# 网 络 安 全

## ——入侵检测

杭州师范大学信息科学与技术学院

刘雪娇　邮箱：liuxuejiao0406@163.com

# 本章节要求



- 了解IDS的概念和工作原理
- 学习通用入侵检测框架
- 了解数据捕获方式
- 学习IDS部署实例及方式

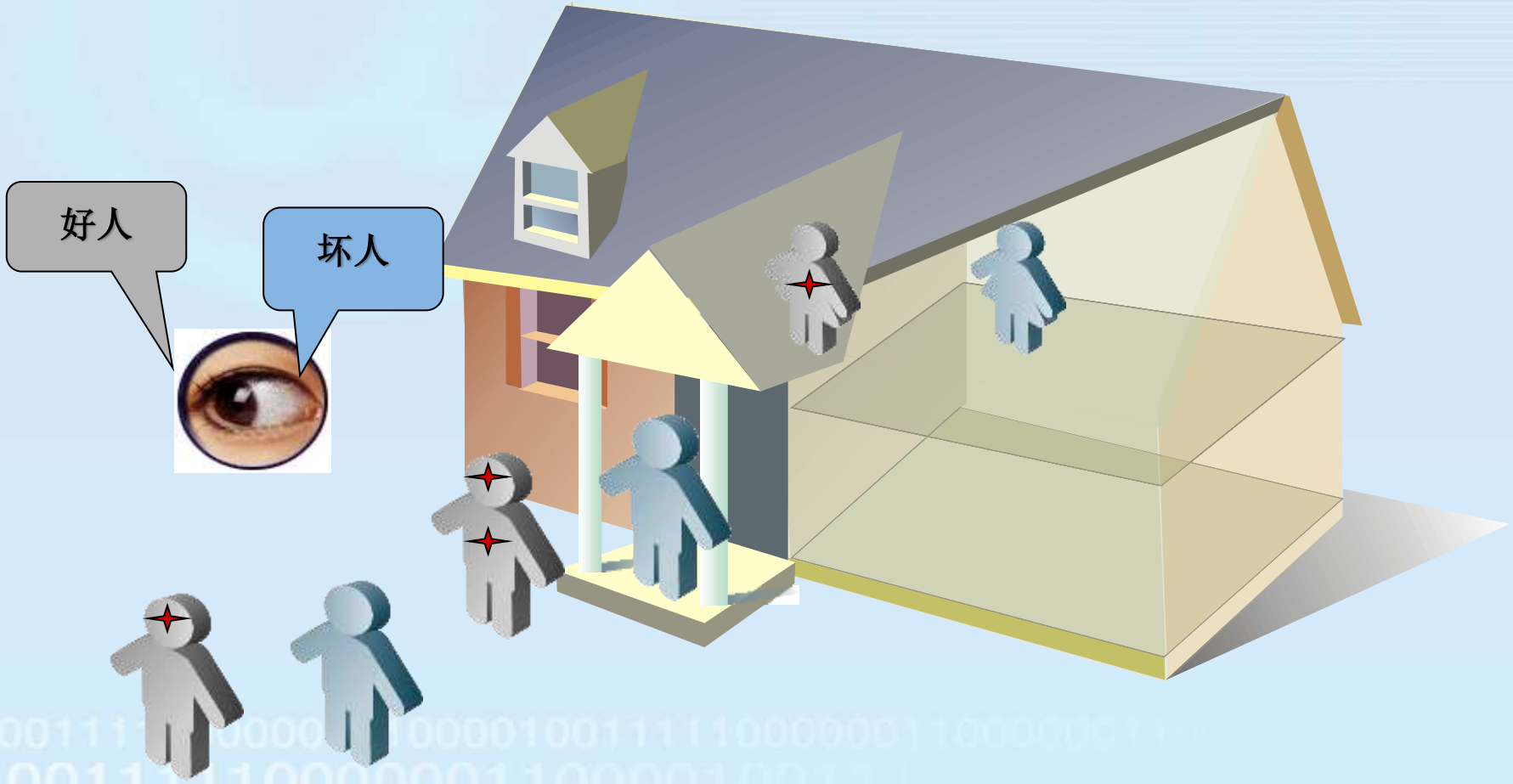

# 第十一章 入侵检测


# 什么是IDS

- 入侵(Intrusion)不仅包括发起攻击的人取得超出范围的系统控制权，也包括收集漏洞信息，造成拒绝访问等对计算机造成危害的行为。
- 入侵检测(Intrusion Detection)即通过从网络系统中的若干关键节点收集并分析信息，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。
- 入侵检测系统IDS（Intrusion Detection System）的概念
  - IDS是执行入侵检测的软件或硬件系统
  - 用于检测对网络的攻击
  - 对攻击的积极响应

# 什么是IDS





# IDS的起源与发展



- 概念的诞生—1980年
  - 美国空军做了题为《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
- 模型的发展—1984~1986年
  - 乔治敦大学的Dorothy Denning和SRI公司的计算机科学实验室Peter Neumann研究出了一个入侵检测模型，取名为IDES（入侵检测专家系统）。它独立于特定的系统平台、应用环境、应用弱点以及入侵类型真正提出的入侵检测思想
- 百花齐放—1990年
  - 美国加州大学第一次将网络数据流作为审计来源分析入侵活动，为入侵检测技术翻开新的一页。从此入侵检测技术分为网络入侵检测技术和主机入侵检测技术，并且两种方式不断壮大起来
- 里程碑—2000年
  - 分布式IDS出现

# IDS的主要作用



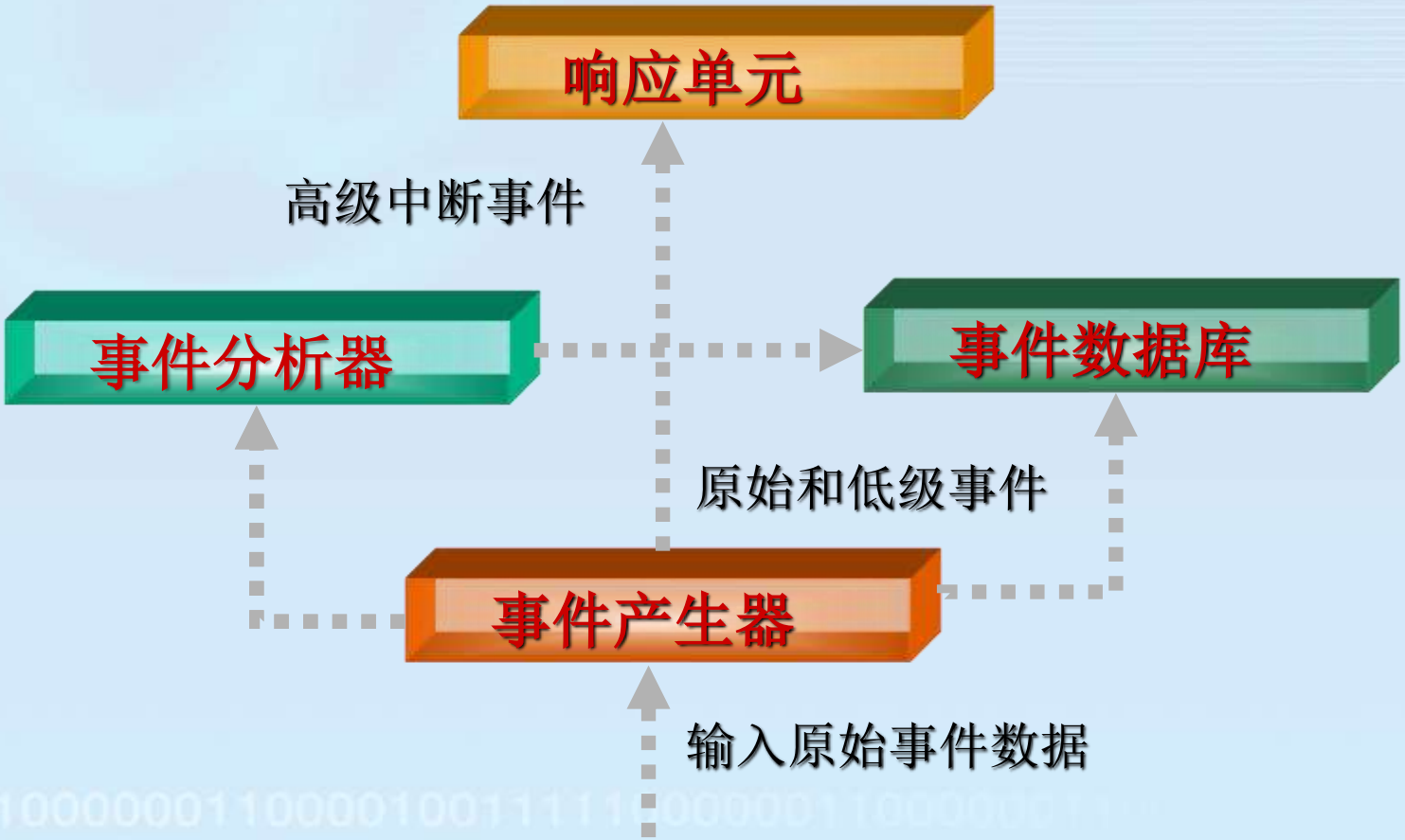
- 入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。
  - 监视、分析用户及系统活动；
  - 系统构造和弱点的审计；
  - 识别反映已知进攻的活动模式并向相关人士报警
  - 异常行为模式的统计分析；
  - 评估重要系统和数据文件的完整性；
  - 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。


# 通用入侵检测框架

- CIDF定义了IDS表达检测信息的标准语言以及IDS组件之间的通信协议。
- 符合CIDF规范的IDS可以共享检测信息、相互通信、协同工作，还可以与其他系统配合，协调实施统一的配置响应和恢复策略。
- CIDF的主要工作在于集成各种IDS使之协同工作，实现各IDS之间的组件重用，所以CIDF也是构建分布式IDS的基础。

# 入侵检测系统构件






# IDS的工作原理

- 根据检测方式：
  - 误用检测系统(misuse detection system)
  - 异常检测系统(anomaly detection system)
- 根据输入数据的来源：
  - 基于主机的入侵检测系统 (Host-Based IDS，HIDS)
  - 基于网络的入侵检测系统 (Network-Based IDS，NIDS)
- 检测方式：协议分析 、基于状态的检测
- 体系结构：集中式、分布式
- 工作方式：在线检测、离线检测

# IDS报警(Alert)



- 什么是报警
  - IDS检测到入侵活动时，都必须产生一些警报以发出信号
- 由于IDS没有100%的正确率，所以IDS报警分为两大类
  - 错误警报
    - ↘误报(false positive)

检测系统在检测时把系统的正常行为判为入侵行为的错误被称为误报；
检测系统在检测过程中出现误报的概率称为系统的误报率。

- ↘漏报(false negative)

检测系统在检测时把某些入侵行为判为正常行为的错误现象称为漏报；
检测系统在检测过程中出现漏报的概率称为系统的漏报率。

# 信息收集的来源



- 系统或网络的日志文件

  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，就包含登录、用户ID改变、用户对文件的访问、授权和认证信息等内容

  不正常的或不期望的行为就是重复登录失败、登录到不期望的位置以及非授权的企图访问重要文件等等

- 网络流量
- 系统目录和文件的异常变化

  网络环境中的文件系统包含很多软件和数据文件，包含重要信息的文件和私有数据文件经常是黑客修改或破坏的目标。

  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

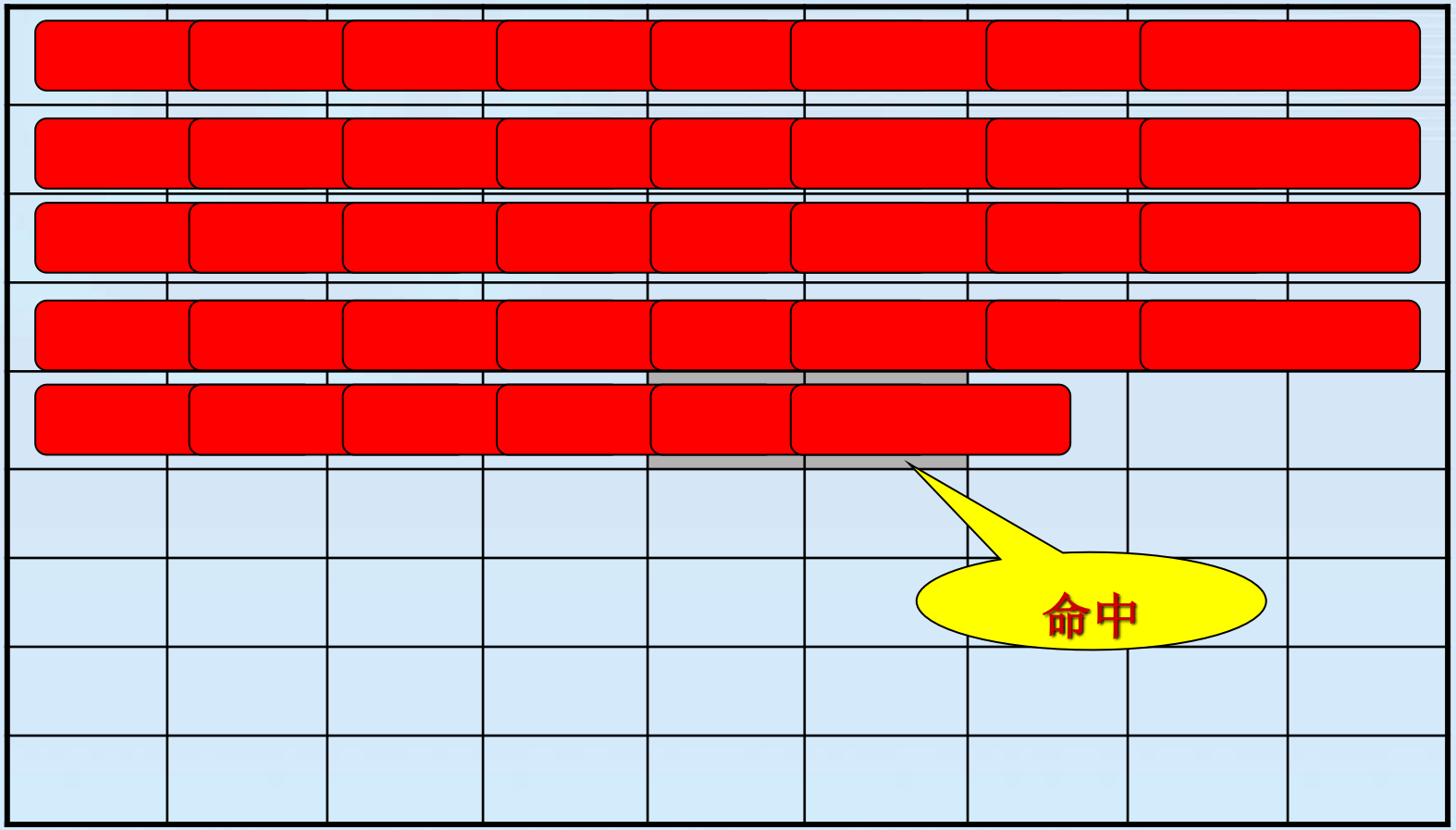
# 误用检测



- 概念
  - 也称为滥用检测，探测与具体特征(Signatures)相匹配的入侵行为，将收集到的信息与特征库匹配，即模式匹配。
- 优点
  - 基于已知的入侵行为
  - 安装后立刻就能进行检测
- 缺点
  - 需要更新签名库（特征库）
  - 有些攻击能绕过IDS
  - 无法检测未知攻击

# 模式匹配图示





# 异常检测



- 概念
  - 也称为模型检测，需要为用户习惯建立模型。模型为用户定义了行为特征，以及为用户执行正常任务定义了一个基线
- 优点
  - 检测以前未发布的攻击
- 缺点
  - 用户习惯改变时，必须更新用户模型
  - 很难把特定的攻击与报警相关联

# 入侵检测技术



- 基于专家系统的入侵检测技术
  - 根据专家对合法行为的分析经验来形成一套推理规则，然后在此基础上构成相应的专家系统，由此专家系统自动地进行攻击分析工作
  - 推理系统的效率较低
- 基于模型推理的入侵检测技术
  - 对已知入侵行为建立特定的模型，监视具有特定行为特征的活动，一但发现与模型匹配的用户行为，就通过相关信息证实或否定攻击的真实性
  - 又称为模式匹配，是应用较多的入侵检测方法

# 入侵检测技术

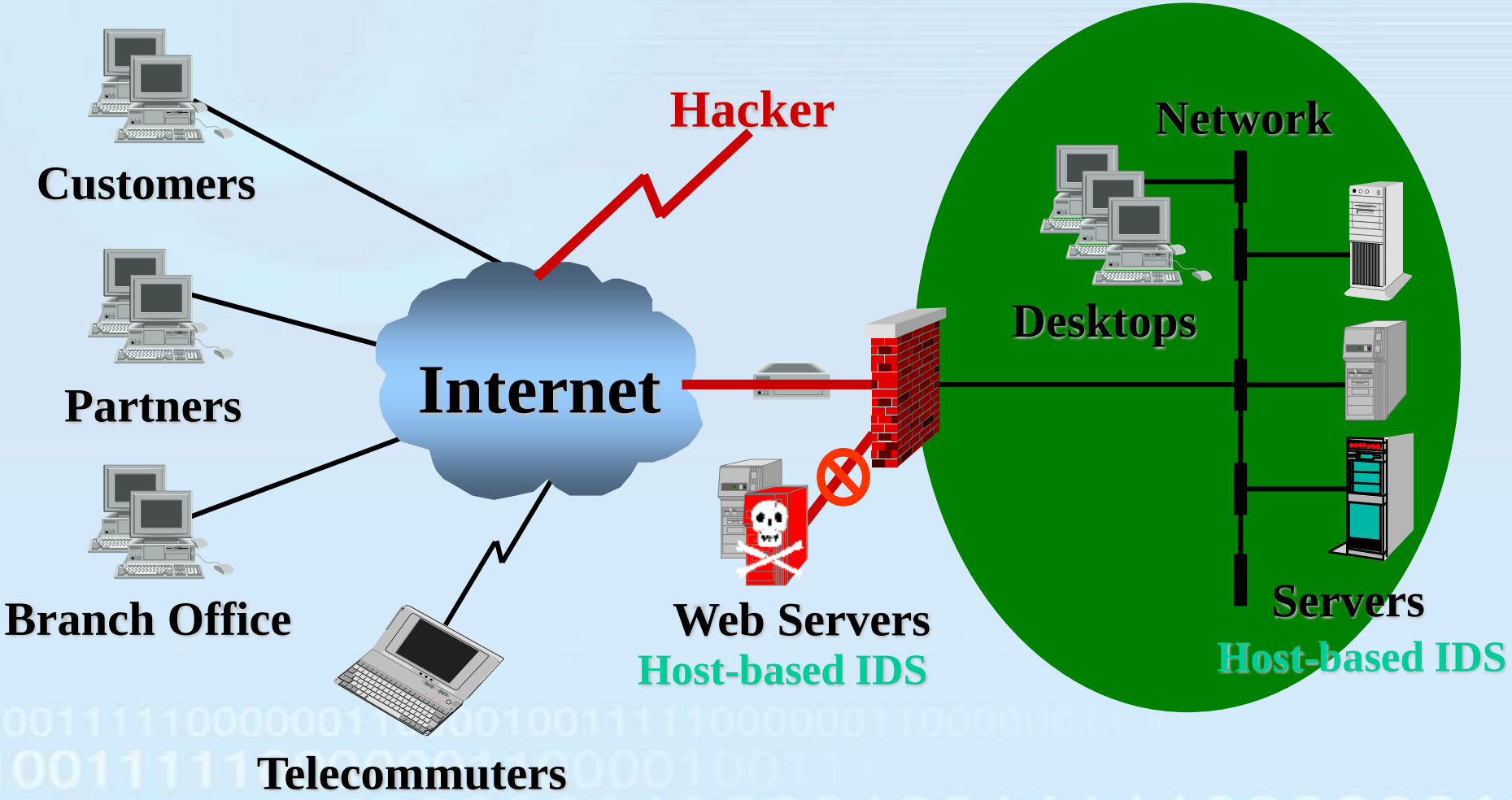


- 基于统计分析的入侵检测技术
  - 基于对用户历史行为进行统计，同时实时地检测用户对系统的使用情况，根据用户行为的概率模型与当前用户的行为进行比较，一但发现可疑的情况与行为，就跟踪、监测并记录，适当时采用一定的响应手段
  - 推理系统的效率较低有一定的自适应能力，稳定，但误警率高
- 基于神经网络的入侵检测技术
  - 将神经网络模型运用于入侵检测系统，可以解决基于统计数据的主观假设而导致的大量虚假警报问题，同时由于神经网络模型的自适应性，使得系统精简，成本较低

# HIDS（Host IDS）



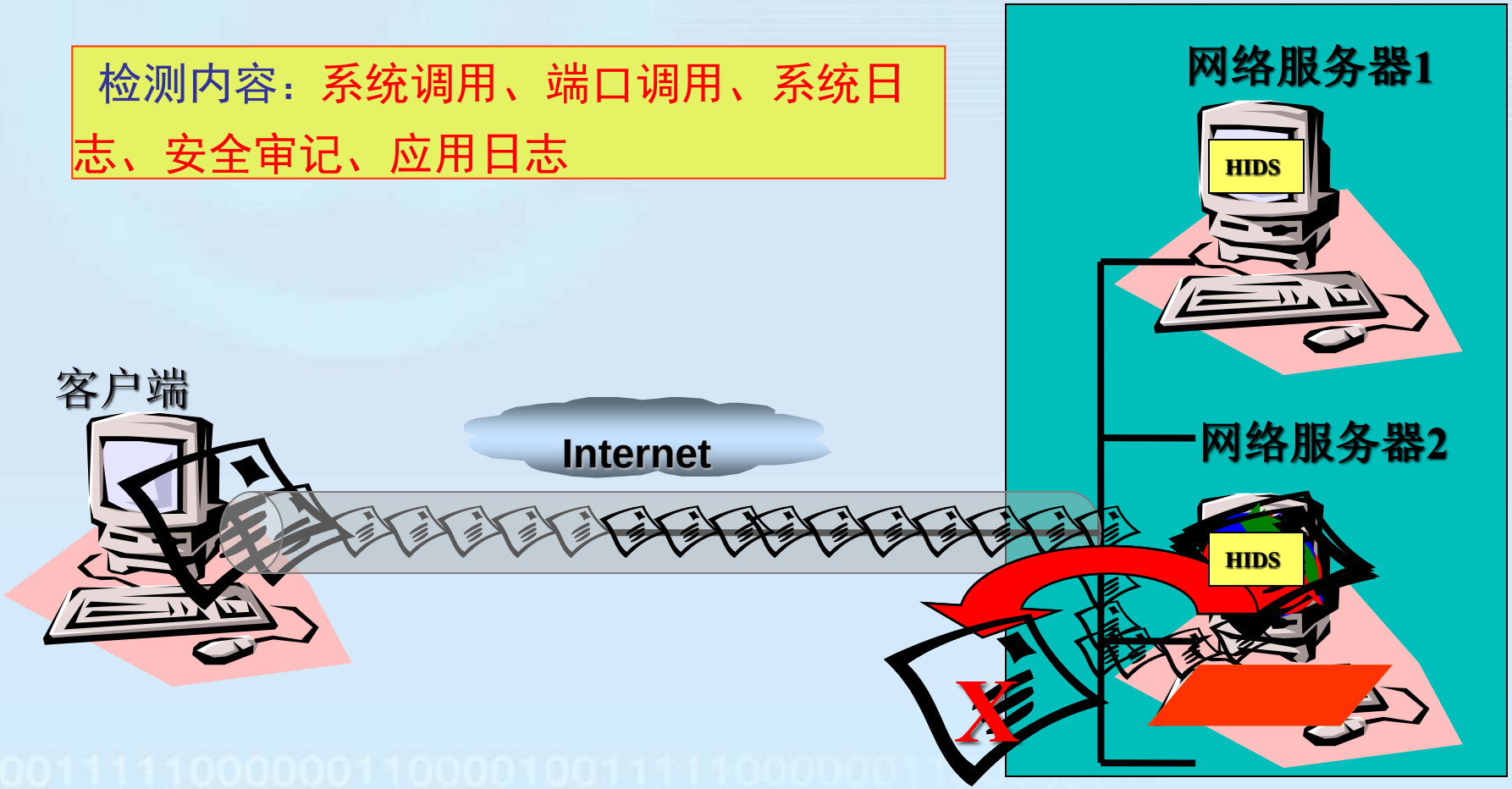
- 举例



# HIDS（Host IDS）



检测内容：系统调用、端口调用、系统日志、安全审记、应用日志



# HIDS（Host IDS）

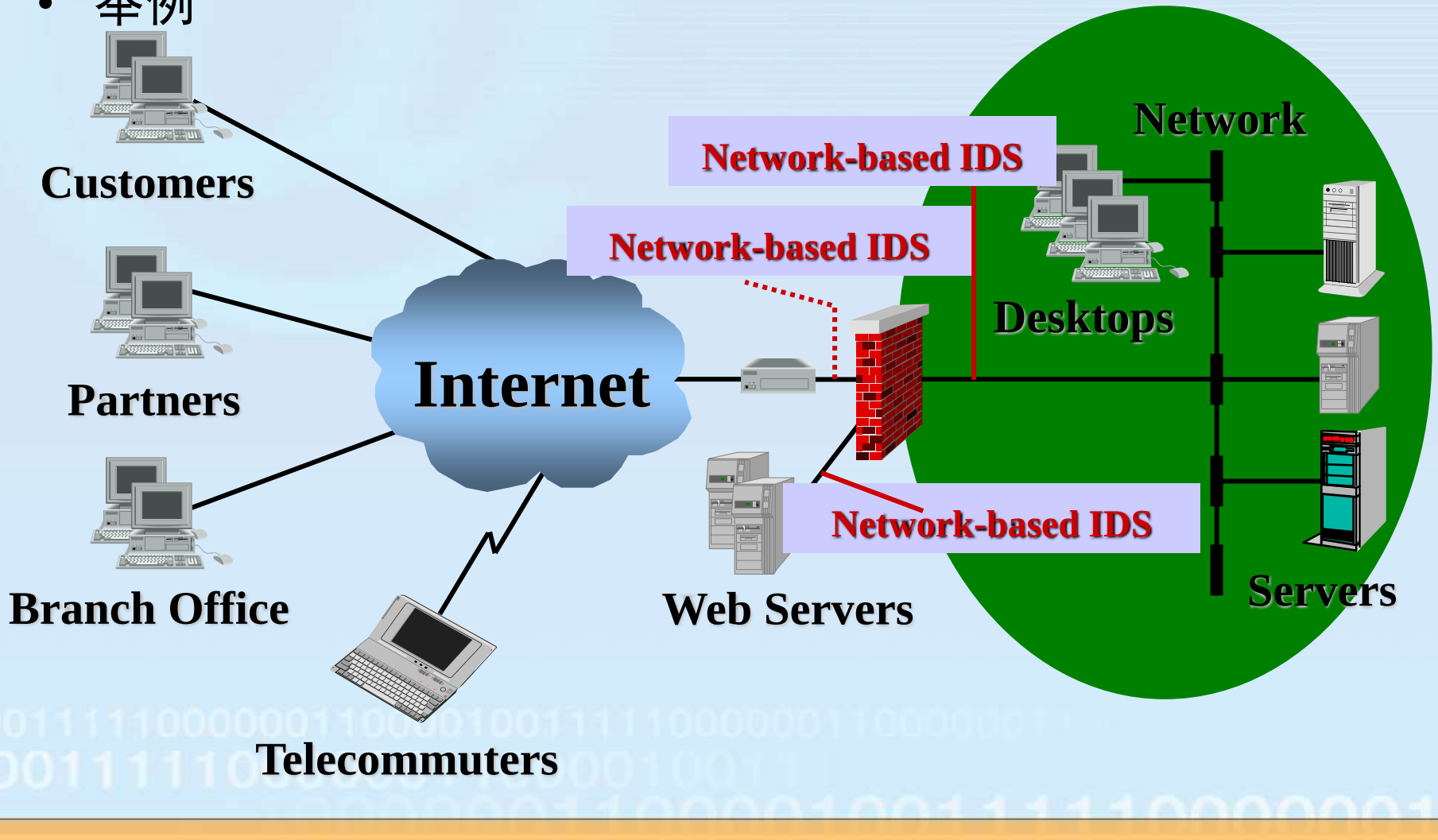


- 在最终目的进行分析
- 对网络的视野有限
- 性能问题
- 部署问题

# NIDS（Network IDS）



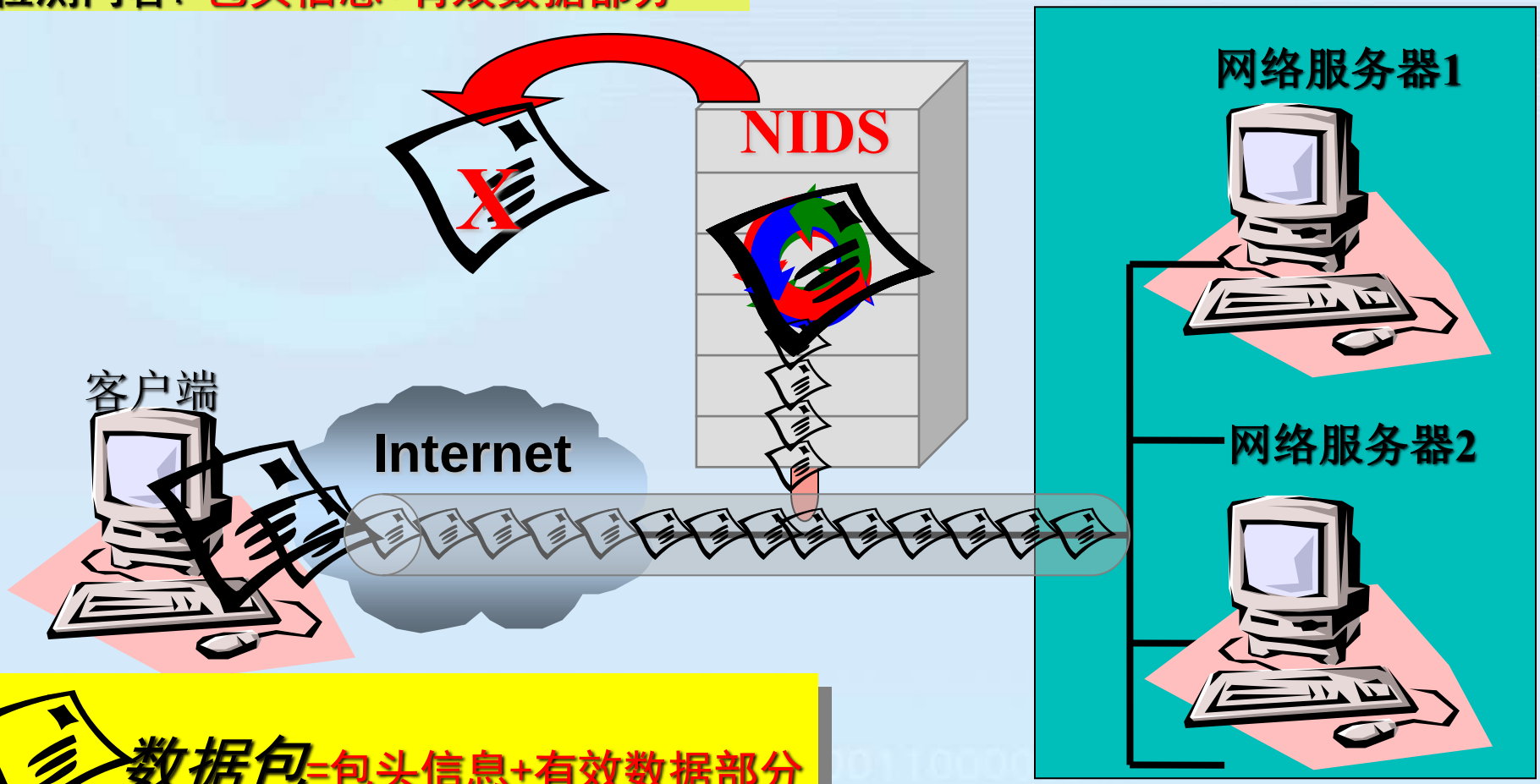
- 举例



# NIDS（Network IDS）



检测内容：包头信息+有效数据部分

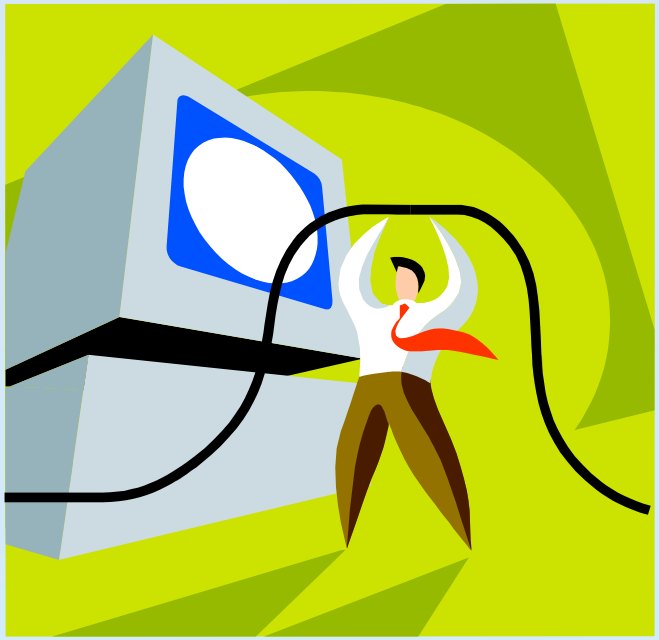



数据包=包头信息+有效数据部分

# NIDS（Network IDS）



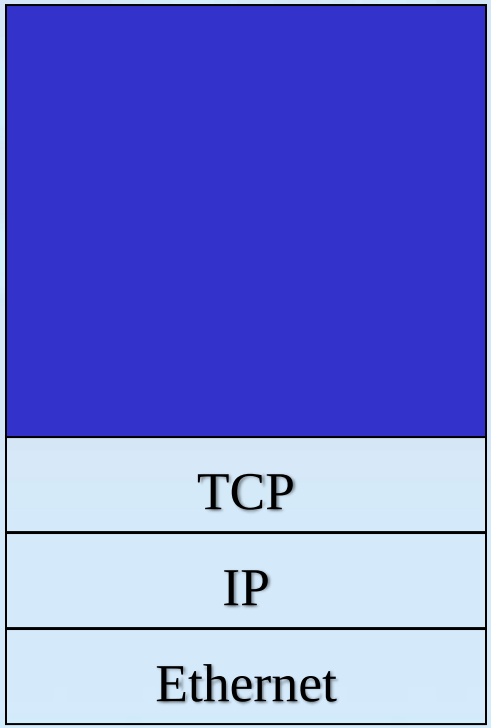
- 视野开阔
- 易于部署
- 带宽、性能问题
- 加密问题



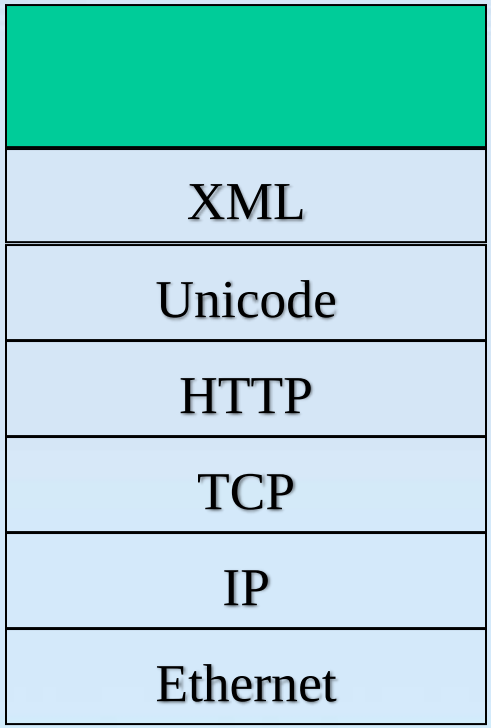
# 分析数据包



模式匹配




协议分析



# 一个攻击检测实例



- 老版本的Sendmail漏洞利用

```
$ telnet mail.victim.com 25
WIZ
shell
或者
DEBUG
#
直接获得rootshell!
```

# 简单的匹配



- 检查每个packet是否包含：

  “WIZ”
  | “DEBUG”

- 缩小匹配范围，检测端口号

  Port 25:{
  “WIZ”
  | “DEBUG”
  }

# 深入决策树

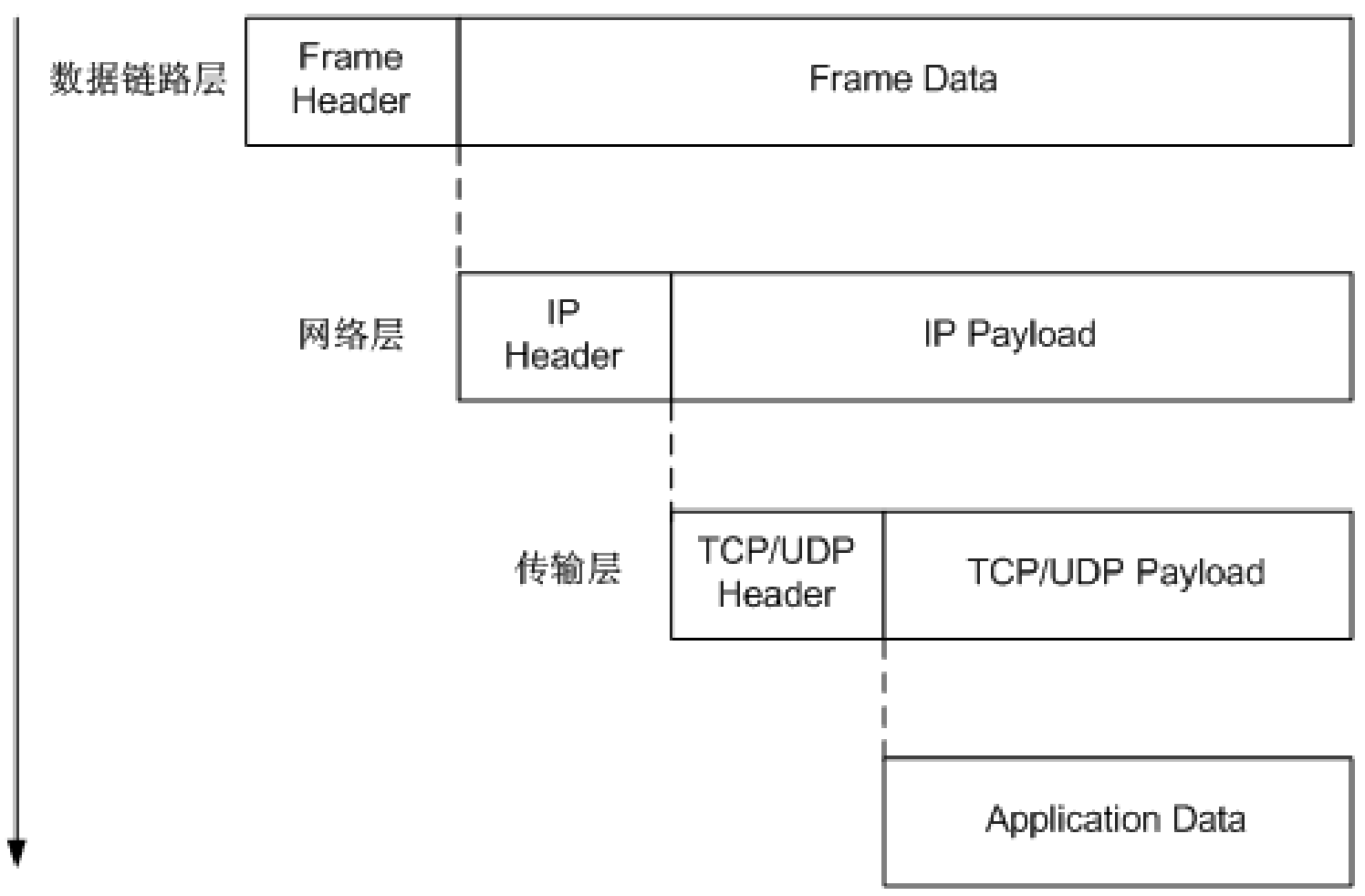


- 只判断客户端发送部分

Port 25:{
  Client-sends: “WIZ” |
  Client-sends: “DEBUG”
}

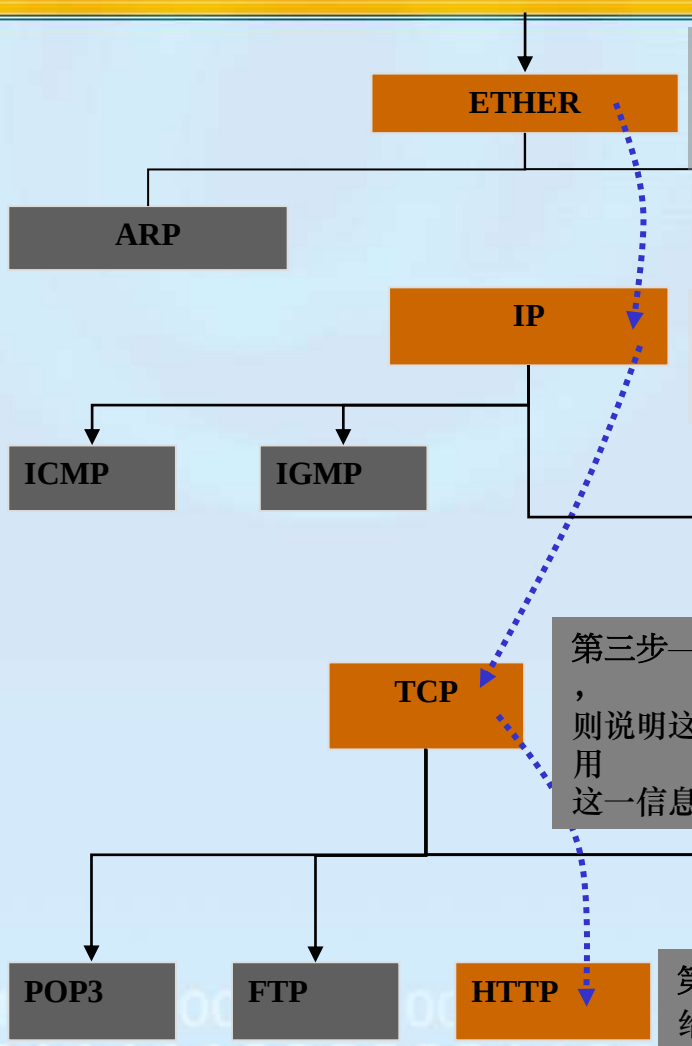
# 协议分析




数据链路层
Frame Header
Frame Data
网络层
IP Header
IP Payload
传输层
TCP/UDP Header
TCP/UDP Payload
Application Data

# 协议分析






第一步——直接跳到第13个字节，并读取2个字节的协议标识。
如果值是0800，则说明这个以太网帧的数据域携带的是IP包，
基于协议解码的入侵检测利用这一信息指示第二步的检测工作。

第二步——跳到第24个字节处读取1字节的第四层协议标识。
如果读取到的值是06，则说明这个IP帧的数据域携带的是TCP包，
入侵检测利用这一信息指示第三步的检测工作。

第三步——跳到第35个字节处读取一对端口号。如果有一个端口号是0080
，
则说明这个TCP帧的数据域携带的是HTTP包，基于协议解码的入侵检测利
用
这一信息指示第四步的检测工作。

第四步——让解析器从第55个字节开始读取URL。 URL串将被提交给HTTP解析器，在它被允许提交给Web服务器前，由HTTP解析器来分析它是否可能会做攻击行为。

# 协议解码



- Protocol Analysis
  - Ether、IP、ARP
  - TCP、UDP、ICMP
  - HTTP、Telnet、DNS、FTP、IRC、NetBIOS、SMB、SMTP、SNMP、TFTP、RPC、POP3、Finger、rlogin、MIME、IMAP4、VNC、RealAudio、NetGames、MS SQL

# 优势



- 提高了性能：协议分析利用已知结构的通信协议，与模式匹配系统中传统的穷举分析方法相比，在处理数据帧和连接时更迅速、有效。
- 提高了准确性：与非智能化的模式匹配相比，协议分析减少了虚警和误判的可能性，命令解析（语法分析）和协议解码技术的结合，在命令字符串到达操作系统或应用程序之前，模拟它的执行，以确定它是否具有恶意。
- 基于状态的分析：当协议分析入侵检测系统引擎评估某个包时，它考虑了在这之前相关的数据包内容，以及接下来可能出现的数据包。与此相反，模式匹配入侵检测系统孤立地考察每个数据包。
- 反规避能力：因为协议分析入侵检测系统具有判别通信行为真实意图的能力，它较少地受到黑客所用的像URL编码、干扰信息、TCP/IP分片等入侵检测系统规避技术的影响。
- 系统资源开销小：协议分析入侵检测系统的高效性降低了在网络和主机探测中的资源开销，而模式匹配技术却是个可怕的系统资源消费者。

# 入侵检测分类



- 按照体系结构
  - 集中式：有多个分布于不同主机上的审计程序，但只有一个中央入侵检测服务器。审计程序把当地收集到的数据踪迹发送给中央服务器进行分析处理。（可伸缩性、可配置性差）
  - 分布式：将中央检测服务器的任务分配给多个HIDS，它们不分等级，负责监控当地主机的可疑活动。（可伸缩性、安全性高；但维护成本高，监控主机的工作负荷重）

# 入侵检测分类

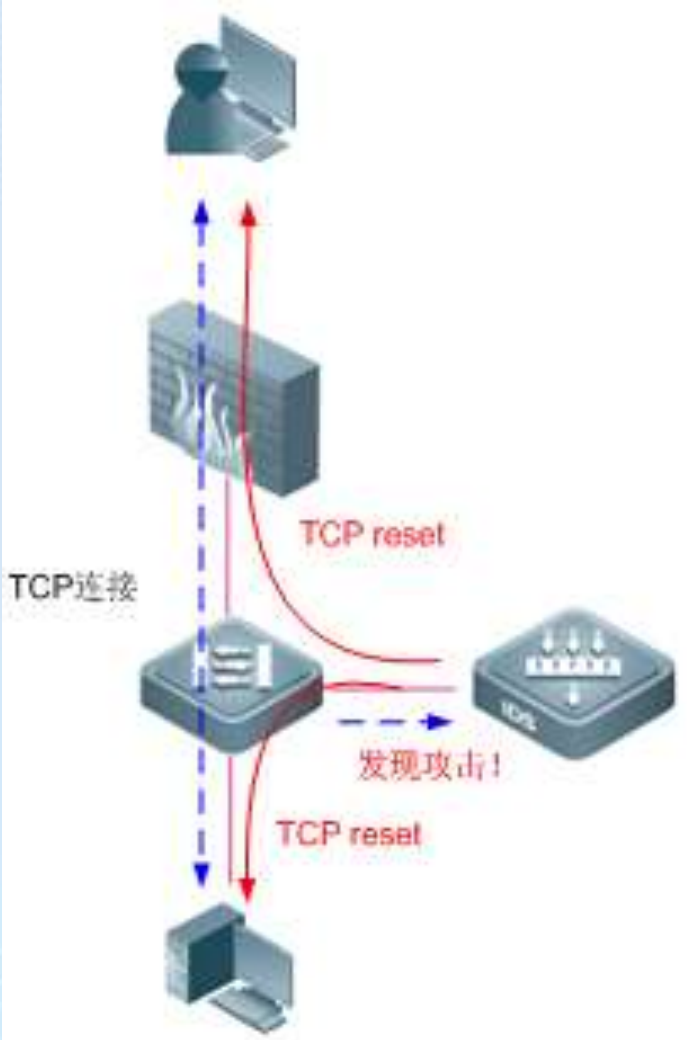


- 按照工作方式
  - 离线检测：非实时工作，在行为发生后，对产生的数据进行分析。（成本低，可分析大量事件、分析长期情况；但无法提供及时保护）
  - 在线检测：实时工作，在数据产生的同时或者发生改变时进行分析（反应迅速、及时保护系统；但系统规模较大时实时性难以得到实际保证）

# IDS响应技术



- 报警
- 记录日志
- TCP reset
- 联动
- SNMP Trap
- 邮件通知



# IDS逃避技术



- 泛洪
  - 使IDS产生大量警报，隐藏真正攻击
  - 消耗IDS系统资源
- 分片
  - 消耗IDS系统资源
- 加密
- 迷惑
  - 使用不同的字符表达方式

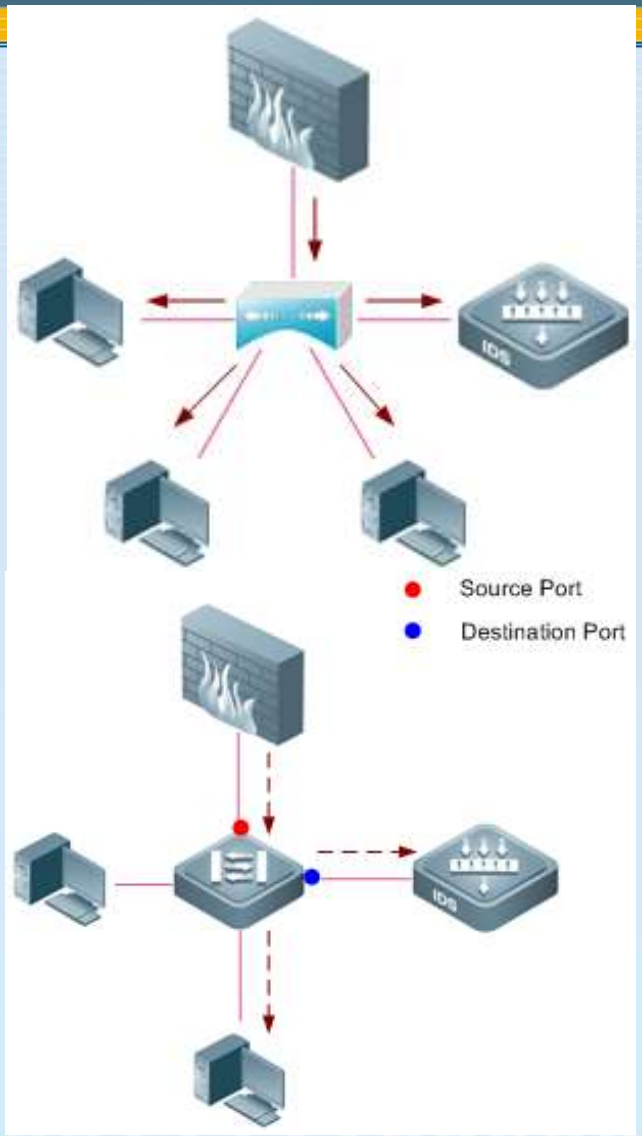

# 数据捕获方式

以太网接口的工作模式

- 正常模式
  - 只接收目的MAC与自己MAC匹配的报文
  - 接收广播报文
- 混杂模式
  - 接收所有报文（目的MAC非自身MAC的报文）
  - IDS接口为混在模式(Promiscuous)

- 物理层设备
- 将流量向所有端口复制
- 安全问题

- SPAN（Switch Port Analyzer）
  - 交换机的端口监控功能
  - 将一个或多个来自某端口或VLAN的数据镜像到另一个目的端口
  - 目的端口常用来连接网络分析仪
  - 安全性高



# 配置SPAN



**Switch(config)#**

**monitor session** *session-number* **source interface** *interface* {**both** | **rx** | **tx**}

- 配置端口镜像的源端口

**Switch(config)#**

**monitor session** *session-number* **destination interface** *interface*

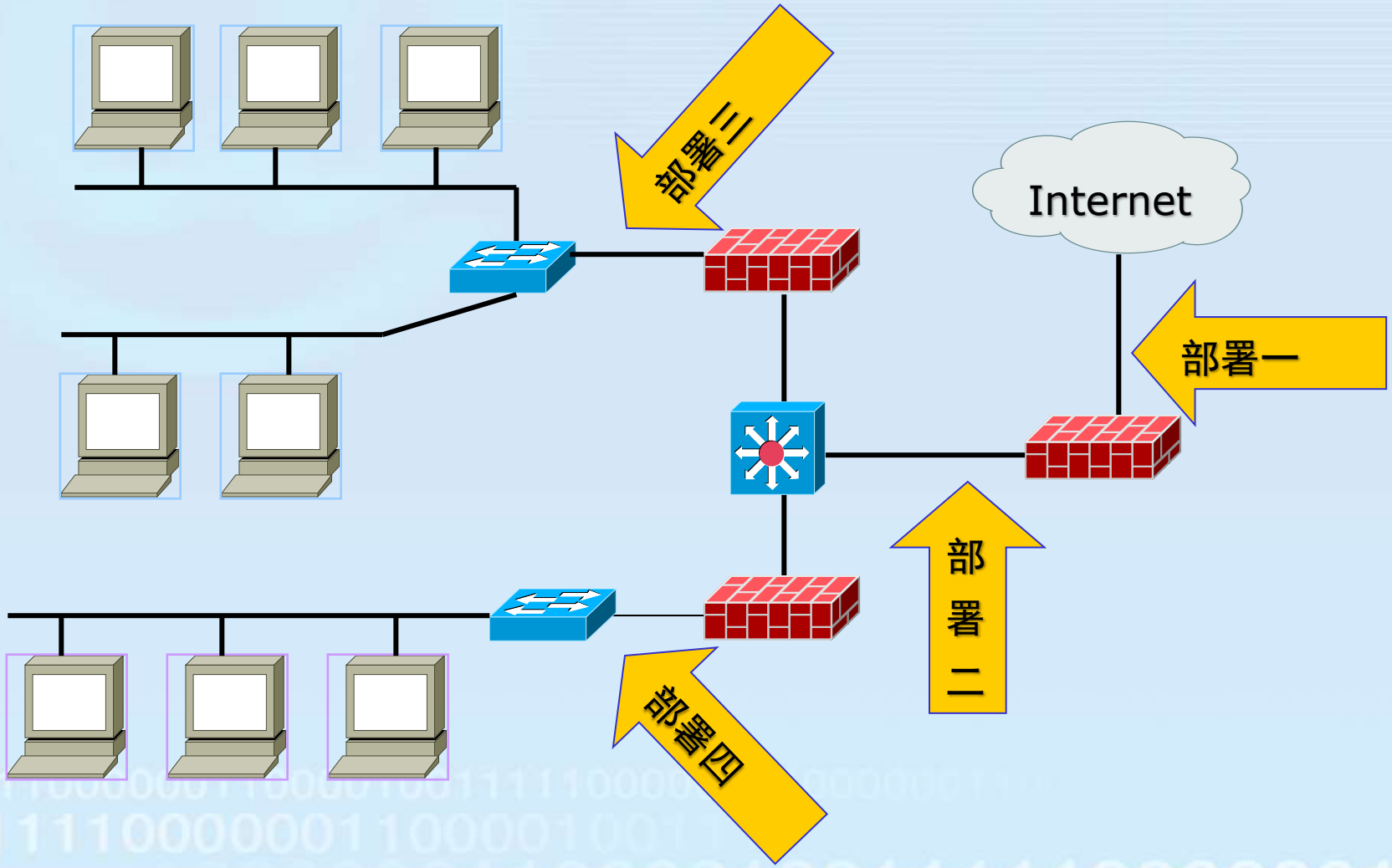
- 配置端口镜像的目的端口


# IDS部署方式

- 检测器部署位置
  - 放在边界防火墙之内
  - 放在边界防火墙之外
  - 放在主要的网络中枢
  - 放在一些安全级别需求高的子网

# 检测器部署示意图





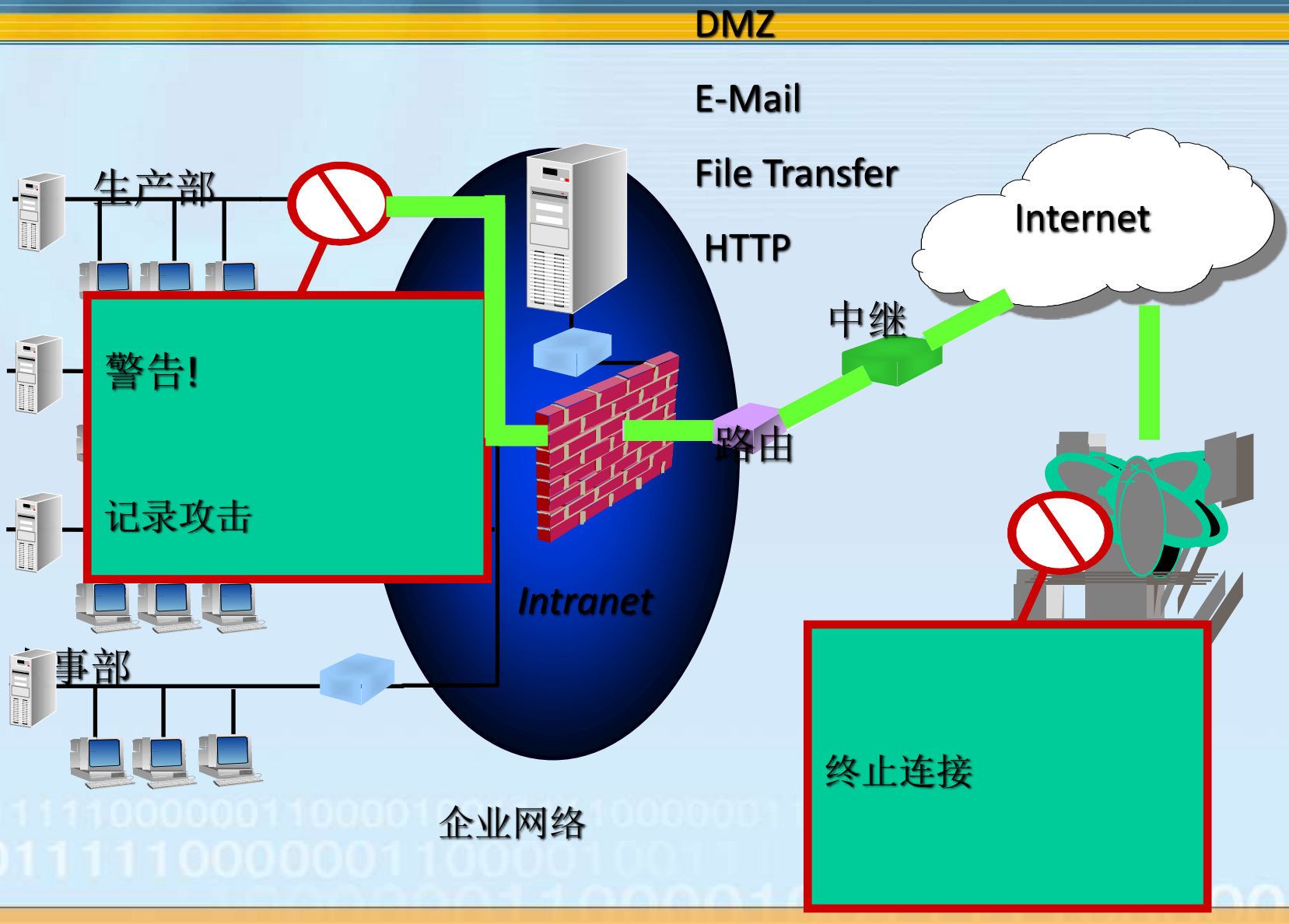

# IDS部署实例

Snort IDS是一个基于软件的入侵检测系统，是一个开放源代码的、功能强大的、轻量级的入侵检测与防御系统。

- 它能实现实时网络流量分析、报警、阻断数据包以及对数据包进行日志记录等功能。
- 它能将协议分析技术和模式匹配技术进行组合以进行异常、误用和攻击检测。

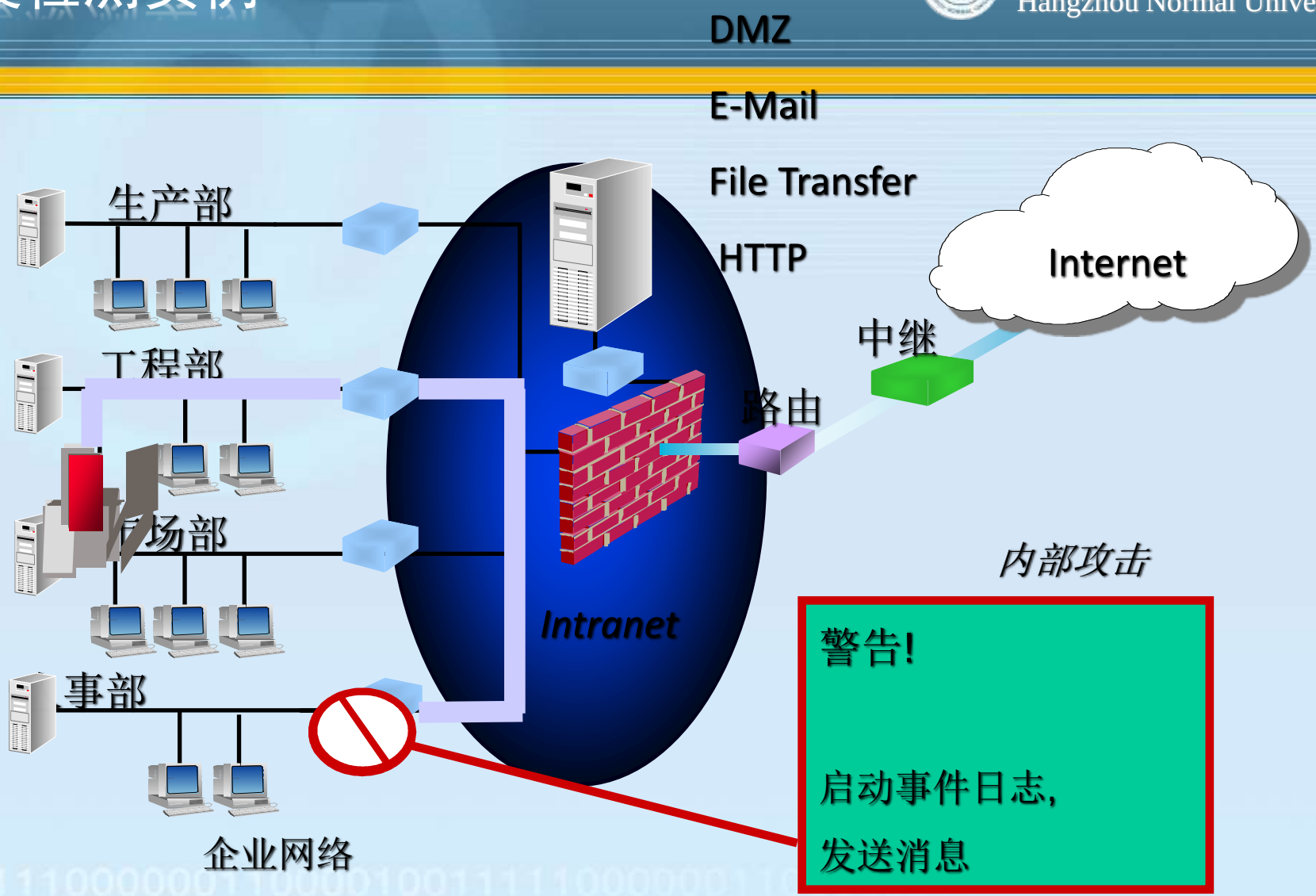
# 入侵检测实例




DMZ
E-Mail
File Transfer
HTTP
Internet
中继
生产部
警告!
记录攻击
路由
Intranet
事部
终止连接
企业网络

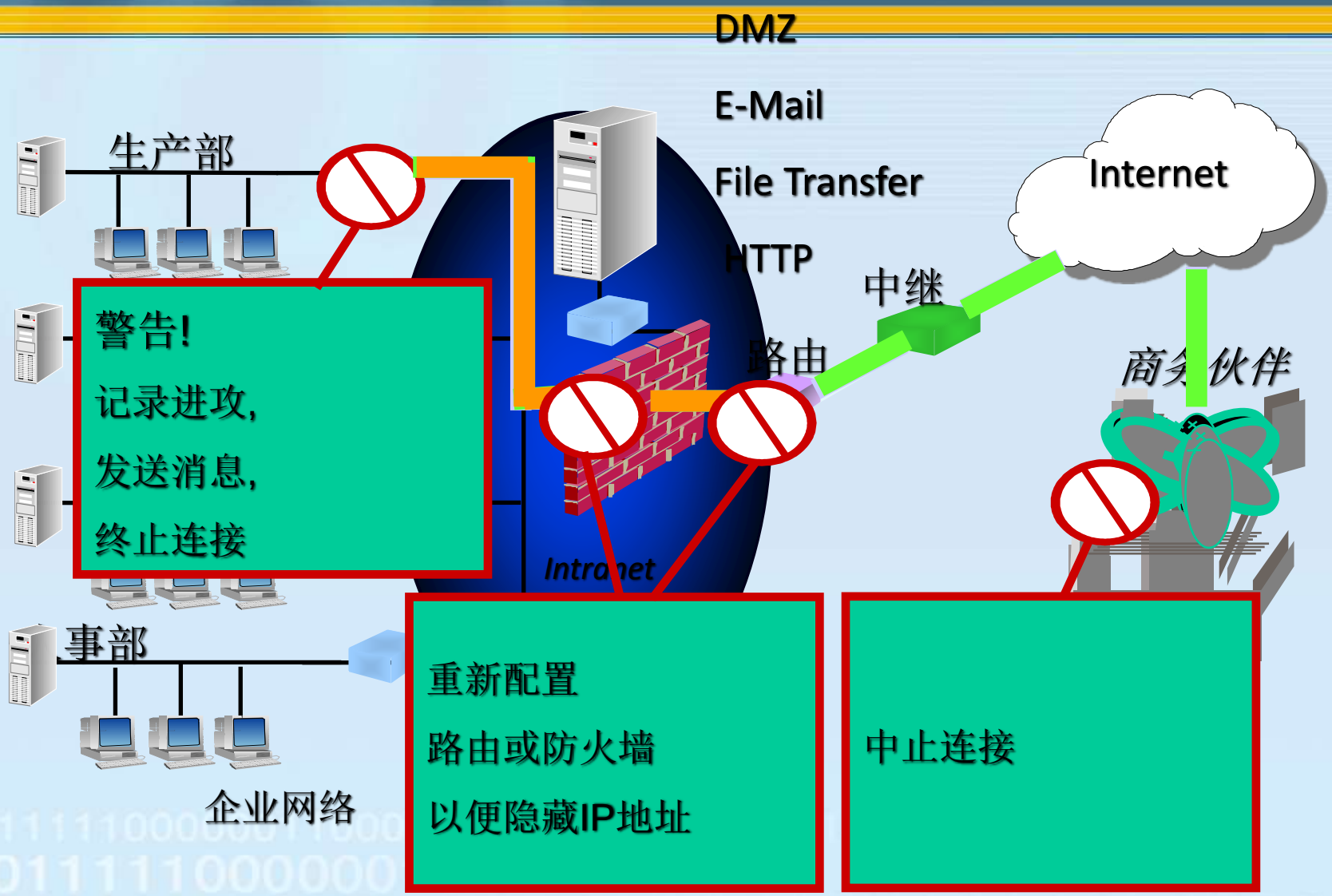
# 入侵检测实例




DMZ
E-Mail
File Transfer
HTTP
Internet
中继
路由
生产部
工程部
市场部
事部
Intranet
企业网络
内部攻击
警告!
启动事件日志,
发送消息

# 入侵检测实例




DMZ
E-Mail
File Transfer
HTTP
生产部
Internet
中继
路由
警告!
记录进攻,
发送消息,
终止连接
Intranet
事部
企业网络
重新配置
路由或防火墙
以便隐藏IP地址
中止连接

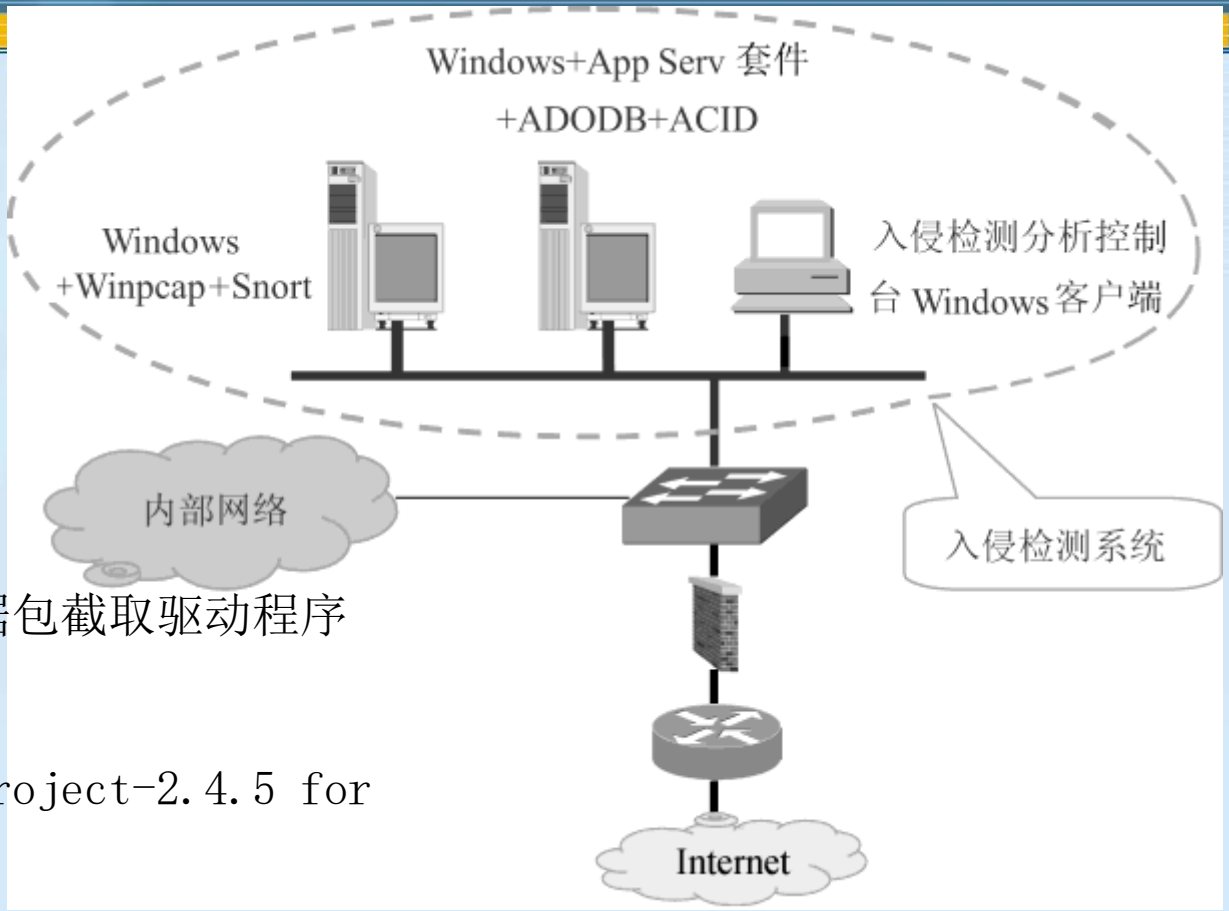
# Snort入侵检测系统简介



- Snort有三大主要功能模块
  - 能像TCPdump那样作为包嗅探工具
  - 也能作为包日志器（这对网络流量跟踪非常有用)
  - 还能作为全方位的网络入侵检测及防御系统。

# Snort入侵检测系统安装






1. 安装Windows系统中的数据包截取驱动程序
2. 安装Snort入侵检测系统
3. 安装The AppServ Open Project-2.4.5 for Windows
4. ACID软件包的安装
5. ADODB软件包的安装
6. 安装PHP的图形库

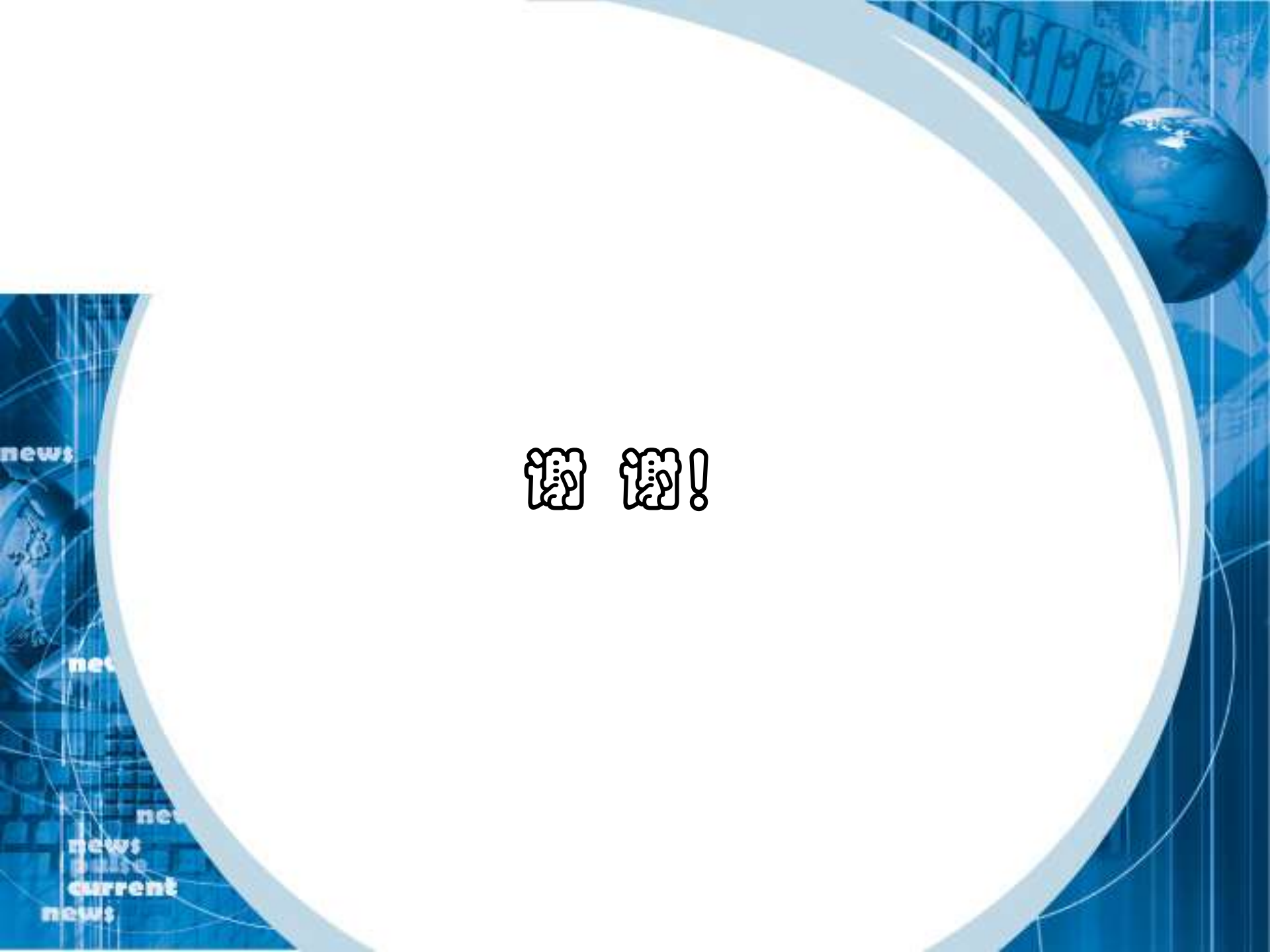

# IDS发展方向

- 面临的问题
  - 入侵者会研制更多的攻击工具，以及使用更为复杂精致的攻击手段，对更大范围的目标类型实施攻击；
  - 入侵者采用加密手段传输攻击信息；
  - 日益增长的网络流量导致检测分析难度加大；
  - 不适当的自动响应机制存在着巨大的安全风险；
  - 存在对入侵检测系统自身的攻击,体系结构存在单点失效和可扩展性有限等问题；
  - 过高的错报率和误报率，导致很难确定真正入侵行为；
  - 采用交换方法限制了网络数据的可见性；
  - 高速网络环境导致很难对所有数据进行高效实时分析

# 发展方向



- 更有效的集成各种入侵检测数据源，包括从不同的系统和不同的传感器上采集的数据，提高报警准确率。
- 对入侵检测系统与防病毒工具、防火墙、VPN等其他安全产品协同工作方面的研究
- 研制可靠的测试和评估标准；
- 提供对更高级的攻击行为如分布式攻击、拒绝服务攻击等的检测手段；
- 智能入侵检测的研究


news
current
news