中山大學
SUN YAT-SEN UNIVERSITY

Module II. Internet Security

Chapter 7
IDS & IPS

Web Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- **7.1 Introduction to IDS**
  - Threats to Computer System
  - Process of Intrusions
  - What Is Intrusion Detection
  - Methods of Intrusion Detection
- **7.2 Framework of IDS**
  - Basic Structure of IDS
  - Host-Based IDS (HIDS)
  - Network-Based IDS (NIDS)
  - HIDS vs. NIDS
- **7.3 Introduction to IPS**
  - The Need of IPS
  - Security Capabilities
  - Types of IPS
  - IPS vs. IDS

7.1 Introduction to IDS

7.1.1 Threats to Computer System

- DoS
- Spoofing
- Eavesdrop
- Password Cracking
- Trojan
- Others： Buffer Overflow …

7.1 Introduction to IDS

7.1.1 Threats to Computer System

❑ DoS

- 服务请求超载：攻击者在短时间内向目标服务器发送大量的特定服务请求，服务器无法及时处理其它正常报文。
- SYN 泛洪：攻击者利用 TCP 的3次握手机制，在短时间内向目标服务器发送大量的半开连接报文 (只发送初始的SYN/ACK 报文而不发送最后的 ACK 报文)，目标服务器为这些恶意的连接保留资源，等待最后的确认报文。目标服务器在短时间内耗尽系统资源，无法对真正的连接请求作出响应。
- 报文超载：攻击者向目标主机发送的大量响应报文 (如 ICMP 回应请求报文)，使目标主机无法及时处理其它正常报文。

7.1 Introduction to IDS

7.1.1 Threats to Computer System

❑ Spoofing

- IP 地址欺骗：攻击者将其数据包的源 IP 地址伪装成合法用户的 IP 地址，骗取网络安全设备的信任。
- 路由欺骗：攻击者利用协议特性伪造或修改路由表，包括：把构造的 ICMP 重定向报文发给目标主机，目标主机因此修改路由表，将报文按照攻击者设定的路由发往不可控制的网络；利用 RIP (Route Information Protocol) 广播错误的路由信息，使目标网络构建错误的路由表。
- DNS 欺骗：攻击者先于 DNS 服务器向目标主机返回一个伪造的响应报文，目标主机因此连接到攻击者设定的服务器上。

7.1 Introduction to IDS

7.1.1 Threats to Computer System

- **Eavesdrop**
  - 攻击者抓取并分析网络中的数据流量 (比如 IP 包)，从而获得目标网络的拓扑结构、用户的帐号密码等信息。大多数网络协议是开放的，将网卡配制成混杂模式，可以获得整个子网上传递的明文信息。
- **Password Cracking**
  - 帐户/密码模式仍然是目前最常用的认证方式。面对很多针对密码的破解方法 (比如根据用户习惯的字典攻击法)，用户在密码的保密性与复杂性方面往往训练不够。
    - ✧ 随着计算设备的处理速度不断加快，原来被认为安全的密码也存在被暴力破解的可能性。

7.1 Introduction to IDS

7.1.1 Threats to Computer System

- **Trojan**
  - 木马是目前计算机网络面临的最大威胁。攻击者利用各种欺骗手段将木马程序植入目标主机，而后通过木马程序的运行在用户系统中开辟后门，将用户的重要信息传递到其指定的服务器上。
- **Buffer Overflow**
  - 程序向缓冲区内填充数据时超出缓冲区本身的容量，溢出的数据将覆盖在合法数据上。理想的情况是由程序检查数据长度并不允许输入超过缓冲区长度的字符，但是绝大多数系统都会假设数据长度总是与所分配的储存空间相匹配，这就形成了缓冲区溢出的脆弱性。

7.1 Introduction to IDS

7.1.2 Process of Intrusions

❑ Three Steps of Intrusion

- Information of the targets
  - ✧ OS: Windows or Linux?
  - ✧ Software version
  - ✧ Active net service
    - ◌ Bugs they have
  - ✧ Its social information
    - ◌ When to attack
    - ◌ Guess the password
- Conduct of the attack
- Afterwards
  - ✧ Clear the footprints (logs and records)
  - ✧ Open backdoors

7.1 Introduction to IDS

7.1.2 Process of Intrusions

❑ Three Steps of Intrusion

- 确定攻击目标
  - ✧ 攻击者根据其目的选择不同的攻击对象。攻击行为的初始步骤是搜集攻击对象尽可能详细的信息，包括：攻击对象操作系统的类型及版本、攻击对象提供的网络服务、各服务程序的类型及版本以及相关的社会信息。可以通过正常的访问过程中系统返回的相关信息进行判断，或者发送特殊的数据包，根据对象的反应区别目标的系统类型。
  - ✧ 操作系统的不同决定攻击方式的不同。服务的版本信息也是决定攻击方式的依据，因为不同版本服务的可利用的漏洞也是不同的。
  - ✧ 还有一些与系统的技术因素无关的信息，可以决定探测字典的构造、攻击时间等。

7.1 Introduction to IDS

7.1.2 Process of Intrusions

❑ Three Steps of Intrusion

- 实施攻击
  - ✧ 获得了攻击对象的足够多的信息后，攻击者可以利用相关漏洞的攻击方法渗透目标系统。
  - ✧ 攻击行为通常都要经过一个先期获取普通合法用户权限，进而获取超级用户权限的过程。这是因为很多信息窃取和破坏操作必须要有超级用户的权限才能够进行。
  - ✧ 由此看来，对用户权限特别是超级用户权限的管理和监督尤为重要。

7.1 Introduction to IDS

7.1.2 Process of Intrusions

❑ Three Steps of Intrusion

- 攻击后处理
  - ✧ 攻击者在成功实施完攻击行为后通常需要作一些善后处理，比如消除登录路径上的路由记录、删除攻击对象系统内的系统日志中的相关记录、根据需要设置后门等隐秘通道为下一次的入侵行为做准备。

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ Definition

- Intrusion Detection is the act of detecting actions that attempt to compromise the Confidentiality, Integrity or Availability of a resource.

❑ Intruders

- Masquerader (假冒者)
  - ✧ From outside
- Misfeasor (行为不端/滥用职权者)
  - ✧ From inside
- Clandestine user (隐匿者)
  - ✧ Outside or inside

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ Threat Monitoring

- 入侵检测方法的起源
  - ✧ *James P. Anderson* (University of Reading, Eng., 1980), Computer Security Threat Monitoring and Surveillance, 计算机安全威胁监控与监视
    - ◌ 第一次详细阐述了入侵检测的概念
    - ◌ 对计算机系统威胁进行分类
      - 外部渗透
      - 内部渗透
      - 不法行为
    - ◌ 提出了利用审计跟踪数据监视入侵活动的思想

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ Concepts for Intrusion Detection

- 入侵行为 (Intrusion)
  - ✧ 指系统内发生的任何违反安全策略的事件，具体包括：
    - ◌ 对系统的非授权访问
    - ◌ 授权用户的超越自身权限的访问
    - ◌ 合法用户的非法访问
    - ◌ 恶意程序攻击、对系统配置信息和安全漏洞的探测等

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ Concepts for Intrusion Detection

- 审计 (Audit)
  - ✧ 产生、记录并检查按时间顺序排列的系统事件记录的过程。
  - ✧ 审计的目标：
    - ○ 确定和保持系统活动中每个人的责任
    - ○ 重建事件
    - ○ 评估损失
    - ○ 监测系统的问题区
    - ○ 提供有效的灾难恢复
    - ○ 阻止系统的不正当使用

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ Concepts for Intrusion Detection

- 入侵检测 (Intrusion Detection)
  - ✧ 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、其它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以及被攻击的迹象。
    - ◌ 入侵检测作为一种积极主动的安全防护技术，为系统提供抵抗内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前对入侵进行拦截和响应。
- 入侵检测系统 IDS (Intrusion Detection System)
  - ✧ 实现入侵检测的软件与硬件的组合。

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ Functions of IDS

- Identify attacks already known
- Identify and block operations which is illegal or beyond the user's authority
- Check integrity of data
- Find vulnerability and bugs in the system
- Record legal behaviors
- Analyze illegal behaviors and intruders and record their features

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ Functions of IDS

1. 识别并阻断系统活动中存在的已知攻击行为，防止入侵行为对受保护系统造成损害。
2. 识别并阻断系统用户的违法操作行为或者越权操作行为，防止用户对受保护系统有意或者无意的破坏。
3. 检查受保护系统的重要组成部分以及各种数据文件的完整性。
4. 审计并弥补系统中存在的弱点和漏洞，其中最重要的一点是审计并纠正错误的系统配置信息。
5. 记录并分析用户和系统的行为，描述这些行为变化的正常区域，进而识别异常的活动。
6. 通过技术手段记录入侵者的信息、分析入侵者的目的和行为特征，优化系统安全策略。
7. 加强组织或机构对系统和用户的监督与控制能力，提高管理水平和管理质量。

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ IDS vs. Firewall

- A firewall is
  - ✧ Facing attacks from outside
  - ✧ Deployed at the “frontline”
  - ✧ Static relatively

Firewall

Door and Lock

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ IDS vs. Firewall

- An IDS is
  - ✧ Facing threats from inside
  - ✧ Deployed in the “building”

Intrusion Detection System

Monitor

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ IDS vs. Firewall

- 防火墙为网络提供了第一道防线，入侵检测系统被认为是防火墙之后的第二道安全闸门。
  - ✧ IDS 在不影响网络性能的情况下对网络进行检测，提供对内部攻击、外部攻击和误操作的实时保护。作为防火墙后的又一道防线，入侵检测系统可以大大减少网络免受各种攻击的损害。
  - ✧ 假如说防火墙是一幢大楼的门锁，那么 IDS 就是这幢大楼里的实时监控系统。门锁可以防止小偷从大门进入大楼，但不能防止大楼内部个别人员的不良企图。一旦小偷爬窗进入大楼，或内部人员有越界行为，门锁就失去了保护作用。这时，只有实时监控系统才能发现情况并发出警告。

7.1 Introduction to IDS

7.1.3 Intrusion Detection

❑ IDS vs. Firewall

- IDS 不仅仅针对外来的入侵者，同时也针对内部人员或组件的入侵行为。
  - ✧ 相当部分与网络安全相关的损失是由内部因素造成的，包括：盗取私有信息、破坏数据或网络、内部人员滥用网络访问、非授权的内部人员访问等等。
  - ✧ 安防系统的 “监控摄像机” 不是预防设备，但它们能起很大的威慑作用，并利于在事后找出肇事者、评估损害、追究责任、弥补缺陷等。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

❑ Anomaly Detection and Misuse Detection

- There are two ways to tell whether a behavior is malicious: Anomaly Detection (异常检测) and Misuse Detection (误用/滥用/盗用检测)
  - ✧ Anomaly Detection
    - ◌ How far from normal behaviors
      - Based on Behaviors - Behavioral Model
    - ◌ Statistics Analysis (统计分析法)
    - ◌ Neural Network (基于神经系统/学习系统的方法)
    - ◌ Data Mining (基于数据挖掘的方法)

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

❑ Anomaly Detection and Misuse Detection

- There are two ways to tell whether a behavior is malicious: Anomaly Detection (异常检测) and Misuse Detection (误用/滥用/盗用检测)
  - ✧ Misuse Detection
    - ◌ How similar to the attacks already known
      - Based on Rules – Knowledge Model
    - ◌ Pattern matching (模式匹配法)
      - Finding certain strings
      - Simple but more false-alarms, higher system burden
    - ◌ State transition (状态迁移法)
      - Enhanced pattern matching
      - Fast and flexible
      - Depend on system states
    - ◌ Expert system (基于专家系统的方法)

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

❑ Anomaly Detection and Misuse Detection

- 异常检测
  - ✧ 异常检测也称行为检测，或基于行为的检测。
  - ✧ 思路：根据已知的正常行为模型，判断当前行为是否是正常行为，若不是正常行为，则可以认为是攻击行为。
  - ✧ 方法：检测行为的特征与正常行为的特征的距离有多远。
    - ◌ 在应用程序层次监控用户的行为；
    - ◌ 可以用于监控权限升级攻击；
    - ◌ 更好的捕获那些富有经验的攻击者。
- 滥用/误用/盗用检测
  - ✧ 滥用也称特征检测，或基于知识的检测。
  - ✧ 思路：根据已知攻击行为的特征知识，推断当前行为是否为攻击行为
  - ✧ 方法：检测行为的特征与攻击行为的特征的距离有多近。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

❑ Behavioral Model of Anomaly Detection

- 异常检测的行为模型
  - ✧ 人或系统的正常行为具有一定的规律，可以通过行为分析、日志信息分析对这些规律进行总结。入侵行为通常和正常的行为存在严重的差异，通过检查这些差异可以实现入侵检测。
  - ✧ 异常检测建立主体正常活动的“行为模型”。检测时将当前主体活动与“行为模型”进行比较，如果发生显著偏离则可以认为该活动可能是入侵行为。
  - ✧ 异常检测根据使用者的行为或资源使用状况来判断是否发生入侵 (例如通过流量统计分析，将异常时间的异常网络流量视为可疑)，因此也称为基于行为的检测。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

- **Behavioral Model of Anomaly Detection**
  - 异常检测的行为模型
    - 基于行为的检测与系统相对无关，通用性较强。它甚至可能检测出以前从未出现过的新的攻击方式，而不像滥用检测那样受到已知行为模式的限制。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

❑ Behavioral Model of Anomaly Detection

- 统计分析技术
  - ✧ 构建异常检测 IDS 最常用的技术是利用统计理论提取用户或系统正常行为的特征轮廓。
    - ◌ 对系统和用户行为按照一定的时间间隔进行采样，样本包括用户登录和退出情况、CPU 和内存的占用情况、进程运行情况、硬盘及存储介质的使用情况等。
    - ◌ 利用统计理论提取系统和用户每次采样的行为轮廓与已有的轮廓进行合并，最终得到系统和用户正常行为的轮廓特征。
  - ✧ 统计的采样周期可以从几分钟到几个月甚至更长。IDS 通过对系统审计轨迹中的数据进行统计处理，并与正常行为轮廓特征进行比较，根据二者的偏差是否超过指定的门限来进一步判断是否有入侵发生。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

❑ Behavioral Model of Anomaly Detection

- 神经网络技术
  - ✧ 神经网络技术应用于入侵检测领域的研究时间较长，并在不断发展中。神经网络方法强调自学习和自适应功能，经过训练后能够根据实际检测到的信息进行有效处理，并做出入侵可能性的判断。
  - ✧ 将神经网络技术应用于攻击模式的学习，理论上也是可行的。但目前主要应用于系统行为的学习，包括用户以及系统守护程序的行为。与统计理论相比，神经网络技术更好地表达了变量间的非线性关系，且能自动学习并更新。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

❑ Behavioral Model of Anomaly Detection

- 数据挖掘技术
  - ✧ 计算机网络上的数据包流量及主机上的日志和审计信息的记录数据是海量的，单独依靠手工方法来发现记录中的异常现象非常困难。*Salvatore J. Stolfo* (1998) 等人率先应用数据挖掘的方法从海量的数据中提取感兴趣的知识。这些知识是隐含的、事先未知的、潜在的有用信息，提取的知识表示为概念、规则、规律、模式等形式，并用这些知识去检测异常入侵。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

- **Misuse Detection**
  - 模式匹配
    - 模式匹配是最基本的误用检测模式，通过在网络中查找特定的字符串或编码组，即搜索攻击行为的特征，来实现误用入侵检测。
    - 模式匹配方法简单易行，但是计算量大、误报率高、系统负载重，不适用于高速网络。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

- **Misuse Detection**
  - 状态转移 (状态迁移)
    - 状态转移方法以系统状态和状态转移表达式描述已知的攻击模式，采用优化的模式匹配来处理误用检测问题。
    - 由于处理速度的优势和系统的灵活性，状态转移法已成为当今最具竞争力的入侵检测模型之一。
    - 状态转移分析是针对事件序列的分析，所以不适合太复杂的事件分析，而且不能检测与系统状态无关的入侵。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

- **Misuse Detection**
  - 专家系统
    - 专家系统是基于知识的检测中应用最多的一种方法，它包含一系列描述攻击行为的规则 (Rules)，当审计数据事件被转换为可能被专家系统理解的包含特定警告程度信息的事实 (Facts) 后，专家系统应用一个推理机 (Inference Engine) 在事实和规则的基础上推理出最后结论。

7.1 Introduction to IDS

7.1.4 Methods of Intrusion Detection

❑ Anomaly Detection vs. Misuse Detection

1. 异常检测可以试图发现一些未知的入侵行为；误用滥用检测主要根据已有的、已建立的入侵特征模式进行检测，它只能检测已知的入侵行为，对于未知的入侵无能为力。
2. 异常检测根据使用者的行为或资源使用状况来判断是否有入侵行为，而不依赖于具体行为是否出现来检测；误用滥用检测大多是通过对一些具体行为的判断和推理，从而检测出入侵，检测相对直观。
3. 异常检测的主要缺陷在于误检率很高，尤其在用户数量众多或工作行为经常改变的环境中；误用滥用检测根据攻击特征库进行判断，具有较高的准确度。
4. 异常检测对具体系统的依赖性相对较小；误用滥用检测对具体的系统依赖性太强，移植性不够好。

Outline

- 7.1 Introduction to IDS
  - Threats to Computer System
  - Process of Intrusions
  - What Is Intrusion Detection
  - Methods of Intrusion Detection
- **7.2 Framework of IDS**
  - Basic Structure of IDS
  - Host-Based IDS (HIDS)
  - Network-Based IDS (NIDS)
  - HIDS vs. NIDS
- 7.3 Introduction to IPS
  - The Need of IPS
  - Security Capabilities
  - Types of IPS
  - IPS vs. IDS

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

- **Information Gathering**
  - System and network logs
  - Anomalous changes of system directories and files
  - Anomalous behavior in program executing
- **Analysis Engine**
  - Pattern matching
  - Statistics analysis
  - Integrity analysis
- **Response Unit**
  - Alert
  - Cut off connection
  - Block user
  - Change file attributes

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Information Gathering

- System and network logs
  - ✧ Login
  - ✧ Authorization
- Anomalous changes of system directories and files
  - ✧ Unexpected read, write and delete
  - ✧ Changed log files
- Anomalous behavior in program executing
  - ✧ Unexpected access for some processes to resources or data

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Information Gathering

- 系统或网络的日志文件纪录
  - ✧ 攻击者常在系统日志文件中留下他们的踪迹，充分利用系统和网络日志文件信息是检测入侵的必要条件。
  - ✧ 日志文件中记录了各种行为类型，每种类型又包含不同的信息
    - ◌ 例如记录“用户活动”类型的日志，包含了登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。
  - ✧ 用户活动的不正常的或不期望的行为
    - ◌ 重复登录失败
    - ◌ 登录到不期望的位置
    - ◌ 非授权访问重要文件

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Information Gathering

- 系统目录和文件的异常变化
  - ✧ 网络环境的文件系统中，包含重要信息的文件和私有数据文件经常是攻击者修改或破坏的目标。
  - ✧ 目录和文件中发生的不期望的改变 (包括修改、创建和删除等操作引起的，特别是针对那些正常情况下限制访问对象的)，很可能就是一种入侵产生的指示和信号。
  - ✧ 入侵者经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。
- 程序执行中的异常行为

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Analysis Engine - Methods of Detection

- Pattern matching
- Statistics analysis
  - ✧ Mean and standard deviation (平均测量值与标准值背离)
  - ✧ Operational model: large number of login in short period
  - ✧ Multivariate: Operational model with multi variables
  - ✧ Markov process: transition probabilities among various states
  - ✧ Time series: whether an event happens at correct time and lasts regular period
- Integrity analysis
  - ✧ Focus on files recently modified
  - ✧ Files planted Trojans

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Analysis Engine - Methods of detection

- 模式匹配
  - ✧ 模式匹配就是将收集到的信息与已知的网络入侵和系统误用特征数据库进行比较，从而发现违背安全策略的行为。
  - ✧ 一般来讲，一种攻击模式可以用一个过程 (如执行一条指令) 或一个输出 (如获得权限) 来表示。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或指令)，也可以很复杂 (如利用正则表达式来表示安全状态的变化)。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Analysis Engine - Methods of detection

- 统计分析
  - ✧ 统计分析方法首先给系统对象 (如用户、文件、目录和设备等) 创建一个统计描述，统计正常使用时的一些测量属性 (如访问次数、操作失败次数和延时等)。
  - ✧ 对主体行为进行测量得到的结果与上述正常测量属性进行平均值和偏差的比较，任何观察值在正常值范围之外时，就认为有入侵发生。
- 完整性分析 (事后)
  - ✧ 完整性分析主要关注某个文件或对象是否被更改。
  - ✧ 分析内容包括文件和目录的内容及属性。
  - ✧ 可以有效发现被更改的、被安装木马的应用程序。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

- **Response Unit**
  - Alert
  - Cut off connection
  - Block user
  - Change file attributes

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

- **Response Unit**
  - 简单报警
  - 切断连接
  - 锁定用户
  - 改变文件属性
  - #回击攻击者

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ IDES and NIDES

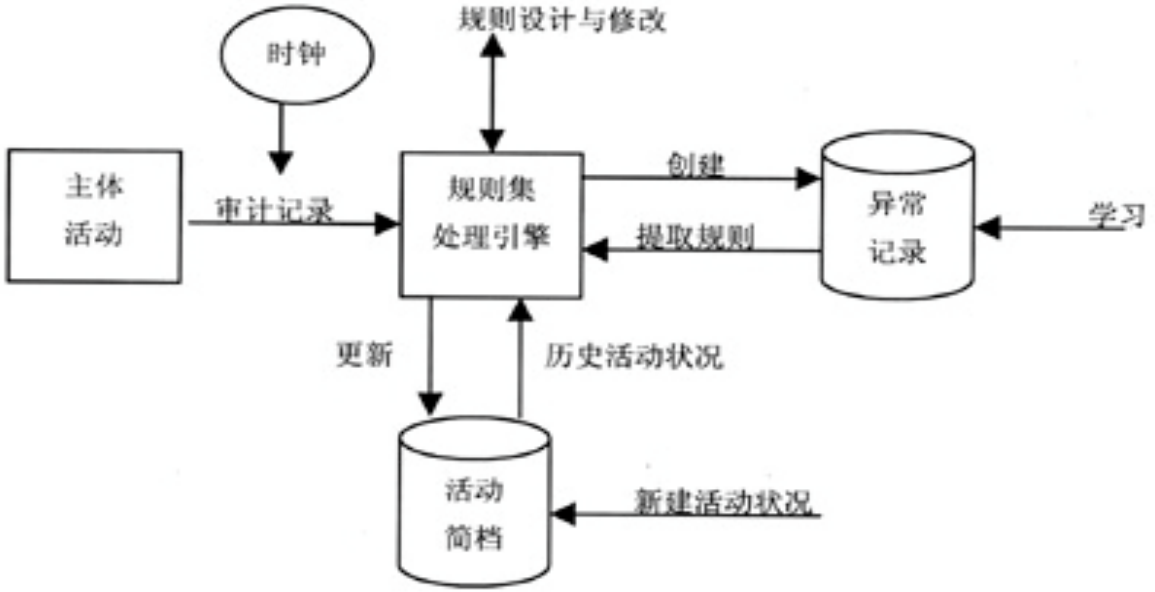
- **IDES,** Intrusion Detection Expert System
  - ✧ *Dorothy Denning*, 1986
- **NIDES,** Next-Generation Intrusion Detection Expert System
  - ✧ Subjects
  - ✧ Objects
  - ✧ Audit records:
    <Subject, Action, Object, Exception-Condition, Resource-Usage, Time-Stamp>
  - ✧ Activity Profile
  - ✧ Anomaly Record
    <Event, Time-Stamp, Profile>
  - ✧ Activity Rules

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Intrusion Detection Model

- *Denning* 模型
  - ✧ 最早的入侵检测模型由 *Dorothy Denning* 在1986年提出，并被此后的大部分实用系统所借鉴。*Denning* 模型是一个通用模型，与具体系统和具体输入无关，其体系结构如下



7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Intrusion Detection Model

- IDES & NIDES
  - ✧ 入侵检测专家系统 IDES (Intrusion Detection Expert System) 与其后继版本 NIDES (Next-Generation IDES) 均基于 *Denning* 模型。*Denning* 模型的最大缺点是它没有包含已知系统漏洞或攻击方法的知识，而这些知识在许多情况下是非常有用的信息。
  - ✧ IDES 模型由主体、客体、审计记录、活动简档、异常记录和活动规则6个主要部分构成：

① Subjects 主体

- ◌ 系统操作中的主动发起者，如操作系统的进程、网络的服务连接等

② Objects 客体

- ◌ 系统中被操作的对象，如文件、设备、命令、网络服务端接口等系统资源。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Intrusion Detection Model

- IDES & NIDES

③ Audit Records 审计记录

- Audit Records 由六元组构成：

<Subject, Action, Object, Exception-Condition, Resource-Usage, Time-Stamp>

- Action (活动) 是主体对目标的操作，对操作系统而言，这些操作包括读、写、登录、退出等；
- Exception-Condition (异常条件) 是系统对主体的该活动的异常报告，例如违反系统读写权限；
- Resource-Usage (资源使用状况) 纪录系统的资源消耗情况，如CPU、内存使用率等；
- Time-Stamp (时间戳) 纪录活动发生时间。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Intrusion Detection Model

- IDES & NIDES

④ Activity Profile 活动简档

- Activity Profile 保存主体正常活动的有关信息，刻划主体对客体的行为，其具体实现技术与检测方法有关。使用随机变量和统计模型从事件数量、频度、资源消耗等方面定量描述主体对客体的行为活动特征时，可以使用方差、马尔可夫模型等方法实现。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Intrusion Detection Model

- IDES & NIDES

④ Activity Profile 活动简档

- Activity Profile 定义了三种类型变量：
  - Event Counter 事件记数器：简单记录特定事件的发生次数 (数量)。
  - Interval Timer 间隔计时器：记录特定事件此次发生和上次发生之间的时间间隔 (频度)。
  - Resource Measure 资源计量器：记录某个时间内特定动作所消耗的资源量。
- 设 $x_1, x_2, \ldots, x_n$ 是随机变量 X 从审计记录中观测到的 n 个值，通过选择适当的统计模型，IDES 判断新观测到的下一个值 x_{n+1} 是否异常。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Intrusion Detection Model

- IDES & NIDES

④ Activity Profile 活动简档

- Activity Profile 是一个10元组：

<Variable-Name, Action-Pattern, Exception-Pattern, Resource-Usage-pattern, Period, Variable-Type, Threshold, Subject-pattern, Object-Pattern, Value>

  - Variable-Name 变量名称
  - Action-Pattern 动作模式
  - Exception-Pattern 例外模式
  - Resource-Usage-Pattern 资源使用模式
  - Period：测量的间隔时间或者取样时间。
  - Variable-Type：抽象数据类型定义。
  - Threshold 阈值
  - Subject-Pattern 主体模式
  - Object-pattern 客体模式
  - Value：当前观测值和统计模式所用的参数值

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ Intrusion Detection Model

- IDES & NIDES

⑤ Anomaly Record 异常记录

- 由 <Event, Time-stamp, Profile> 组成。用以表示异常事件的发生情况。发生时采取相应的措施。

⑥ Activity Rules 活动规则

- 活动规则集是检查入侵是否发生的处理引擎，它结合活动简档，应用专家系统或统计方法分析接收到的审计记录，调整内部规则或统计信息，在判断有入侵发生时采取相应的措施。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

- **CIDF**, Common Intrusion Detection Framework
  - What is CIDF
    - CIDFTG, 1998
    - CIDF is an effort to develop protocols and application programming interfaces so that intrusion detection research projects can share information and resources and so that intrusion detection components can be reused in other systems.
      - The Common Intrusion Detection Framework Architecture
      - A Common Intrusion Specification Language
      - Communication in the Common Intrusion Detection Framework
      - Common Intrusion Detection Framework APIs

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

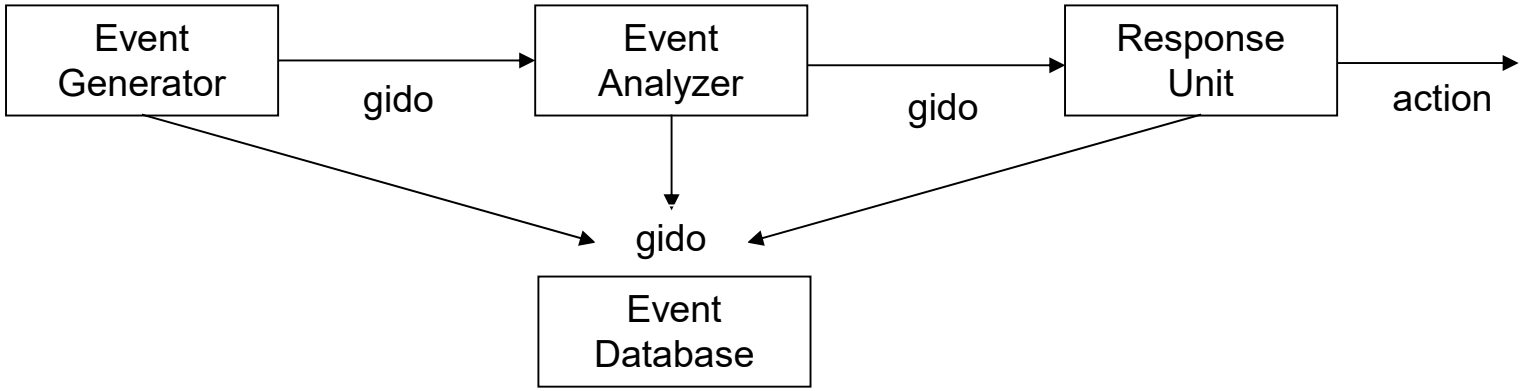
- **CIDF**, Common Intrusion Detection Framework
  - What is CIDF
    - 通用入侵检测框架 CIDF (Common Intrusion Detection Framework, CIDFTG 1998) 是为了解决不同入侵检测系统的互操作性和共存问题而提出的入侵检测的框架。
    - 目前大部分的入侵检测系统由不同机构独立研究与开发，不同系统之间缺乏互操作性和互用性。一个入侵检测系统的模块无法与另一个入侵检测系统的模块进行数据共享，在同一台主机上两个不同的入侵检测系统无法共存。为了验证或改进某个部分的功能就必须重构整个入侵检测系统，而无法重用现有的系统和构件。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ CIDF

- The architecture of CIDF
  - ✧ Event
  - ✧ GIDO (Generalized Intrusion Detection Objects)
  - ✧ Event generators
  - ✧ Event analyzers
  - ✧ Event databases
  - ✧ Response units

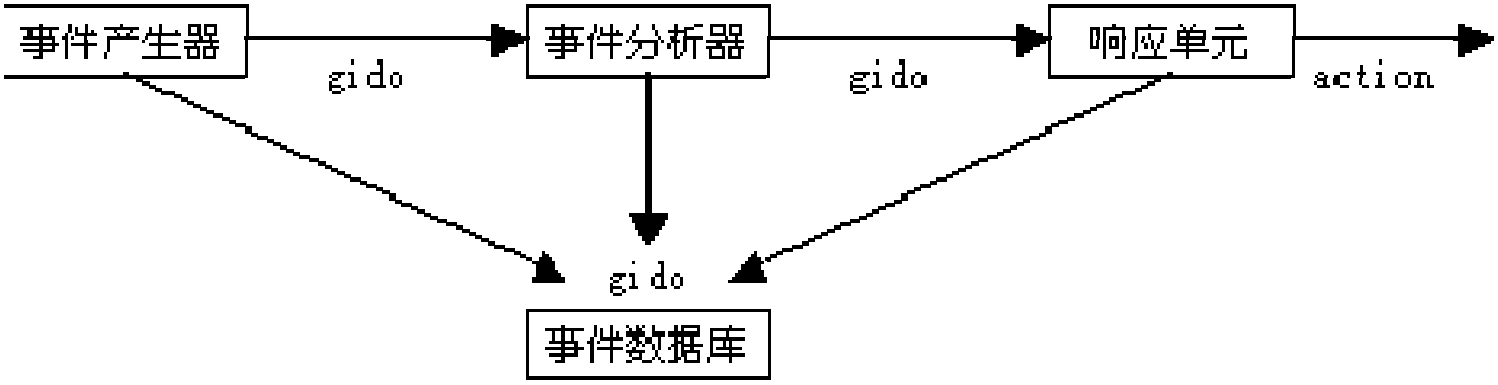


7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ CIDF

- The architecture of CIDF
  - ✧ CIDF 在 IDES 和 NIDES 的基础上提出了一个通用模型，将入侵检测系统分为四个基本组件：事件产生器、事件分析器、响应单元和事件数据库。
    - ◌ 事件 (Event)：入侵检测系统需要分析的数据统称为事件。可以是基于网络的入侵检测系统中网络中的数据，也可以是从系统日志或其它途径得到的信息。



7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ CIDF

- The architecture of CIDF
  - ✧ 四个基本组件只是逻辑实体，一个组件可能是某台计算机上的一个线程或进程，也可能是多个计算机上的多个进程，它们以统一入侵检测对象 GIDO (Generalized Intrusion Detection Objects) 格式进行数据交换。
    - ◌ GIDO 是对事件进行编码的标准通用格式，由 CIDF 描述语言 CISL 定义。GIDO 数据流可以是发生在系统中的审计事件，也可以是对审计事件的分析结果。

7.2 Framework of IDS

7.2.1 Basic Structure of IDS

❑ CIDF

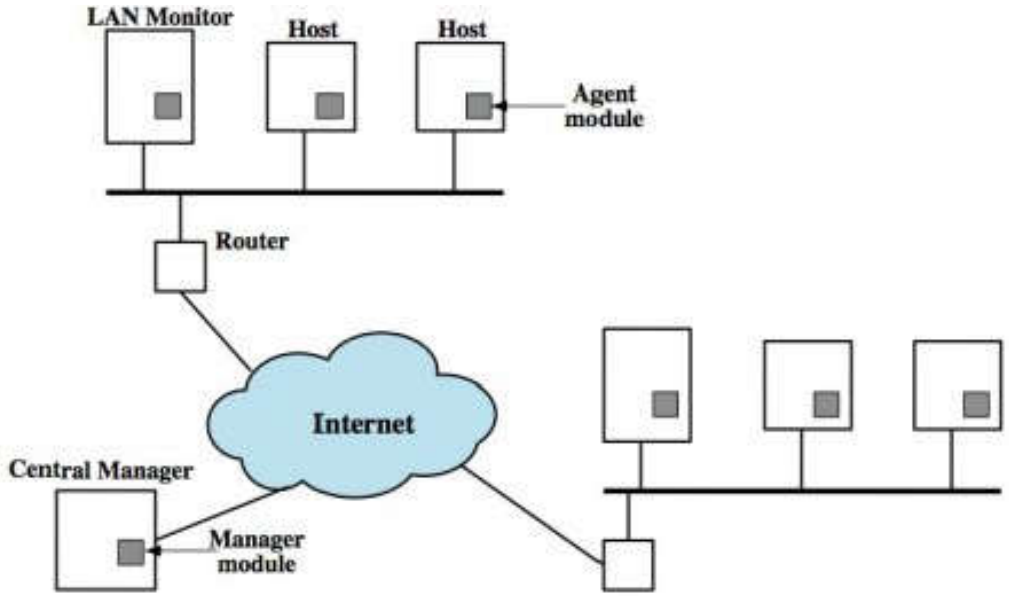
- The architecture of CIDF
  - ✧ Event Generators 事件产生器
    - ◌ 从入侵检测系统之外的计算环境中收集事件，并将这些事件转换成 CIDF 的 GIDO 格式传送给其他组件。
  - ✧ Event Analyzers 事件分析器
    - ◌ 分析从其它组件收到的 GIDO，产生新的 GIDO，再传送给其它组件。
  - ✧ Response Units 响应单元
    - ◌ 处理收到的 GIDO，并据此采取相应的措施。
  - ✧ Event Databases 事件数据库
    - ◌ 用于存储 GIDO。

7.2 Framework of IDS

7.2.2 Host-based IDS

❑ Host-based IDS (HIDS)

- Monitor activities on the system
- Detect both external and internal intrusions
- Deployment (Distributed Host)



7.2 Framework of IDS

7.2.2 Host-based IDS

❑ Host-based IDS (HIDS)

- HIDS 概述
  - ✧ HIDS 始于20世纪80年代早期，通过查看针对可疑行为的审计记录，对新的记录条目与攻击特征进行比较，并检查不应该被改变的系统文件的校验和来分析系统是否被侵入或者被攻击。如果发现与攻击特征匹配，IDS 系统通过向管理员报警和其他呼叫行为来响应。
  - ✧ HIDS 的主要目的是在事件发生后提供足够的分析来阻止进一步的攻击。反应的时间依赖于定期检测的时间间隔，实时性不及基于网络的 NIDS。
  - ✧ HIDS 可以部署在各种计算机上，包括服务器和 PC 机，但通常被部署在具有较高价值的服务器上，包括各种关键的基础网络服务器、业务服务器和数据库服务器。

7.2 Framework of IDS

7.2.2 Host-based IDS

❑ Some Potential Threats to HIDS

- Abuse of privilege
  - ✧ Temporary root
  - ✧ Former employees
  - ✧ Invisible account created by former administrator
- Access and modification on key information
  - ✧ Student scores, e.g.
  - ✧ Individual information
  - ✧ Coopetition (合作-竞争关系)
- Security configuration
  - ✧ Guest account
  - ✧ Nomadic user (游牧用户)
  - ✧ Screen saver not activated

7.2 Framework of IDS

7.2.2 Host-based IDS

❑ Some Potential Threats to HIDS

- 特权滥用
  - ✧ 暂时的 root 权限
    - ◌ 用户要安装软件时，管理员出于方便可能先提高他的特权再降低，但却忘记回收。
  - ✧ 前职员使用旧帐户
    - ◌ 职员离职时，原来的帐户删除往往要花费一些时间，造成了一个窗口。
  - ✧ 前管理员创建后门帐户
    - ◌ 管理员有时为了方便，直接利用自己的特权增加一个帐户，管理员离职后，却没人知道这个帐户的存在。

7.2 Framework of IDS

7.2.2 Host-based IDS

❑ Some Potential Threats to HIDS

- 关键数据访问及修改
  - ✧ 修改、伪造数据
  - ✧ 非授权泄露
    - ◌ 当两个部门存在既合作又竞争的关系时，共享的资源可能造成信息泄露。
  - ✧ 私人信息窃取
    - ◌ 拥有很多客户信息的大服务商内部人员可以相对容易地获得客户的个人信息。

7.2 Framework of IDS

7.2.2 Host-based IDS

❑ Some Potential Threats to HIDS

- 安全配置不当
  - ✧ 存在访客帐户 (guest account)
  - ✧ 游牧用户 (nomadic user) 配置不当
    - ◌ 经常出入网络的笔记本用户，可能从外部带来威胁。
  - ✧ 用户为使用方便不激活屏保程序

7.2 Framework of IDS

7.2.2 Host-based IDS

❑ HIDS Policy

- HIDS 根据系统内部的各种数据及相关记录实现检测。
- 系统审计记录
  - ✧ 系统审计记录对一个系统的运行状况及效率进行检测与评价，利于系统的使用或改进，保证取得实际的应用效果。
  - ✧ 系统审计记录由操作系统核心的审计子系统产生，用于记录当前系统的活动信息，如进程的调用状态、执行的命令及参数等。不同的操作系统中审计记录组织方式可能不同，但基本上都是按照时间顺序将这些信息记录到多个审计文件中，内容比较详尽。
  - ✧ 操作系统设计时已经考虑到了系统审计记录的可靠性、安全性和可信性，因此是 HIDS 的首选数据源。

7.2 Framework of IDS

7.2.2 Host-based IDS

❑ HIDS Policy

- 系统日志
  - ✧ 系统日志是利用操作系统日志机制生成的日志文件的总称，它专门记录系统内部各种信息源产生的信息。
  - ✧ 不同于系统审计记录，系统日志由系统内核之外的程序产生，并没有足够高的安全性。
  - ✧ 系统日志包括系统内进程的启动、运行、终止等信息，以及关键命令的运行、用户的登入登出操作等信息。
- 应用程序日志
  - ✧ 由应用程序维护，保存关于特定应用的日志信息。
- 其他数据源

7.2 Framework of IDS

7.2.2 Host-based IDS

❑ HIDS – Advantages & Disadvantages

Advantages	Disadvantages
Near targets of attacks	Operating system dependent
No extra hardware devices	Burden on the host
Independent on network	Limited to the host
Deal with unencrypted messages	Complicated install and maintenance

7.2 Framework of IDS

7.2.2 Host-based IDS

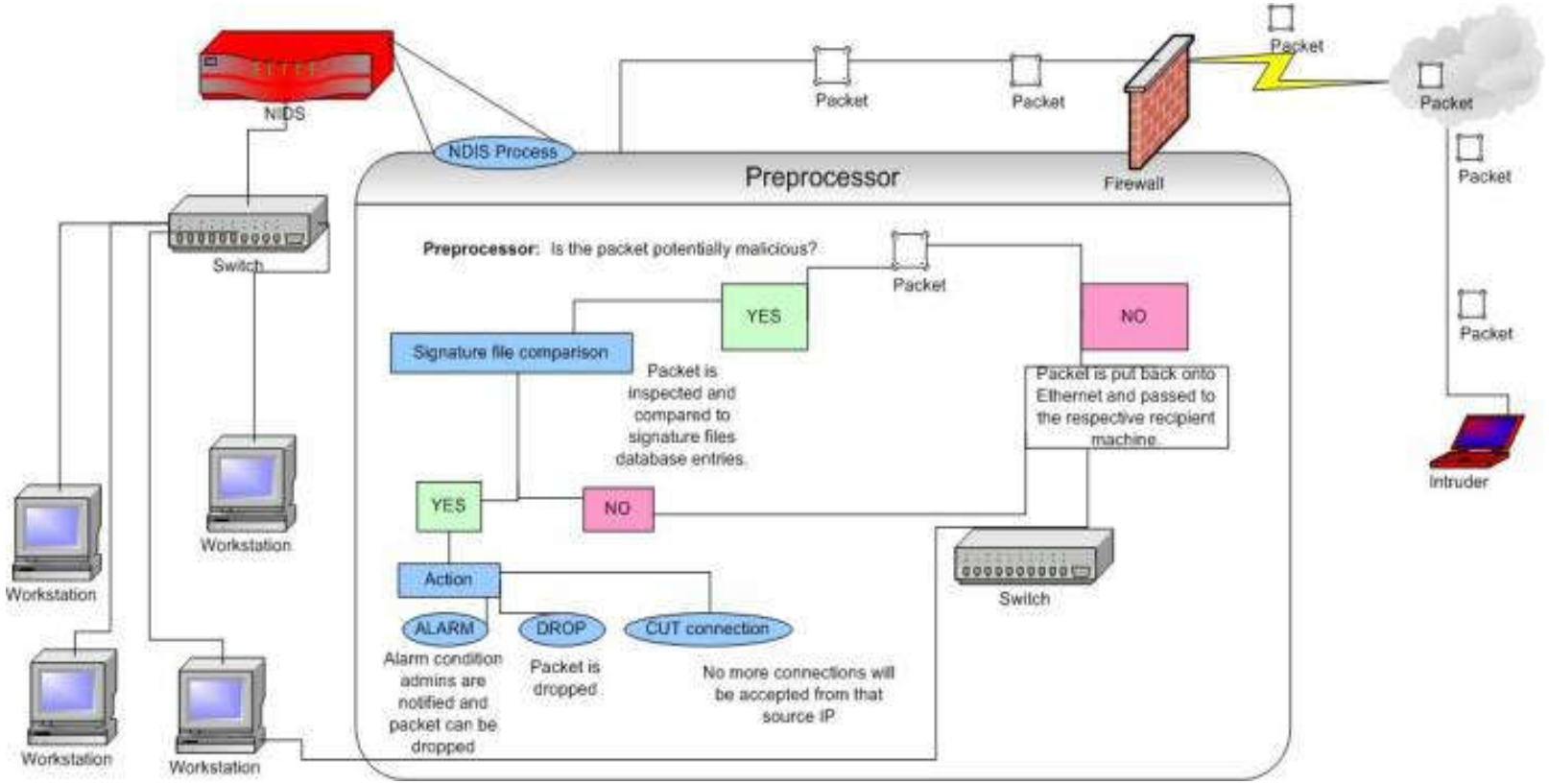
❑ HIDS – Advantages & Disadvantages

- 优点：
  - ✧ 能够监测所有的系统行为，可以精确监控针对主机的攻击过程
  - ✧ 不需要额外的硬件支持
  - ✧ 适合加密的环境 (处理解密后的数据，因此能够应对基于加密数据包的攻击)
  - ✧ 网络无关性
- 缺点：
  - ✧ 开发成本高，有技术壁垒保护
  - ✧ 没有平台无关性，可移植性差
  - ✧ 较多的检测手段会影响主机的性能
  - ✧ 维护和管理工作较为复杂
  - ✧ 无法判断基于网络的入侵行为

7.2 Framework of IDS

7.2.3 Network-based IDS (NIDS)

❑ **Illustration of an NIDS**

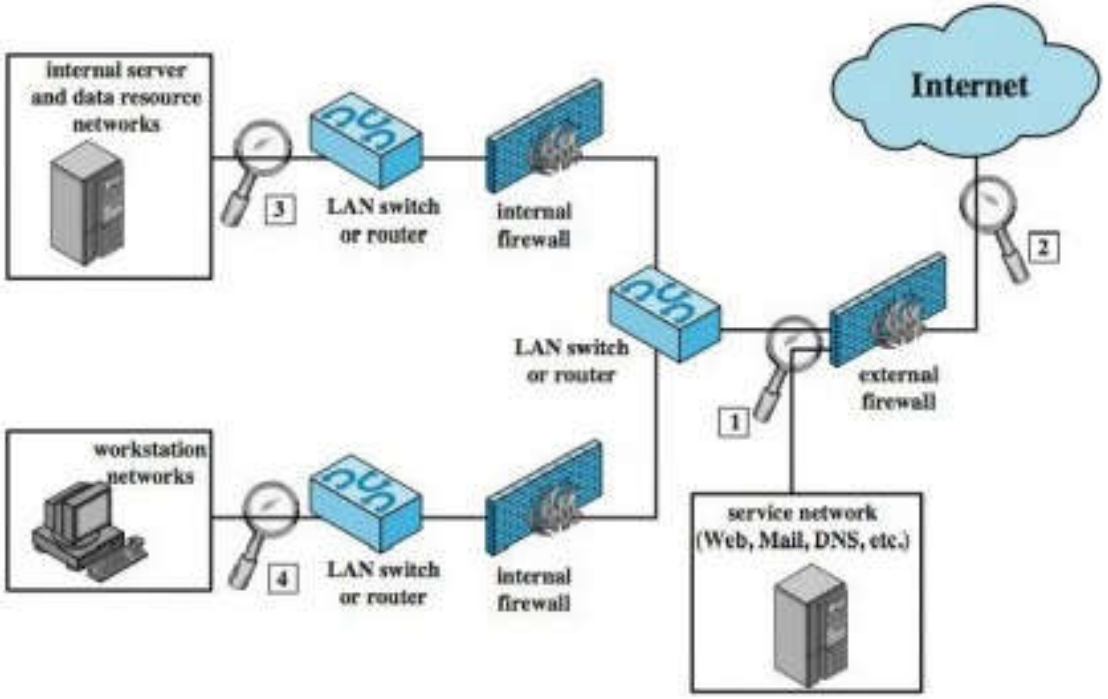


7.2 Framework of IDS

7.2.3 Network-based IDS (NIDS)

❑ Components of NIDS

- NIDS typically includes:
  - ✧ A number of sensors
  - ✧ One or more servers for NIDS management
  - ✧ One or more management consoles for human interface

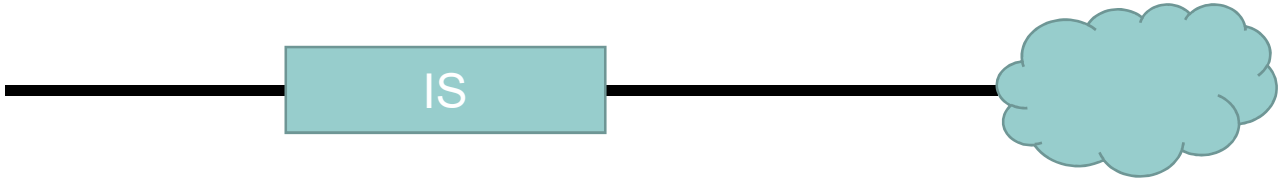


7.2 Framework of IDS

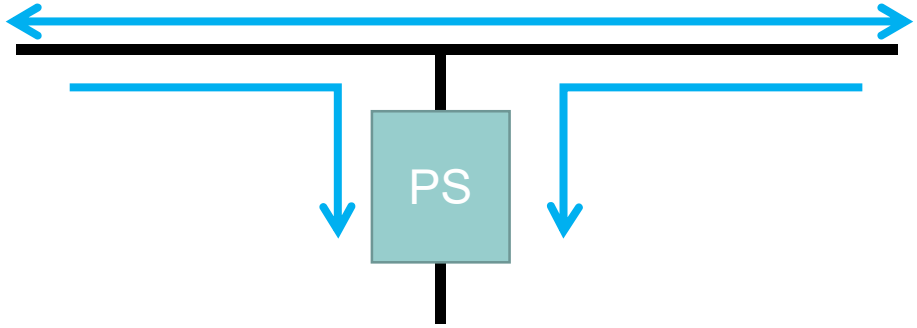
7.2.3 Network-based IDS (NIDS)

❑ Components of NIDS

- Sensors
  - ✧ Inline sensor



  - ✧ Passive sensor



7.2 Framework of IDS

7.2.3 Network-based IDS (NIDS)

❑ Detecting Techniques

- Signature Detection 特征检测
  - ✧ Application layer: DHCP, IMAP, NFS, DNS, FTP…
  - ✧ Transport layer: SYN floods
  - ✧ Network layer: spoofed IP address
- Anomaly Detection 异常检测
  - ✧ DoS: significant increasing packet traffic or connection attempts
  - ✧ Scanning:
  - ✧ Worms:

7.2 Framework of IDS

7.2.3 Network-based IDS (NIDS)

❑ 一些攻击场景

- 非授权访问
  - ✧ 外部人员利用一些程序的安全漏洞，未经允许登录到系统中。
  - ✧ 攻击者通过本地计算机访问与同一网段的其他计算机，从而达到隐蔽的效果。
- 数据、资源窃取
  - ✧ 重要商业信息、口令下载；带宽窃取 (利用大公司的带宽，架设自己的网站，为自己谋利)。
- 拒绝服务

7.2 Framework of IDS

7.2.3 Network-based IDS (NIDS)

❑ NIDS – Advantages & Disadvantages

Advantages	Disadvantages
Operating system independent	Unable to deal with encrypted messages
Not influence the hosts	Capability problems
Transparent to intruders	
Protect a domain	Vulnerable to DoS
Can detect lower layer attacks	
Original packets	

7.2 Framework of IDS

7.2.3 Network-based IDS (NIDS)

❑ NIDS – Advantages & Disadvantages

- 优点：
  - ✧ 平台无关性
  - ✧ 不影响受保护主机性能
  - ✧ 对攻击者透明
  - ✧ 能够进行较大范围的安全保护
  - ✧ 检测数据有很高的真实性
  - ✧ 可检测基于低层协议的攻击

7.2 Framework of IDS

7.2.3 Network-based IDS (NIDS)

❑ NIDS – Advantages & Disadvantages

- 缺点：
  - ✧ 不在通信的端点，无法处理全部网络协议层次的攻击
  - ✧ 对加密传输无能为力
  - ✧ 对交换网络支持不足，只能检测一个网段
  - ✧ 处理能力可能不足
  - ✧ 易受 DoS 攻击

7.2 Framework of IDS

7.2.4 HIDS vs. NIDS

❑ Host-Based IDS vs. Network-Based IDS

- Comparative analysis of HIDS vs. NIDS

  http://www.windowsecurity.com/articles/hids_vs_nids_part1.html

7.2 Framework of IDS

7.2.4 HIDS vs. NIDS

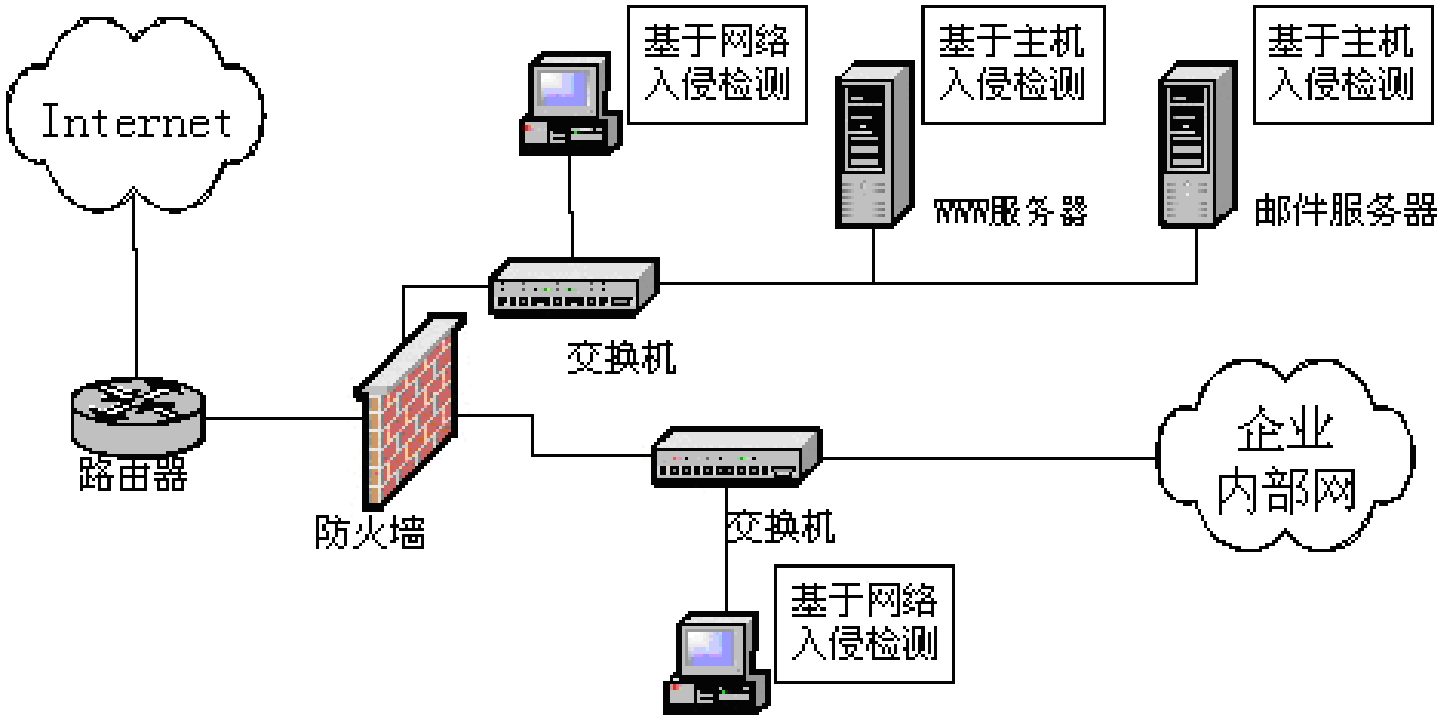
❑ **HIDS vs. NIDS**

类别	数据源内容	优点	缺点
NIDS	网络中的所有数据包	不会影响业务系统的性能；采取旁路侦听工作方式，不会影响网络的正常运行	不能检测通过加密通道的攻击；
HIDS	计算机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	能够提供更为详尽的用户行为信息；系统复杂性小；误报率低	对主机的依赖性很强、性能影响很大；不能监测网络情况

7.2 Framework of IDS

7.2.4 HIDS vs. NIDS

- **Mixed Deployment of HIDS and NIDS**



Outline

- 7.1 Introduction to IDS
  - Threats to Computer System
  - Process of Intrusions
  - What Is Intrusion Detection
  - Methods of Intrusion Detection
- 7.2 Framework of IDS
  - Basic Structure of IDS
  - Host-Based IDS (HIDS)
  - Network-Based IDS (NIDS)
  - HIDS vs. NIDS
- **7.3 Introduction to IPS**
  - The Need of IPS
  - Security Capabilities
  - Types of IPS
  - IPS vs. IDS

7.3 Introduction to IPS

7.3.1 The Need of IPS

- **What is IPS** (Intrusion Prevention System)
  - IPS is a system that identify malicious activity, log information about malicious activity, attempt to block/stop malicious activity, and report malicious activity.
- **The Need of IPS**
  - Users need an automate system to deal with Intrusions.
  - Users need a preferable system to remedy (补救) IDS's defects.
  - Users need a high-performance system to keep the network's security.

7.3 Introduction to IPS

7.3.1 The Need of IPS

❑ The Need of IPS

- IDS 不能完全满足安全目标的需求
  - ✧ IDS 的设计目标
    - ◌ IDS 检测和监控网络中的数据包等网络运行的状态，通过一系列的分析机制来判定当前网络是否受到威胁。这种设计目标很难完全满足用户的应用要求：许多用户不但需要知道自己所处的网络环境是否受到威胁，还要求有一系列相应的智能化的解决方案去自动消除他们所面对的威胁。
    - ◌ IDS 只能检测出系统是否受到威胁。IDS 的检测机制是被动的、事后的，不能主动抵挡这些攻击。用户对系统智能处理入侵事件的能力需求，促进了 IPS 的研究与发展。

7.3 Introduction to IPS

7.3.1 The Need of IPS

❑ The Need of IPS

- IDS 不能完全满足安全目标的需求
  - ✧ IDS 自身存在的缺陷
    - ◌ IDS 作为一款系统软件本身可能存在设计和实现的漏洞。入侵者一旦发现这些漏洞，就可以凭借漏洞来隐蔽自己的攻击行为。
    - ◌ 由于网络环境的复杂性，IDS 很难将其检查范围覆盖到整个庞大复杂的网络。另外，覆盖整个网络的入侵检测系统开销巨大，这样也可能导致系统无法识别出一些入侵者的行为。

7.3 Introduction to IPS

7.3.1 The Need of IPS

❑ The Need of IPS

- IDS 不能完全满足安全目标的需求
  - ✧ IDS 的判别能力
    - ◌ IDS 产品的评价以其漏判率 (false negative rate) 和误判率 (false positive rate) 作为参考。漏判率是 IDS 将有危险性的行为当作无害的行为的概率；误判率是 IDS 将没有危险性的行为当作有害的行为的概率。漏判率和误判率都是越低越好。
    - ◌ 漏判率和误判率是相互对立的属性，高的漏判率将会导致低的误判率，而低的漏判率将会导致高的误判率，IDS 必须在两者间取得一个平衡。但由于设计、技术、算法等原因，IDS 的生产厂商往往采用“宁可报错，不可漏报”，牺牲误判率换取低的漏判率，导致系统整体性能下降。

7.3 Introduction to IPS

7.3.2 Security Capabilities of IPS

❑ Security Capabilities an IPS should have

- Detect Intrusion
  - ✧ Signature-Based Detection 基于特征的检测模式
  - ✧ Anomaly-Based Detection 基于异常的检测模式
  - ✧ Stateful Protocol Analysis 基于状态的协议分析
  - ✧ HoneyPot 蜜罐技术
  - ✧ Evaluating the detect capabilities
    - ◌ Threshold 极限/阈值
    - ◌ Blacklists & Whitelists
    - ◌ Alert Setting
    - ◌ Code Viewing and Editing
- Log Intrusion
- Stop Intrusion
- Report Intrusion

7.3 Introduction to IPS

7.3.2 Security Capabilities of IPS

❑ Security Capabilities an IPS should have

- 基于特征的检测模式
  - ✧ 建立一个已知入侵行为的特征集合，然后根据此集合对网络上各种行为进行甄别。
- 基于异常的检测模式
  - ✧ 先对某段时间内正常情况下网络的各种状态进行记录 (profile)，定义在网络上的何种行为 (或者是环境条件，如单位时间内流经某节点的数据包数目) 是正常的，以此来辨别一个行为是否具有威胁性。
- 基于状态的协议分析
  - ✧ 依靠厂商预先定义的网络应该执行的协议以及执行的步骤来区分网络在运行过程中是否受到了攻击。

7.3 Introduction to IPS

7.3.2 Security Capabilities of IPS

❑ Security Capabilities an IPS should have

- Log Intrusion
  - ✧ IPS log information about the intrusion that they detect. The information is helpful to evaluate the intrusion and to find out an appropriate way to protect the target.
  - ✧ 使用日志文件等记录网络上发生过的具有威胁性的行为：IPS 应提供日志功能对网络入侵行为进行记录，例如入侵者的攻击频率和特征等资料，有助于更为有效地制定网络安全策略。
  - ✧ 日志文件可以作为分析入侵者的第一手资料，在帮助网络管理员进行管理分析、提高网络安全性能方面具有很大的参考价值。

7.3 Introduction to IPS

7.3.2 Security Capabilities of IPS

- **Security Capabilities an IPS should have**
  - Stop Intrusion
    - Stop the attack independently
      - Terminate the network connection
      - Block the malicious packages
      - Block the access to target
    - Changes the security environment
      - The IPS could change the configuration of other security controls.
      - For example: apply patches to a attacked host, alert the firewall to block the access of the intruders, etc.
    - Change the attack's content
      - The IPS could remove or replace malicious portions of an attack to make it benign

7.3 Introduction to IPS

7.3.2 Security Capabilities of IPS

- **Security Capabilities an IPS should have**
  - Stop Intrusion
    - 阻止具有威胁性的行为的发生，或者是当上述行为已经发生之后，阻止其对系统造成更大的损害
      - IPS 应该能自主地阻止入侵行为，如：阻止任何数据传输到受保护的节点、自动过滤有害的数据包等等；另外，IPS 还可以提供维护安全环境、修复有害数据包内容的能力。
      - 例如，一封电子邮件中可能附带了具有危险性的可执行程序，那么 IPS 可以把这个可执行程序删除，把修复后的邮件的原文发送给目的主机。

7.3 Introduction to IPS

7.3.2 Security Capabilities of IPS

❑ Security Capabilities an IPS should have

- Report Intrusion
  - ✧ Report the Intrusion in detail or in summary depending on the require of users.
  - ✧ When the intrusion begin, alert the manager as soon as possible.

7.3 Introduction to IPS

7.3.2 Security Capabilities of IPS

- **Security Capabilities an IPS should have**
  - Report Intrusion
    - 向管理者等相关人员发出警告、报告等
      - 当 IPS 检测到网络正在遭受入侵或者已经被入侵时，应该及时通过各种渠道通知网络管理人员和网络安全专家、网络用户等相关人员，这些通知可以是短信、电话或者其他任何有效的形式。
      - 除此之外，系统还应该能够向相关人员提供一份系统检测的情形或者是发生的入侵事件的详细报告或各类事件的总结。

7.3 Introduction to IPS

7.3.3 Types of IPS

❑ Components of IPS

- IPS will contain four major components:
  - ✧ Agent/Sensor
  - ✧ Management Server
  - ✧ Database Server
  - ✧ Console

7.3 Introduction to IPS

7.3.3 Types of IPS

❑ Components of IPS

- Agent/Sensor
  - ✧ Agent/Sensor monitor and analyze network's activity
  - ✧ The Agent is used for HIPS
  - ✧ The Sensor is used for NIPS
- Management Server
  - ✧ A management server is a centralized device that receives information from the sensors or agents and manages them.
  - ✧ Function:
    - ◌ analyze the information
    - ◌ identify the intrusion
    - ◌ control the agents or sensors

7.3 Introduction to IPS

7.3.3 Types of IPS

❑ Components of IPS

- Database Server
  - ✧ A database server is a repository for event information. Particularly, the information is generate by agents or sensor.
- Console
  - ✧ A console is a program provide administration and/or monitoring capabilities for the IPS' users and administrators. It's a interface between the IPS and the IPS' user and administrators.

7.3 Introduction to IPS

7.3.3 Types of IPS

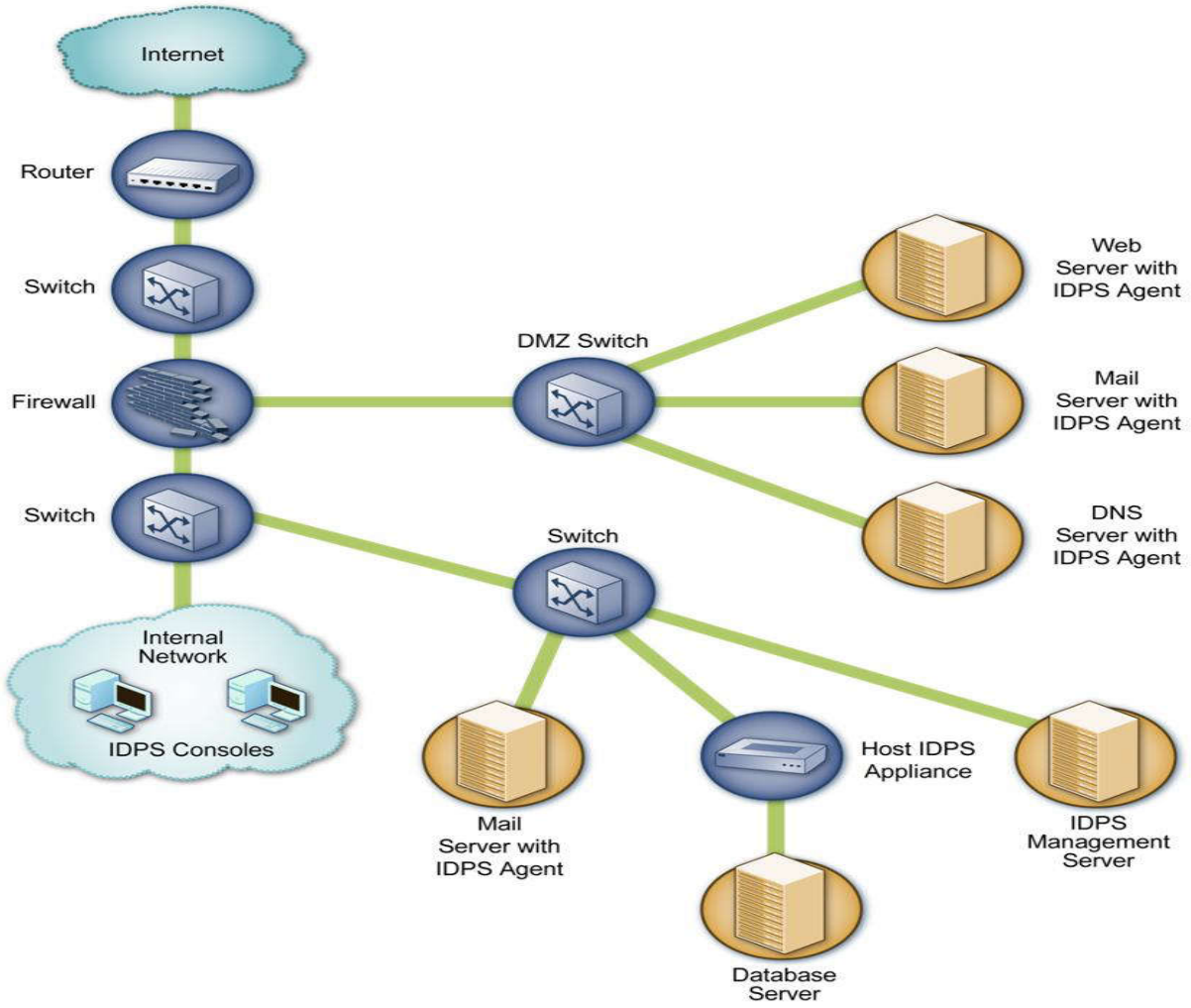
❑ HIPS & NIPS

- Host-Based Intrusion Prevention System, **HIPS**
  - ✧ 基于主机的入侵防御系统 HIPS 通过监控主机上的活动来判断当前网络是否有受到入侵的可能。
  - ✧ HIPS 主要由代理主机、管理服务器、数据服务器和控制台组成。代理是一类安装了检测软件的独立主机，它们可以监控系统中发生的入侵行为，并且阻止这些行为。而管理服务器主要负责接收来自代理的数据，并将这些数据发送到数据服务器中存储起来。控制台负责管理和监控。

7.3 Introduction to IPS

7.3.3 Types of IPS

- **HIPS & NIPS**
  - HIPS



7.3 Introduction to IPS

7.3.3 Types of IPS

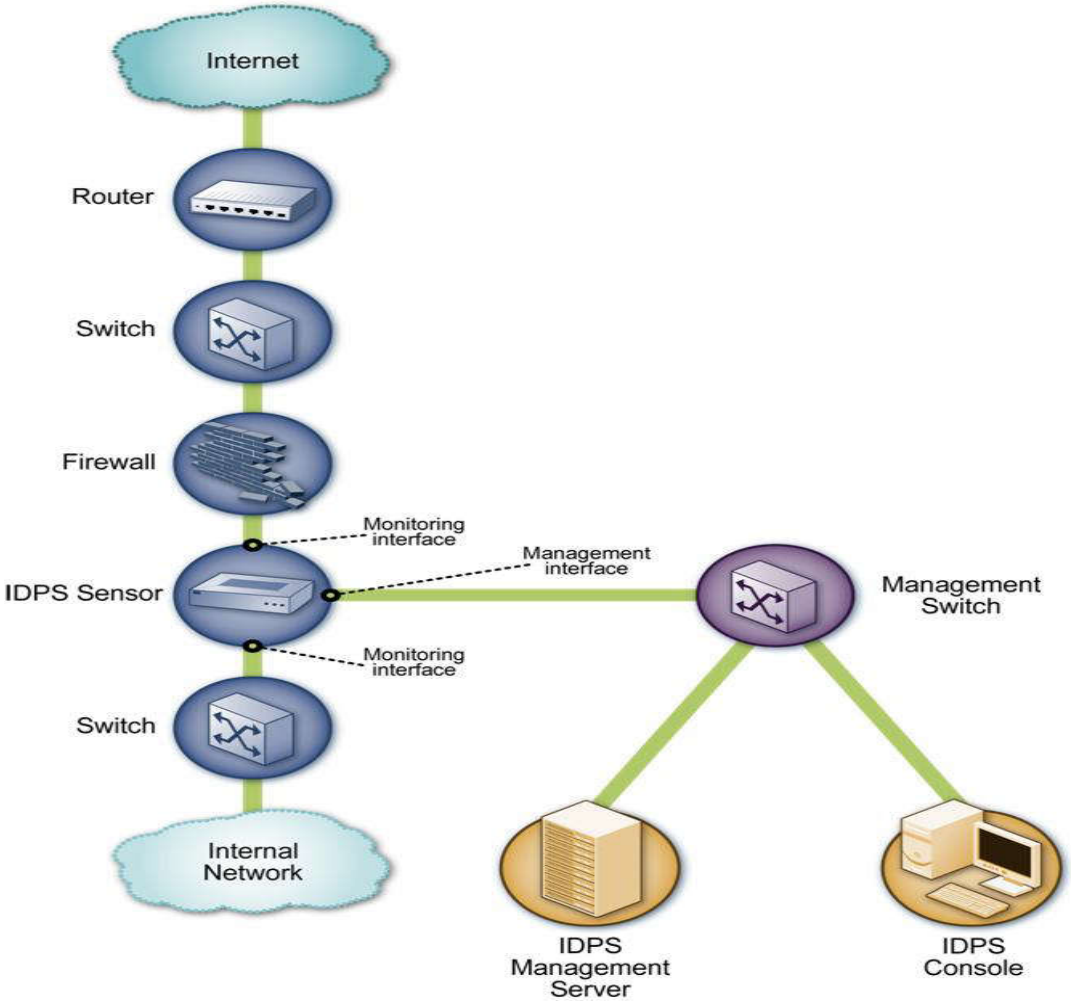
❑ HIPS & NIPS

- Network-Based Intrusion Prevention System, **NIPS**
  - ✧ 基于网络的入侵防御系统 NIPS。在 NIPS 中，负责接收信息的部分称为 sensor，可以根据 sensor 接入网络的方式将 NIPS 其分为内联型 (inline) 和被动接入型 (passive，也称旁路型)。
    - ◌ 内联型中所有的网络数据包必须经过 sensor 的批准放行
    - ◌ 被动接入型中 sensor 处理的是网络数据包的副本

7.3 Introduction to IPS

7.3.3 Types of IPS

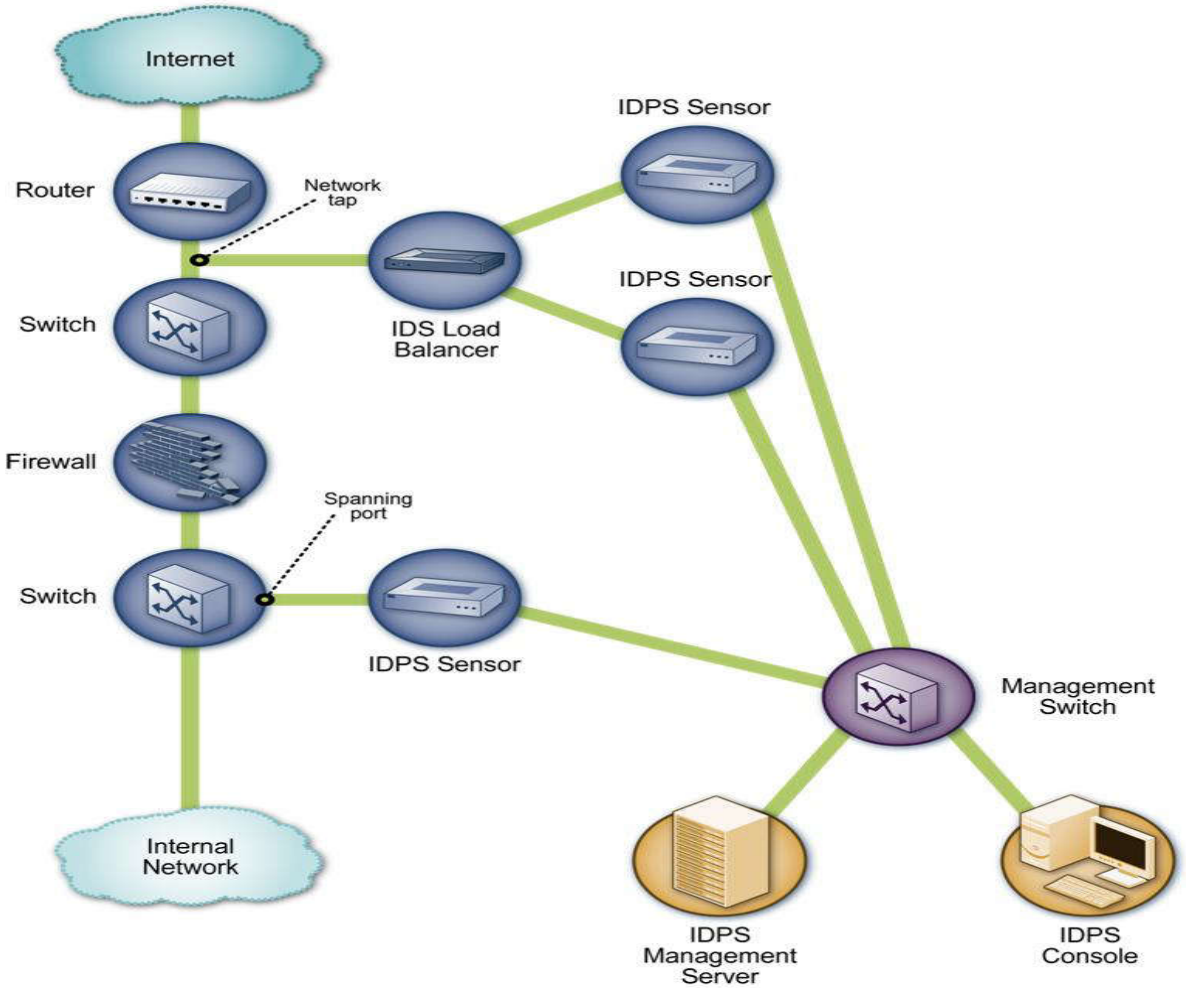
- **HIPS & NIPS**
  - NIPS
    - Inline



7.3 Introduction to IPS

7.3.3 Types of IPS

- **HIPS & NIPS**
  - NIPS
    - Passive



7.3 Introduction to IPS

7.3.4 IPS vs. IDS

❑ IPS vs. IDS

- Usage
  - ✧ IPS is used to defend the outside attack
  - ✧ IDS is used to find out the attack
- Security Policy
  - ✧ IDS will report the intrusion
  - ✧ IPS try to defend it automatically
- Deployment
  - ✧ IDS is deployed near to the center of the network
  - ✧ IPS is usually deployed on the network's boundary

7.3 Introduction to IPS

7.3.4 IPS vs. IDS

❑ IPS vs. IDS

- IPS 与 IDS 的设计有类似之处，IPS 是以 IDS 为基础，增加对入侵行为进行控制的新一代安全系统。
- 作用目的
  - ✧ IDS 部署在网络内部，监控范围可以覆盖整个子网，包括来自外部的数据以及内部终端之间传输的数据。通过对全网信息的分析，了解信息系统的安全状况，进而指导信息系统安全建设目标以及安全策略的确立和调整，对入侵行为只起到发现和报警的作用。
  - ✧ IPS 部署在网络边界，实施既定的安全策略，如果检测到外部攻击，会在攻击扩散到网络的其它地方之前进行阻止，但缺乏对内部攻击行为的应对能力。

7.3 Introduction to IPS

7.3.4 IPS vs. IDS

❑ IPS vs. IDS

- 安全策略
  - ✧ IDS 注重对网络安全状况的监管。
  - ✧ IPS 关注对外部入侵行为的控制。IPS 可以实施深层防御安全策略，即可以在应用层检测出攻击并予以阻断，这是防火墙类和入侵检测类产品所做不到的。
- 检测方法
  - ✧ IPS 对入侵的检测一般依靠对数据包的检测。IPS 将检查进入受保护网络的数据包，确定这种数据包的真正用途，然后决定是否允许这种数据包入网。

7.3 Introduction to IPS

7.3.4 IPS vs. IDS

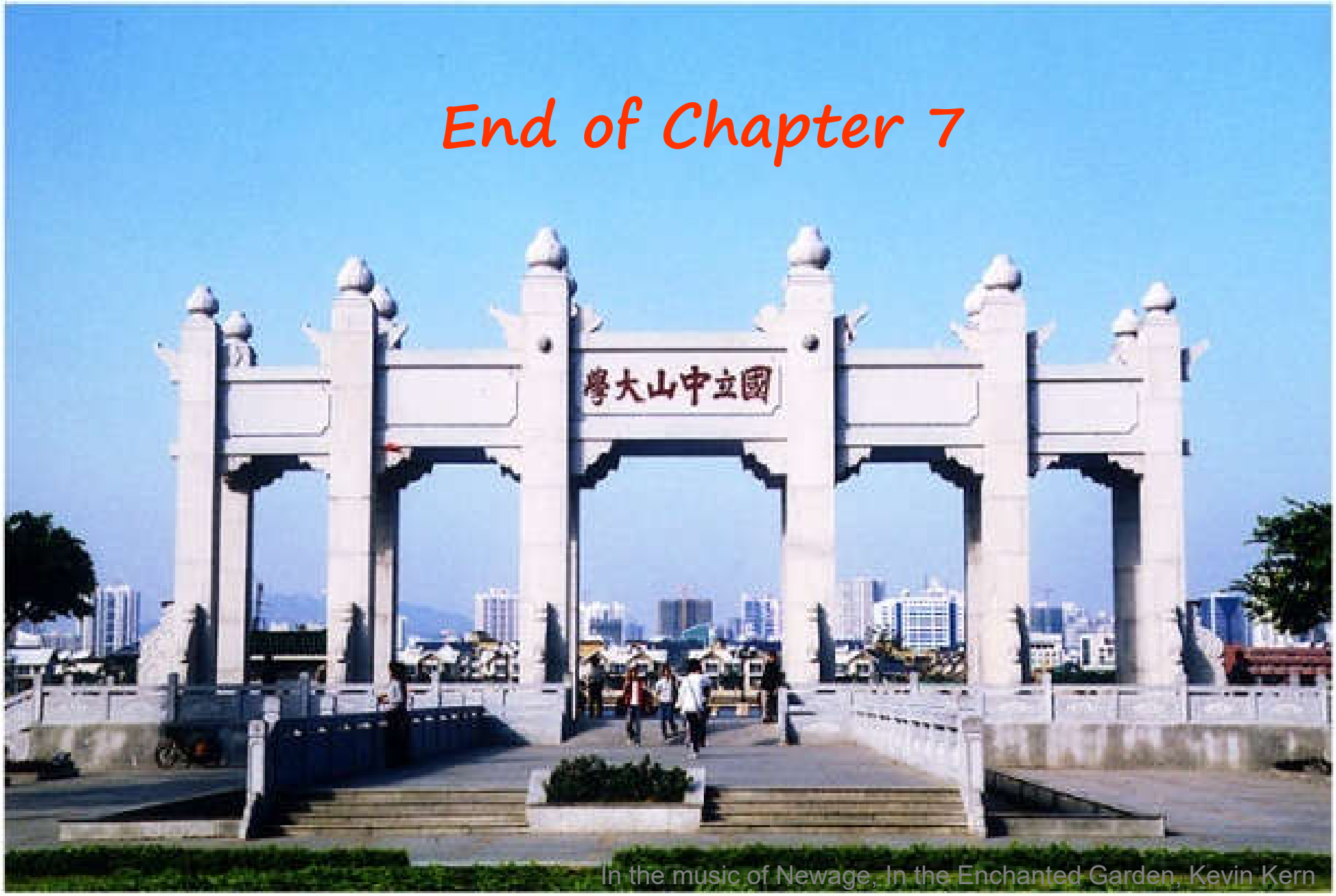
❑ IPS vs. IDS

- 部署
  - ✧ IDS 部署在网络内部的中心点，需要能够观察到所有网络数据。如果信息系统中包含了多个逻辑隔离的子网，则需要在整个信息系统中实施分布部署，即每子网部署一个入侵检测分析引擎，并统一进行引擎的策略管理以及事件分析，以达到掌控整个信息系统安全状况的目的。
  - ✧ IPS 为了实现对外部攻击的防御，需要部署在网络的边界。所有来自外部的数据受到 sensor 的串行或旁路监听，IPS 实时分析网络数据，发现攻击行为立即予以阻断，以保证来自外部的攻击数据不能通过网络边界进入网络。

References

1. The Practical Intrusion Detection Handbook, *Paul E. Proctor*
2. Computer Networks, fourth edition, *Andrew S. Tanenbaum*
3. Intrusion detection – Wikipedia, http://en.wikipedia.org/wiki/Intrusion_detection
4. Intrusion Detection System (IDS) : Dawn of the new Security http://zulcap.wordpress.com/2009/10/27/lecture-9-intrusion-detection-system-ids/
5. Guide to Intrusion Detection and Prevention Systems(IDPS), *Karen Scarfone*, *Peter Mell*, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-94
6. Intrusion prevention system, Wikipedia, http://en.wikipedia.org/wiki/Intrusion_prevention_system

End of Chapter 7



In the music of Newage, In the Enchanted Garden, Kevin Kern