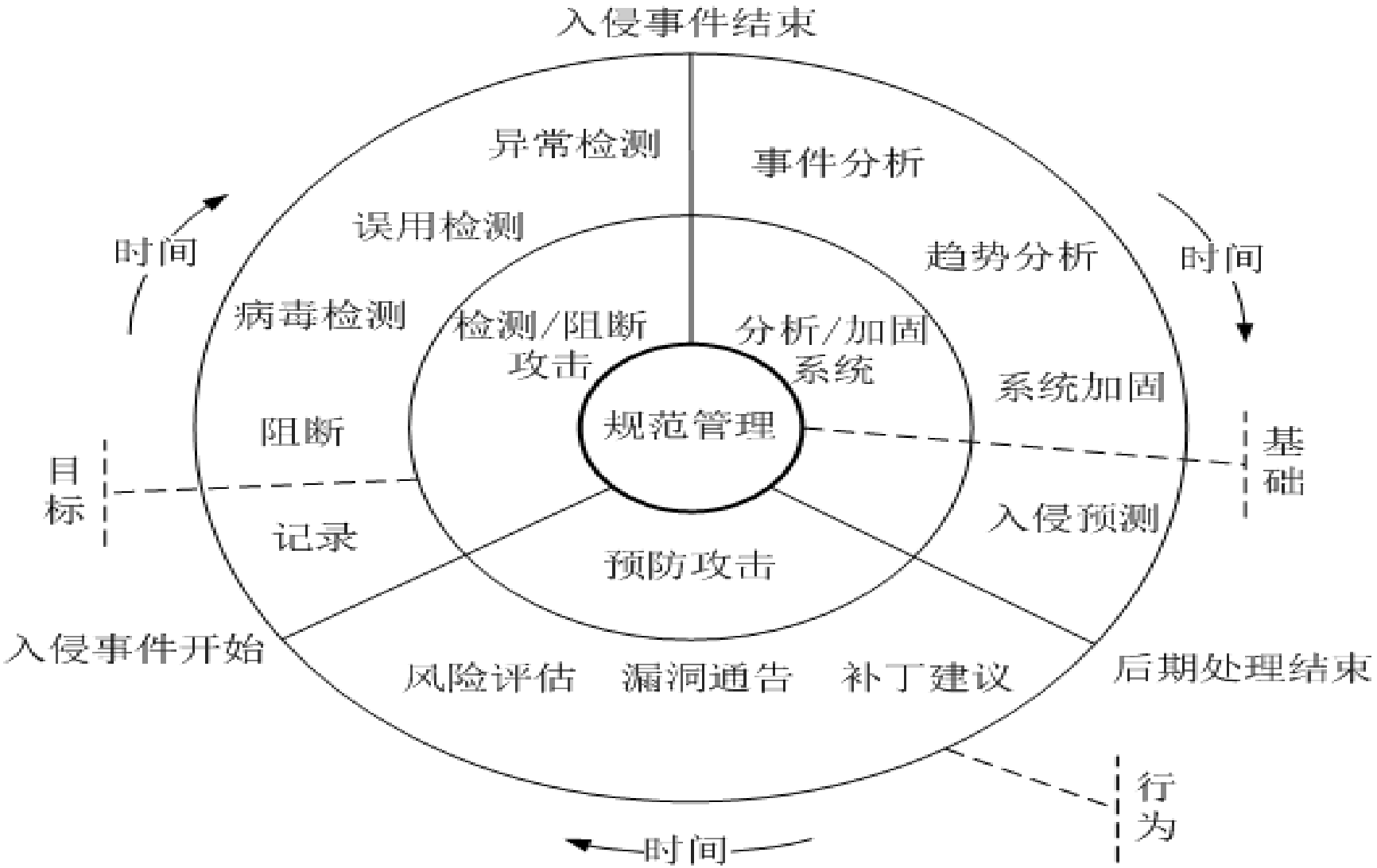
- 因此，IPS必须具有高性能、高可靠性、高安全性。

IMS

- 入侵管理系统IMS（Intrusion Management System）是一个针对整个入侵过程进行统一管理的安全服务系统。
  - 在入侵行为发生前，IMS要考虑网络中存在什么漏洞，判断可能出现的攻击行为和面临的入侵危险；
  - 在入侵行为发生时或即将发生时，IMS不仅要检测出入侵攻击行为，还要进行阻断处理，终止入侵行为；
  - 在入侵行为发生后，IMS要进行深层次的入侵行为分析，通过关联分析，来判断是否还存在下一次入侵攻击的可能性。

- 实际上，IMS应该是一个融合了多种安全防御技术的管理系统。

IMS模型



IMS模型示意图

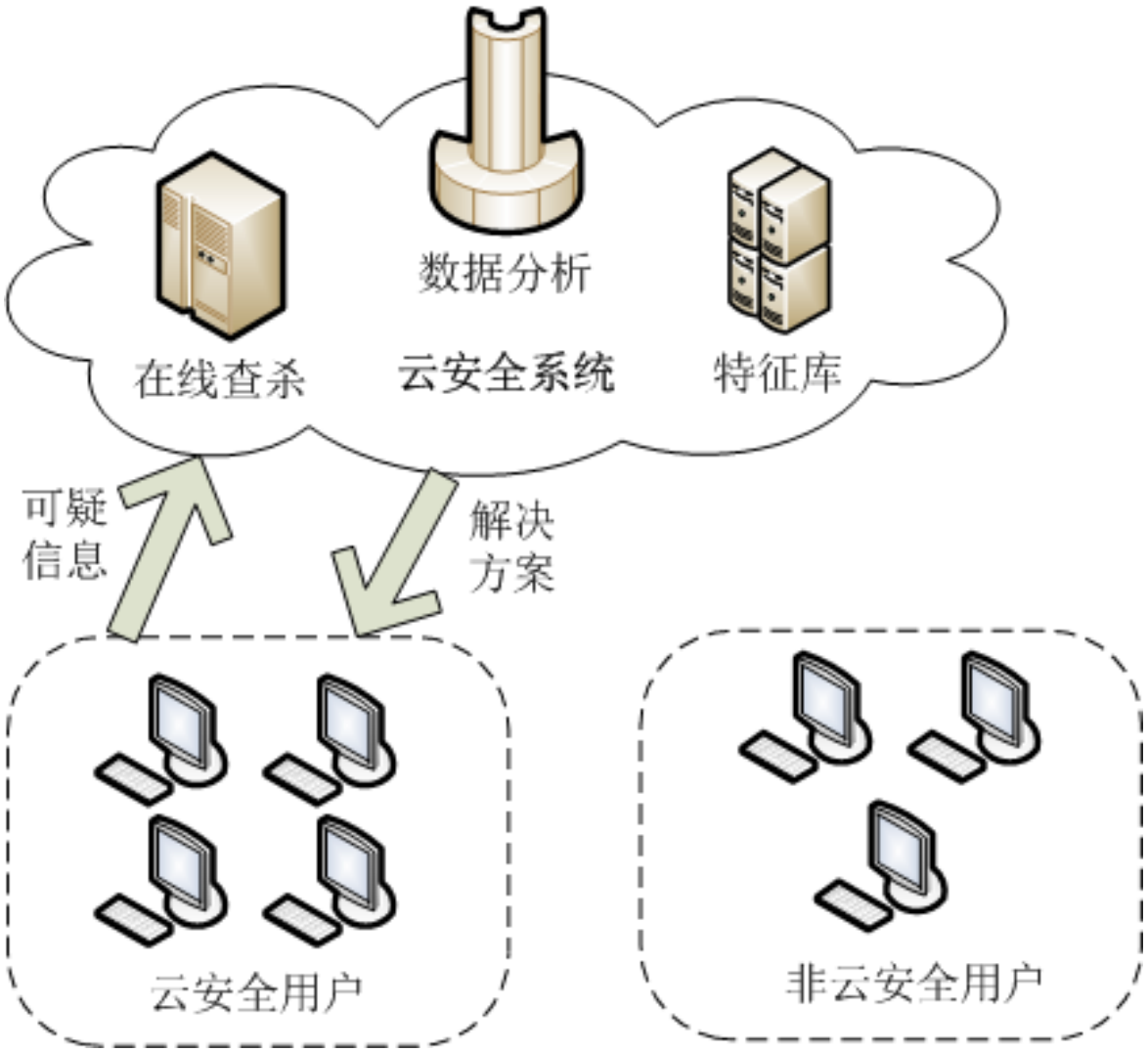
云安全

- “云”是一种新兴技术，云计算（Cloud Compute）、云存储（Cloud Storage）及云安全（Cloud Security）也随之相继产生。

- 最早受IBM、微软、Google等巨头追捧的“云计算”模式，是将计算资源放置在网络中，供许多终端设备来使用，其关键是分布处理、并行处理以及网格计算。云可以理解为网络中的所有可计算、可共享的资源，这是个共享资源的概念。

- 云安全是通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，传送到Server端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。
- 目前，云安全也被称为云杀毒，主要针对木马和病毒。

云安全示意图



云安全的特点

- 云安全更加强调主动和实时，将互联网打造成为一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。

- 与传统信息安全模式相比，云安全具有如下特点：
  - 快速感知，捕获新的威胁。与传统信息安全模式“一个人战斗”相比，云安全的客户数据中心凝聚了互联网的力量，整合了所有可能参与的人，效率大大提高。
  - 云安全的客户端具有更专业的感知能力。

云安全存在的问题

1. 需要海量的客户端
   - 只有拥有海量的客户端，才能对互联网上出现的病毒、木马、挂马网站有最灵敏的感知能力，在第一时间做出反应。

2. 需要专业的反病毒技术和经验
   - 如果没有反病毒技术和经验的积累，无法实现“云安全”系统及时处理处理海量的上报信息，并将处理结果共享给云安全系统的每个成员。

3. 需要大量的资金和技术投入

4. 开放的系统
   - 真正的云安全系统应该满足云的原始定义，即资源共享。

作业

1. 习题2（6）：误用检测和异常检测有什么区别？
2. 习题2（7）：什么是CIDF模型，包含哪些内容？
3. 习题3（1）：有人说，“防火墙的包过滤技术发展到应用层，就可以取代入侵检测系统。”你认为正确与否，为什么？