专业特色选修课《网络信息安全》

黑客攻防和入侵检测技术

下篇

Hackers' Game and Intrusion Detection

嵩天 教授、博士生导师

songtian@bit.edu.cn

北京理工大学网络空间安全学院

本节大纲

- **入侵检测系统概述**
- **入侵检测/防御方法**
- **入侵检测/防御系统的部署**

入侵检测系统概述

- **为何需要入侵检测系统?**
  - **防火墙是网络系统的第一道安全闸门**
  - **当开放特定端口后，防火墙无法区应用类型**
  - **为此，需要更深层次的防御技术**
  - **入侵检测系统是方法之一**

入侵检测系统概述

- **什么是入侵检测?**
- **IDS – Intrusion Detection System**
  - **入侵：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。（1980年）**
  - **入侵检测：对企图入侵、正在进行的入侵或已经发生的入侵进行识别的过程。**

入侵检测系统概述

- **入侵检测的最初作用**
  - **入侵检测，作为增强网络系统安全性和追究入侵者法律责任的依据。**
  - **它从计算机网络系统中的若干关键点收集信息，并分析这些信息，检查网络中违反安全策略的行为和遭到袭击的迹象。**

入侵检测系统概述

- **什么是入侵防御?**
  - **可以理解为：实时入侵检测系统**
  - **以实时发现并阻断入侵为主要目的，取证为次要目的**
  - **当发现网络入侵现象，可以采用适当的方式进行攻击阻断（相当于：入侵检测与防火墙的联动）**

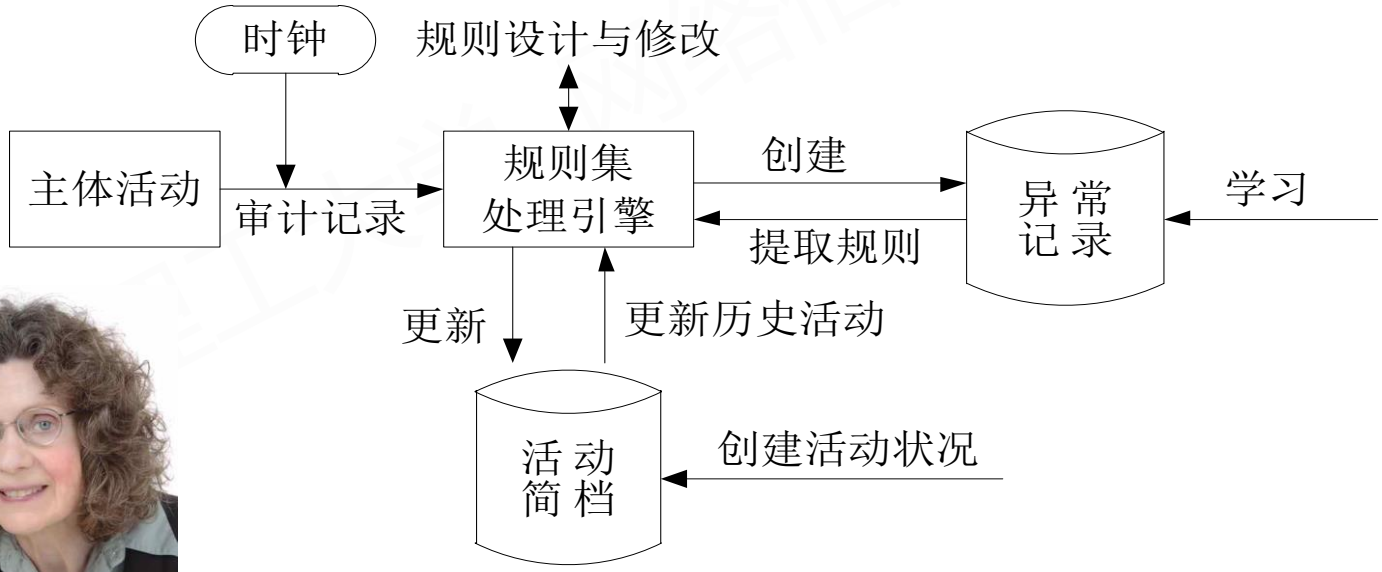
入侵检测系统概述

- **入侵检测系统的作用**
  - **监控网络和系统**
  - **发现入侵企图或异常现象**
  - **实时报警**
  - **主动响应**
  - **审计跟踪**

形象地说，网络入侵检测系统就是网络摄像机，能够捕获并记录网络上的所有数据，能够分析网络数据并提炼出可疑的、异常的网络行为。

入侵检测系统概述

- **入侵检测的发展历程**
  - **1980年， James P.Anderson首先提出了入侵检测的概念**
  - **1987年， Dorothy Denning提出了入侵检测模型**



Denning入侵检测抽象模型

入侵检测系统概述

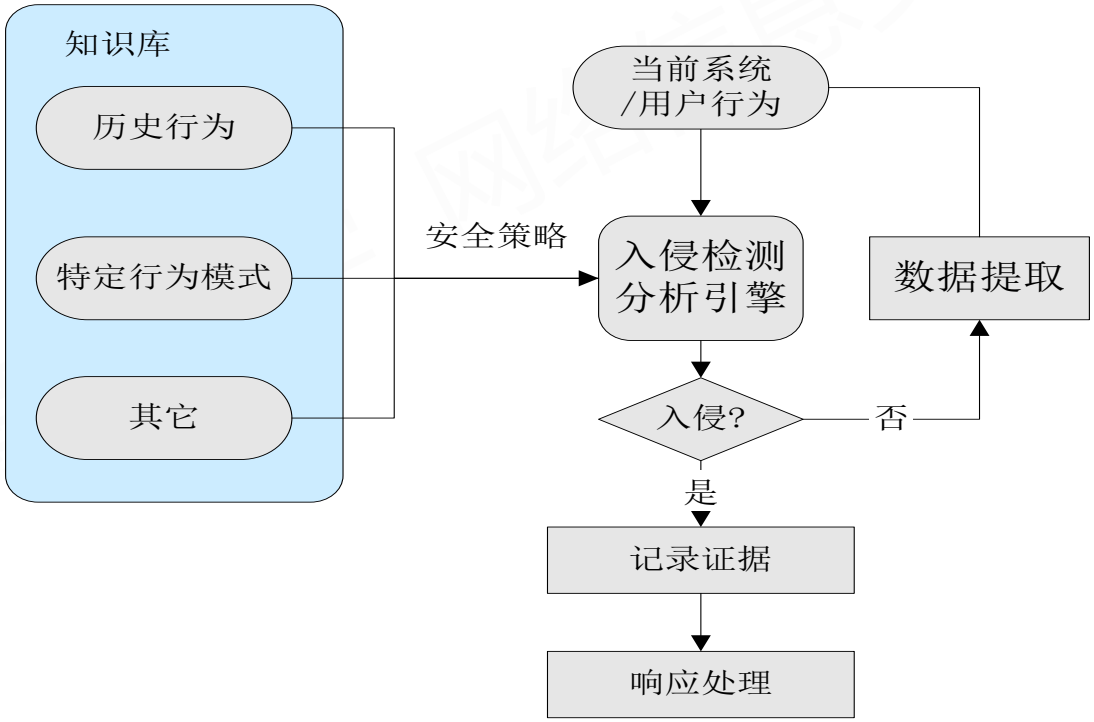
- **入侵检测的发展历程**
  - **1988年， Teresa Lunt等人改进了Denning的入侵检测模型，创建了IDES（Intrusion Detection Expert System）**
  - **1999年， Heberlein等人提出了一个具有里程碑意义的新型概念：基于网络的入侵检测（90年代网络大发展）**
  - **近年来，入侵检测技术研究的主要创新有：将大数据及深度学习方法运用于分布式入侵检测领域**
  - **至今，入侵检测模型仍在研究和改进中**

入侵检测系统概述

- **入侵检测的分类**
  - **入侵检测系统根据数据来源的不同，采用不用的实现方式，一般地可分为主机型、网络型和混合型。**
  - **基于主机的入侵检测系统（HIDS: Host-based IDS）**
  - **基于网络的入侵检测系统（NIDS: Network-based IDS）**
  - **混合型入侵检测系统（Hybrid IDS）**

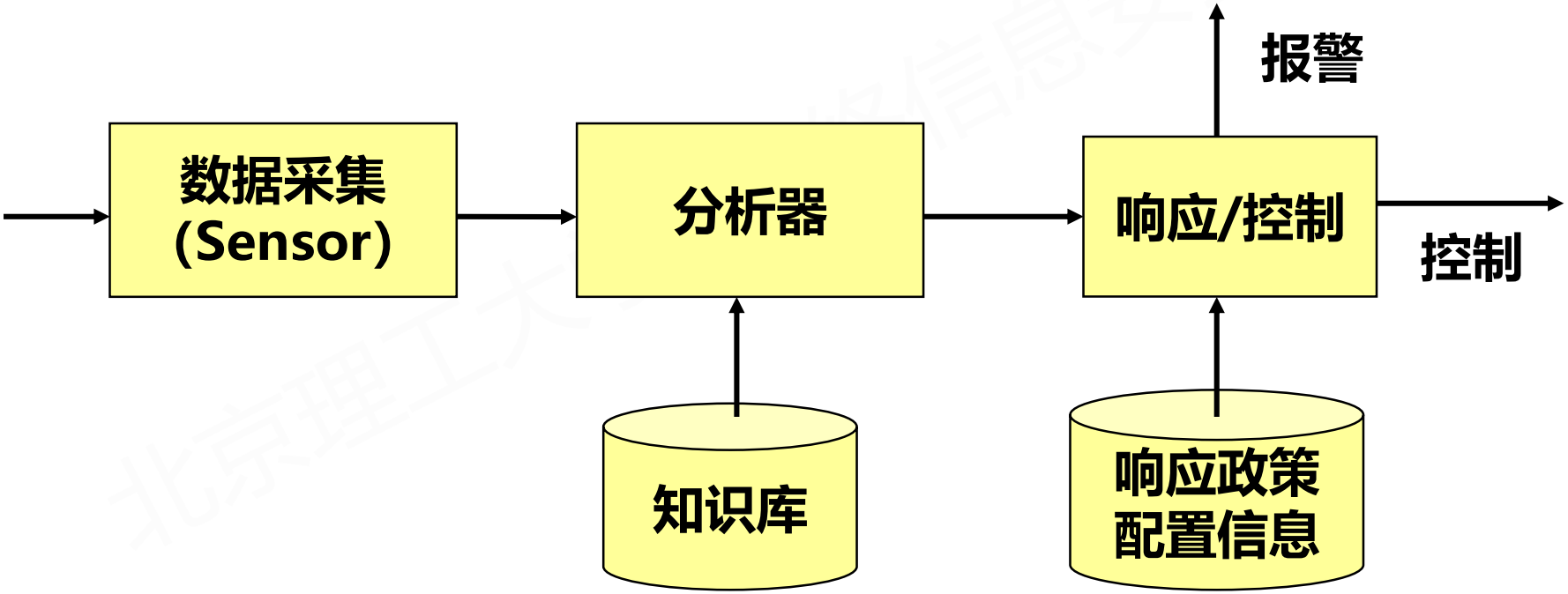
入侵检测系统概述

- **入侵检测系统的一般结构**
  - **主机入侵检测系统**



入侵检测系统概述

- **入侵检测系统的一般结构**
  - **网络入侵检测系统 （与 主机入侵检测系统 具有同样的模型）**



入侵检测系统概述

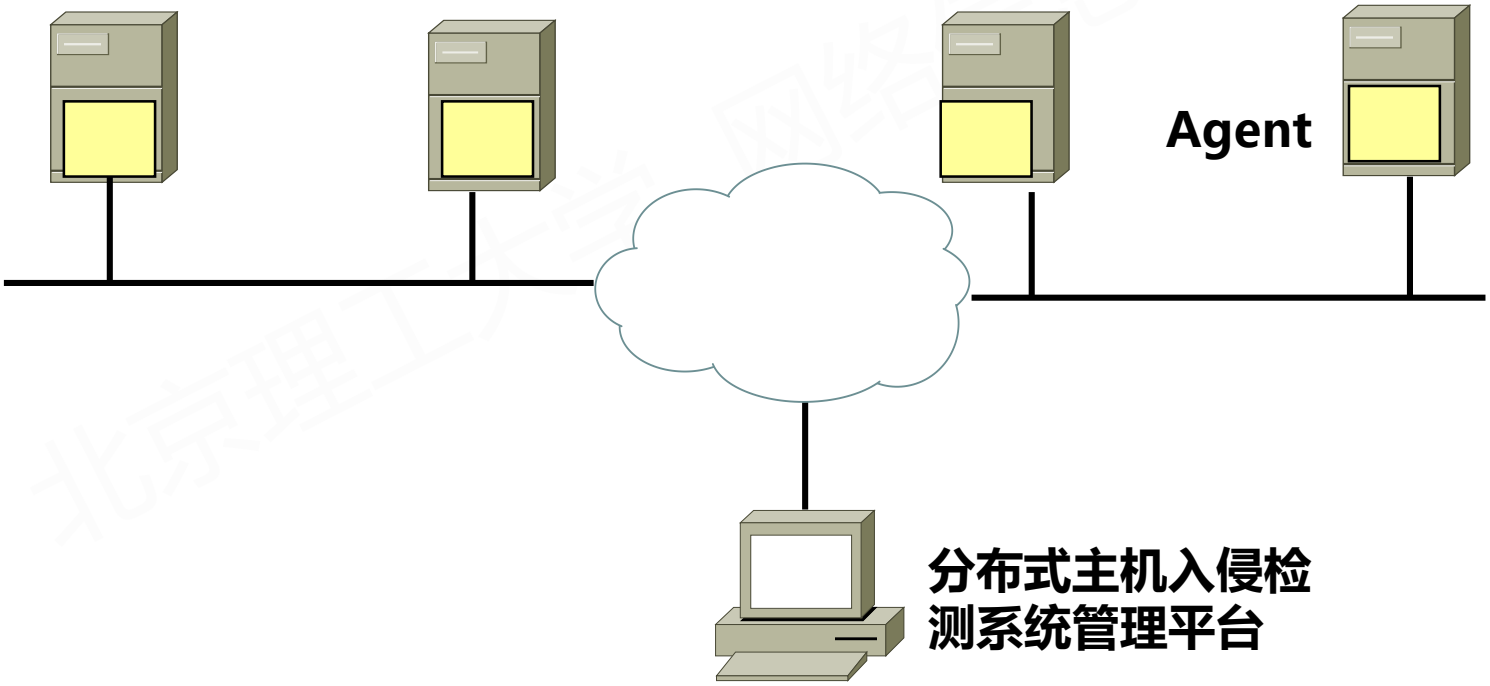
- **基于主机的入侵检测系统**
  - **信息来源**
    - **系统状态信息（CPU, Memory, Network）**
    - **审计信息，登录认证、操作审计，如syslog等**
    - **应用系统提供的审计记录**

入侵检测系统概述

- **基于主机的入侵检测系统**
  - **缺点**
    - **需要在主机上运行，占用系统资源**
    - **多数是事后的分析，实时性差**
    - **和操作系统相关，很难支持异构平台**

入侵检测系统概述

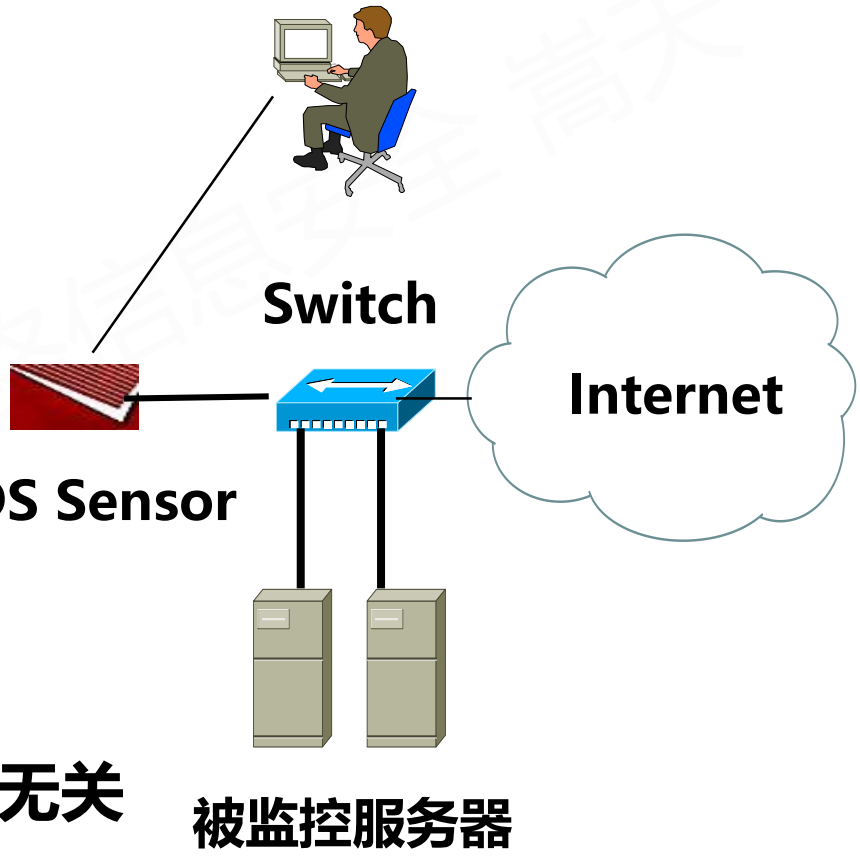
- **基于主机的入侵检测系统**
  - **分布式方式，每台机器中安装代理（Agent）**



入侵检测系统概述

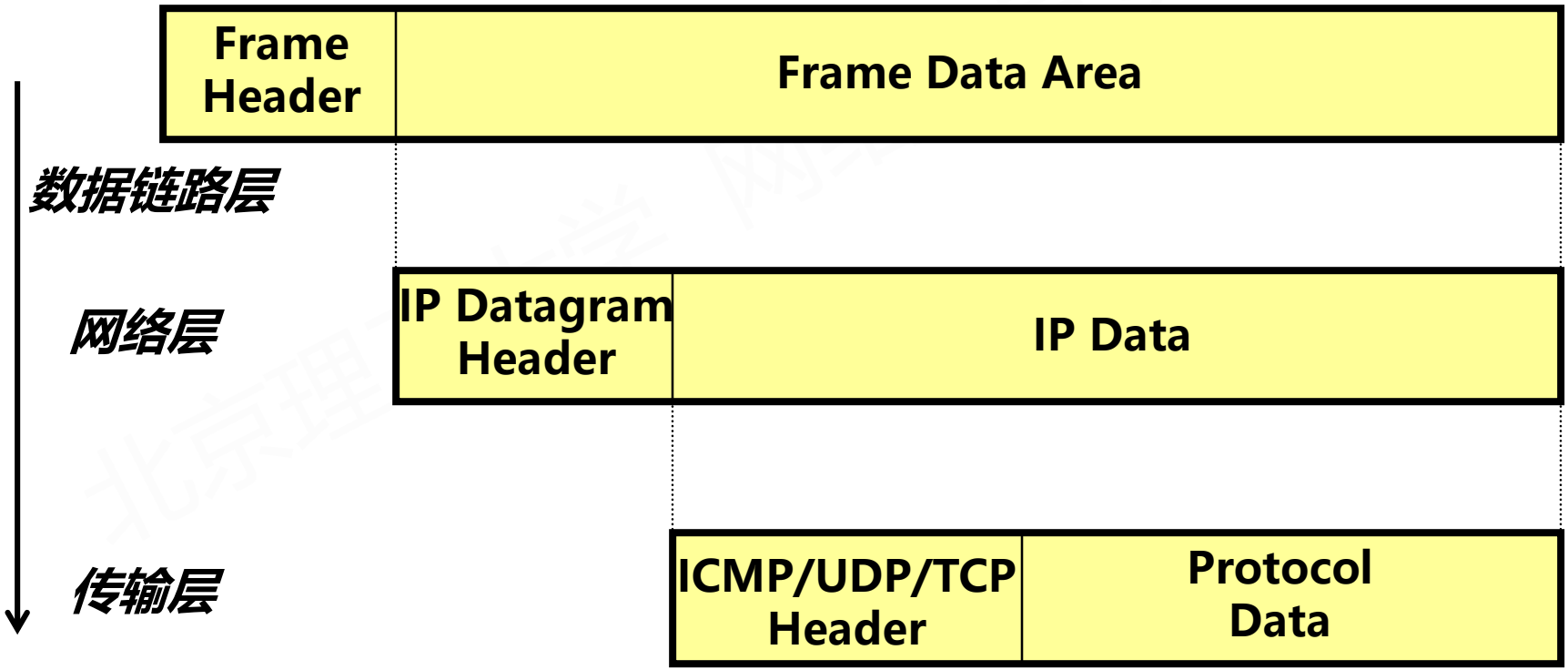
- **基于网络的入侵检测系统**
  - 信息来源
    - 从网络中获取的网络包
  - 旁路监听方式工作

    不影响网络性能
  - 分析网络数据，与操作系统无关
  - 举例：协议分析+模式匹配



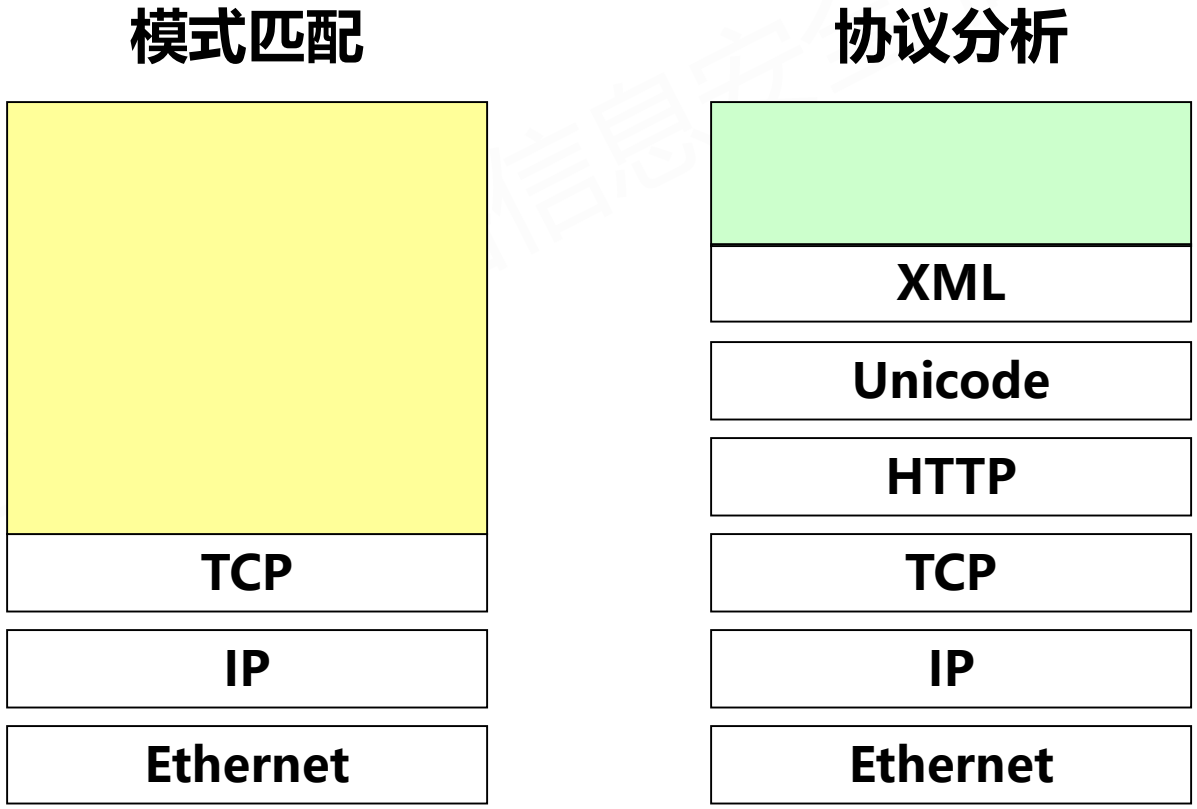
入侵检测系统概述

- **基于网络的入侵检测系统**
  - 协议分析



入侵检测系统概述

- **基于网络的入侵检测系统**
  - 模式匹配



入侵检测系统概述

- **基于网络的入侵检测系统**
  - **直接的模式匹配**
  - **入侵表示为：images/home_collage2.jpg**

```
 0  0050 dac6 f2d6 00b0 d04d cbaa 0800 4500   .P.......M....E.
10  0157 3105 4000 8006 0000 0a0a 0231 d850   .W1.@........1.P
20  1111 06a3 0050 df62 322e 413a 9cf1 5018   .....P.b2.A:..P.
30  16d0 f6e5 0000 4745 5420 2f70 726f 6475   ......GET /produ
40  6374 732f 7769 7265 6c65 7373 2f69 6d61   cts/wireless/ima
50  6765 732f 686f 6d65 5f63 6f6c 6c61 6765   ges/home_collage
60  322e 6a70 6720 4854 5450 2f31 2e31 0d0a   2.jpg HTTP/1.1..
70  4163 6365 7074 3a20 2a2f 2a0d 0a52 6566   Accept: */*..Ref
80  6572 6572 3a20 6874 7470 3a2f 2f77 7777   erer: http://www
90  2e61 6d65 7269 7465 6368 2e63 6f6d 2f70   .ameritech.com/p
a0  726f 6475 6374 732f 7769 7265 6c65 7373   roducts/wireless
b0  2f73 746f 7265 2f0d 0a41 6363 6570 742d   /store/..Accept-
c0  4c61 6e67 7561 6765 3a20 656e 2d75 730d   Language: en-us.
```

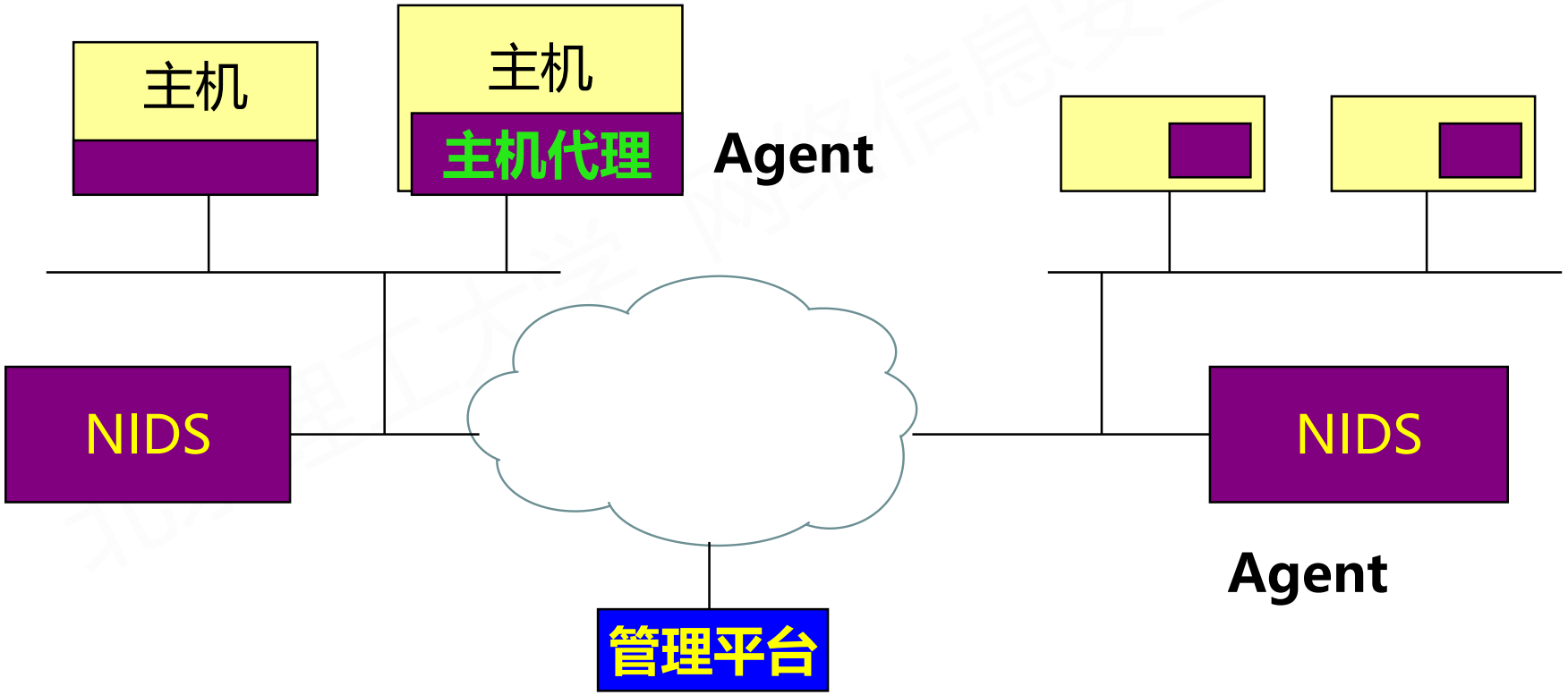
入侵检测系统概述

- **基于网络的入侵检测系统**
  - **经过进一步协议分析后的模式匹配**
  - **入侵表示为：images/home_collage2.jpg**

```
 0  0050 dac6 f2d6 00b0 d04d cbaa 0800 4500   .P.......M....E.
10  0157 3105 4000 8006 0000 0a0a 0231 d850   .W1.@........1.P
20  1111 06a3 0050 df62 322e 413a 9cf1 5018   .....P.b2.A:..P.
30  16d0 f6e5 0000 4745 5420 2f70 726f 6475   ......GET /produ
40  6374 732f 7769 7265 6c65 7373 2f69 6d61   cts/wireless/ima
50  6765 732f 686f 6d65 5f63 6f6c 6c61 6765   ges/home_collage
60  322e 6a70 6720 4854 5450 2f31 2e31 0d0a   2.jpg HTTP/1.1..
70  4163 6365 7074 3a20 2a2f 2a0d 0a52 6566   Accept: */*..Ref
80  6572 6572 3a20 6874 7470 3a2f 2f77 7777   erer: http://www
90  2e61 6d65 7269 7465 6368 2e63 6f6d 2f70   .ameritech.com/p
a0  726f 6475 6374 732f 7769 7265 6c65 7373   roducts/wireless
b0  2f73 746f 7265 2f0d 0a41 6363 6570 742d   /store/..Accept-
c0  4c61 6e67 7561 6765 3a20 656e 2d75 730d   Language: en-us.
```

入侵检测系统概述

- **混合型入侵检测系统**
  - **分布于网络中的重点主机和边界**



入侵检测系统概述

- **混合型入侵检测系统**
  - **需要考虑不同入侵检测Agent之间的协调**
  - **不同类型检测系统有不同的记录格式：基于网络和主机**
  - **检测数据传输的保密性和完整性，比如SNMP数据等**
  - **层级结构的组织**

本节大纲

- 入侵检测系统概述
- 入侵检测/防御方法
- 入侵检测/防御系统的部署

入侵检测/防御方法

- **主要的入侵检测/防御方法分为两类**
  - **误用检测（Misuse Detection）**
  - **异常检测（Abnormal Detection）**

入侵检测/防御方法

- **误用检测（Misuse）**
  - **通过检测用户行为中与已知入侵行为模式类似的行为来检测系统中的入侵活动，是一种基于已有知识的检测**
  - **根据已知的攻击方法或系统安全缺陷方面的知识，建立特征（Signature） 数据库，然后在收集到的网络活动中寻找匹配的使用模式（Pattern）**
  - **优点：准确率较高，速度较快**
  - **缺点：只能检测已知的攻击**

入侵检测/防御方法

- **异常检测（Anomaly）**
  - **非规则检测建立在如下假设的基础上：入侵行为与合法用户或者系统的正常或者期望的行为有偏差**
  - **正常的行为模式可以从大量历史活动分析统计得到**
  - **任何不符合以往活动规律的行为都被视为是入侵行为。**
  - **优点：能够检测出未知的攻击**
  - **缺点：误报率很高　（误用检测的误报率如何？）**

入侵检测/防御方法

- **入侵检测系统举例**
  - **Snort**
  - **IDES（Intrusion Detection Expert System）**
  - **BRO**
  - **Suricate**

入侵检测/防御方法

- **Snort**

  - **由Martin Roesch开发的开源入侵检测系统**
  - **第一个成熟的开源网络入侵检测系统**
  - **支持多种平台：Linux, Solaris, Windows**
  - **利用libpcap 捕获数据包**
  - **基于规则的检测方法，可以检测出缓存溢出、端口扫描、等多种攻击，目前有5000多条常用规则**

入侵检测/防御方法

- **Martin Roesch**
  - **1999年，开发出Snort系统**

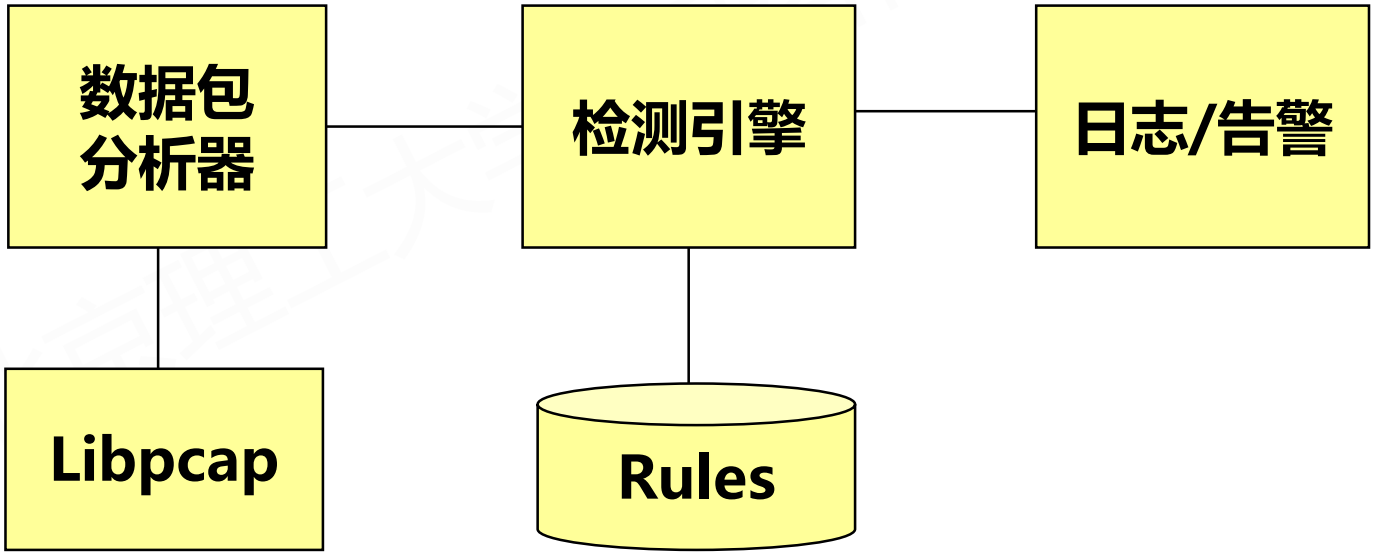
    Snort - Lightweight Intrusion Detection for Networ

    Proceedings of the 13th USENIX conference on System administration

    系统实现类论文，被引用1727次
  - **2001年，创立了Sourcefire公司（Nasdaq：FIRE），任CTO**
  - **2009年11月，FIRE市值$739.86M （7亿美元）**
  - **2013年7月，Sourcefire退市了 被Cisco 27亿美元收购**
  - **毕业于Clarkson University，获学士学位，年收入$63w**

入侵检测/防御方法

- **Snort**
  - http://www.snort.org
  - http://www.sourcefire.com



入侵检测/防御方法

- **Snort规则格式**

```
alert tcp any any -> 192.168.1.0/24 111  (content: "|000186a5|"; msg:"mounted access")
```

规则头 | **规则选项**

入侵检测/防御方法

- **Snort规则格式**

```
alert tcp any any -> 192.168.1.0/24 111  (content: "|000186a5|"; msg:"mounted access")
```

  - **规则头**
    - **规则动作：Alert / Log / Pass**
    - **协议：支持TCP/ UDP/ICMP/ARP/RIP/OSPF 等**
    - **IP 地址：Any 匹配任何地址，支持CIDR （无类别域间路由，前缀聚合），比如：192.168.1.0/24**
    - **端口号Port**

入侵检测/防御方法

- **Snort规则格式**

```
alert tcp any any -> 192.168.1.0/24 111  (content: "|000186a5|"; msg:"mounted access")
```

– **规则头**

• **方向：单向（—>）、双向（< >）**

```
Log   !   192.168.1.0/24    any     < >   192.168.1.0/24 23
     ## 记录所有非本网的telnet 包
Log udp any any -> 192.168.1.0/24   1:1024
```

入侵检测/防御方法

- **Snort规则格式**

```
alert tcp any any -> 192.168.1.0/24 111  (content: ”|000186a5|”; msg:”mounted access”)
```

  - **规则选项**
    - **选项之间用；分隔**
    - **msg 在报警信息中显示的消息**
    - **TTL、dsize（ 数据包的大小）**
    - **content：数据包中的内容**
    - **Offset：从何处开始检索content**

入侵检测/防御方法

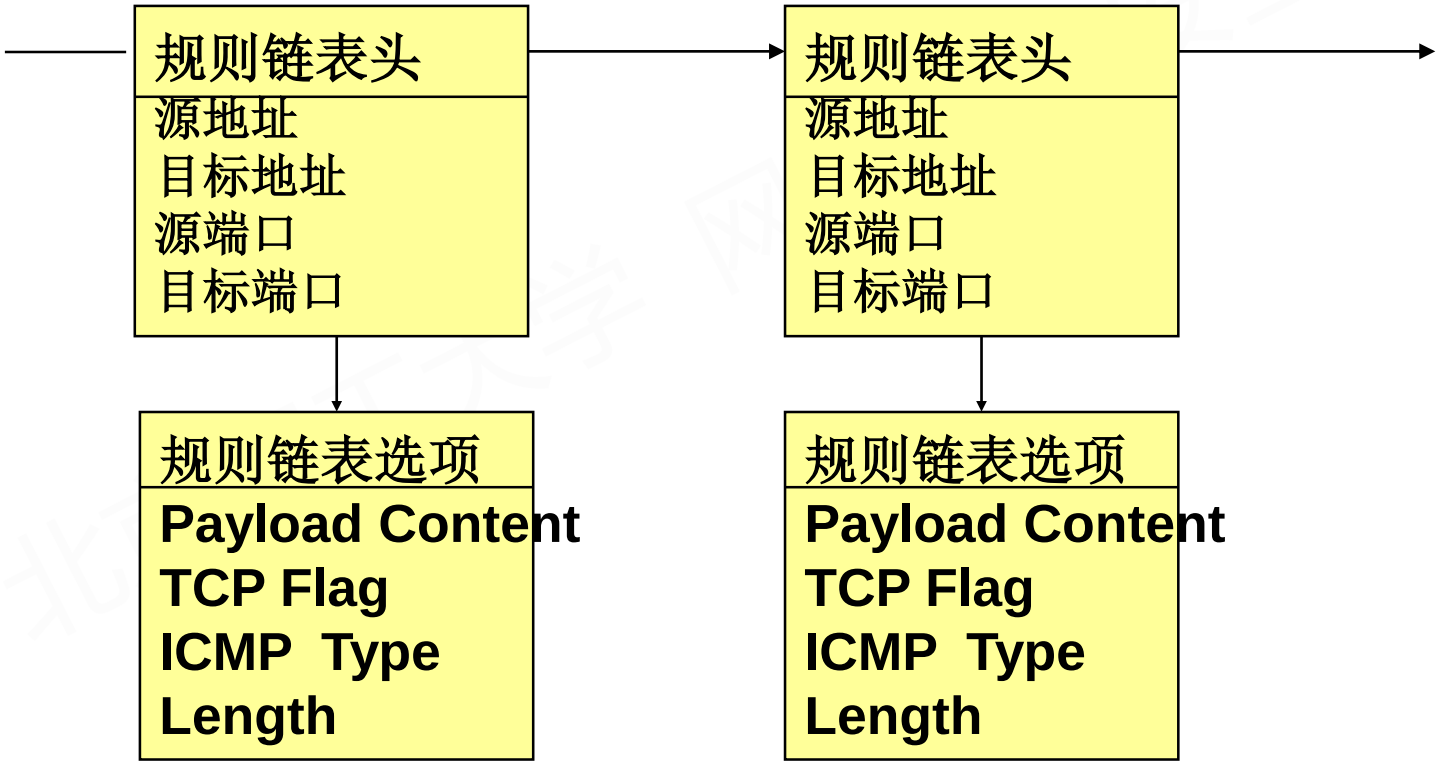
- **Snort**
  - **3种日志模式**
    - **关闭**
    - **文本方式**
    - **二进制方式，与tcpdump 格式相同**
  - **4种告警方式**
    - **Syslog**
    - **SMB消息**
    - **Snmp trap**
    - **Mysql 数据库**

入侵检测/防御方法

- **Snort**
  - **各种监测功能通过各种插件（Plug-in）模块来完成**
    - **例如：IP碎片整理、流重组等**
  - **用户可以编写自己的模块来扩展新的功能**
  - **模式匹配结构组织**

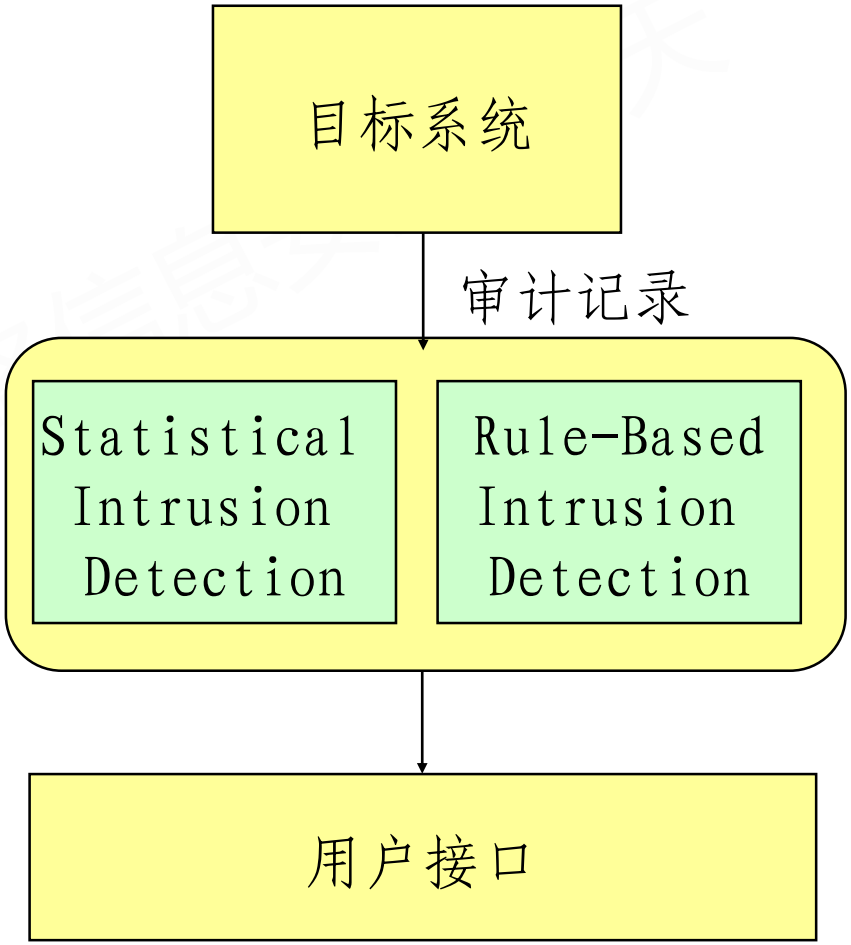
入侵检测/防御方法

- **Snort**
  - 模式匹配结构组织



入侵检测/防御方法

- **IDES**
  - **目标系统根据用户的活动产生审计数据，用一种专用的格式。**
  - **调用统计分析和规则分析两个部件来检测是否存在异常。**
  - **一旦检测出异常就通过用户界面向管理员告警**



入侵检测/防御方法

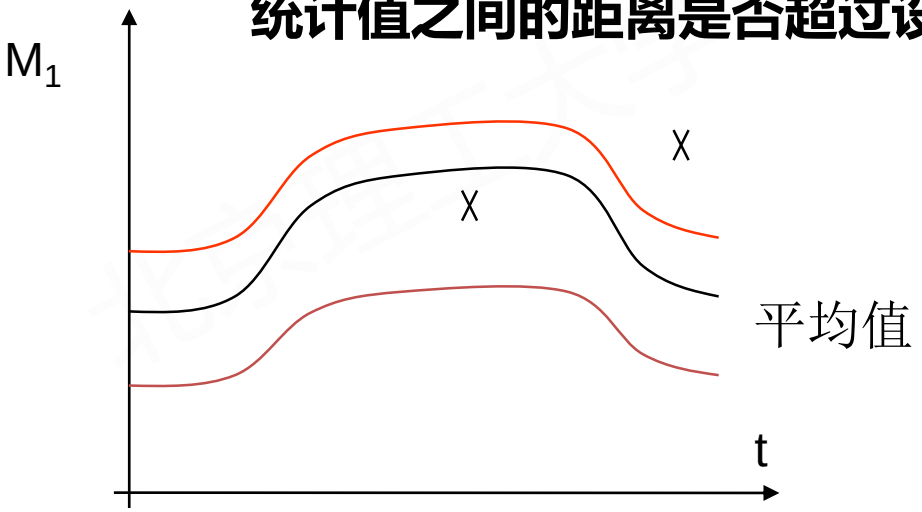
- **IDES**
  - **1986年，提出了系统模型**
  - **特点：**
    - **同时使用了统计的方法和基于规则的方法**
    - **使用了统计的记录格式，独立于被监控的系统平台**
  - **被监控对象**
    - **主体（Subject）：用户、主机、组、整个系统**

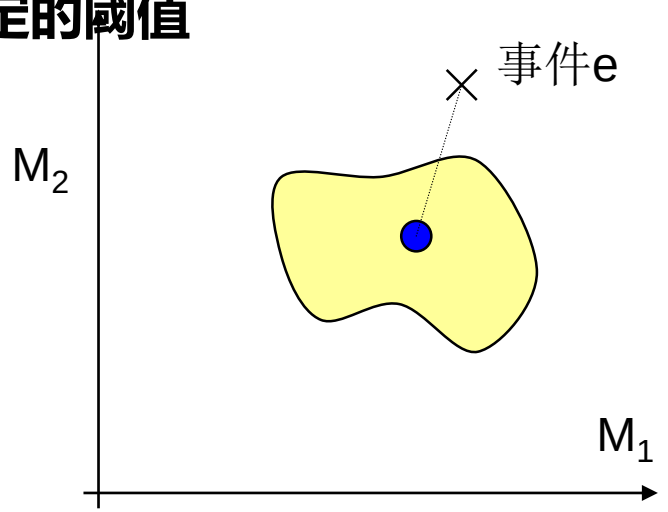
入侵检测/防御方法

- **IDES**
  - **描述主体行为的尺度（Metrics）**
    - **Metrics是描述用户行为的变量（参数）**
    - **比如每次登录时间、每天登录次数、登录的地点等**
    - **离散型尺度：登录地点、访问的文件名称，用每个值的发生概率来描述；**
    - **连续型尺度：每次会话的持续时间等，用概率分布来描述。**
    - **档案（Profile）：不存放大量的历史数据，而是存放各个尺度的平均值、频率表、方差等。**

入侵检测/防御方法

- **IDES**
  - **检测方法**
    - **根据主体的历史档案判断用户的行为是否偏离了过去的行为模式或习惯。**
    - **每次审计记录接收以后，计算N维空间中当前事件与档案中的统计值之间的距离是否超过设定的阈值**





入侵检测/防御方法

- **BRO**
  - **开源的网络入侵检测系统**
  - **由Vern Paxson开发**
    - **加州大学伯克利分校（UC. Berkeley）副教授**
    - **Flex的作者**
  - **与Snort不同，BRO的规则库采用正则表达式描述**

```
signature s2b-654-13 {
  ip-proto == tcp
  dst-port == 25
  event "SMTP RCPT TO overflow"
  tcp-state established,originator
  payload /((^)|(\n+))[rR][cC][pP][tT] [tT][oO][\x20\x09\x0b][^\n]{300}
  requires-reverse-signature | smtp_server_fail
}
```

入侵检测/防御方法

- **入侵检测系统的发展方向**
  - **基于特征匹配的入侵检测系统已经产品化**
  - **基于统计的异常检测技术还有待于进一步的研究**
  - **抗攻击性**
  - **针对大规模网络部署的可扩展性**
  - **高带宽网络流量的处理能力**
  - **基于虚拟化的蜜罐式入侵检测系统**

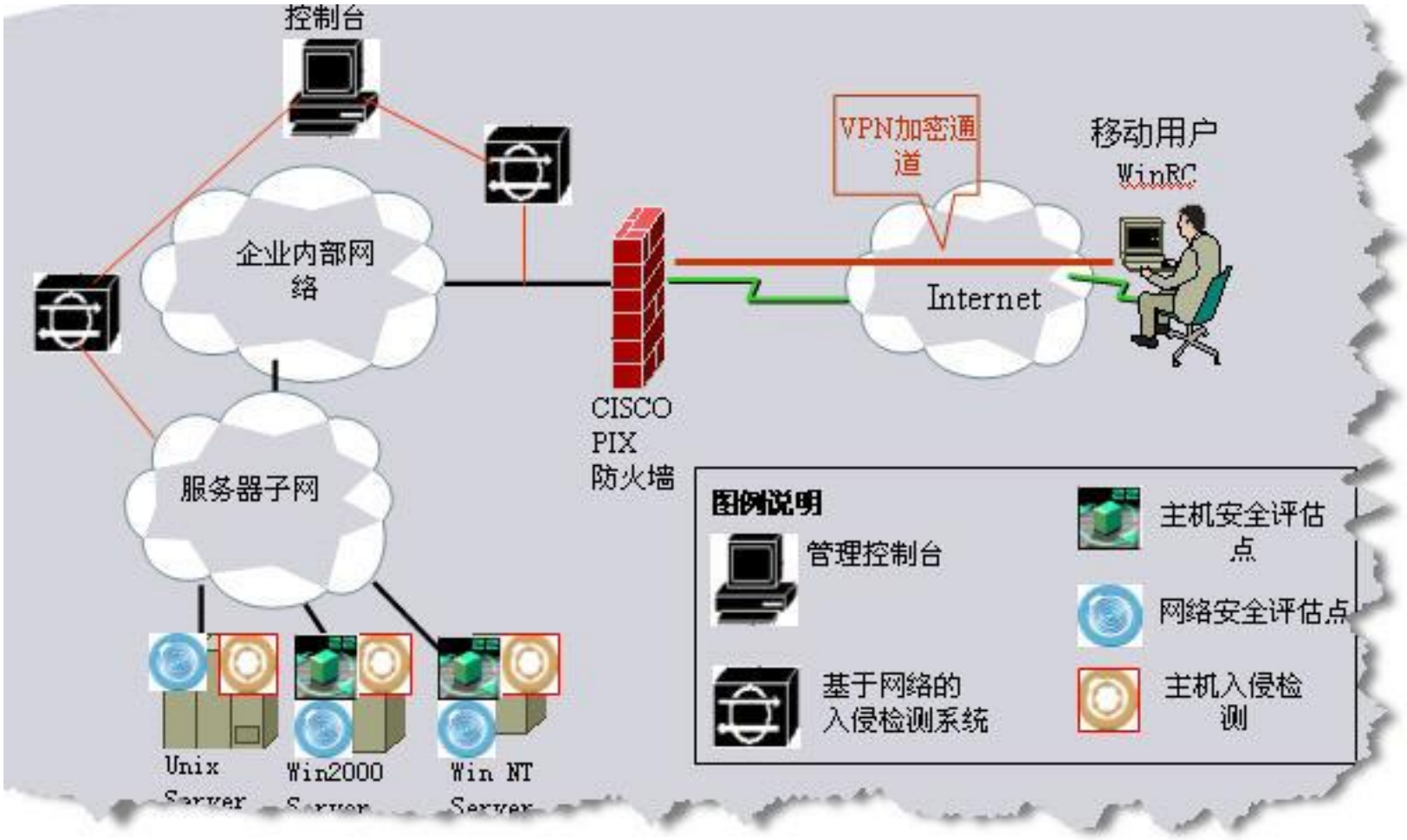
本节大纲

- **入侵检测系统概述**
- **入侵检测/防御方法**
- **入侵检测/防御系统的部署**

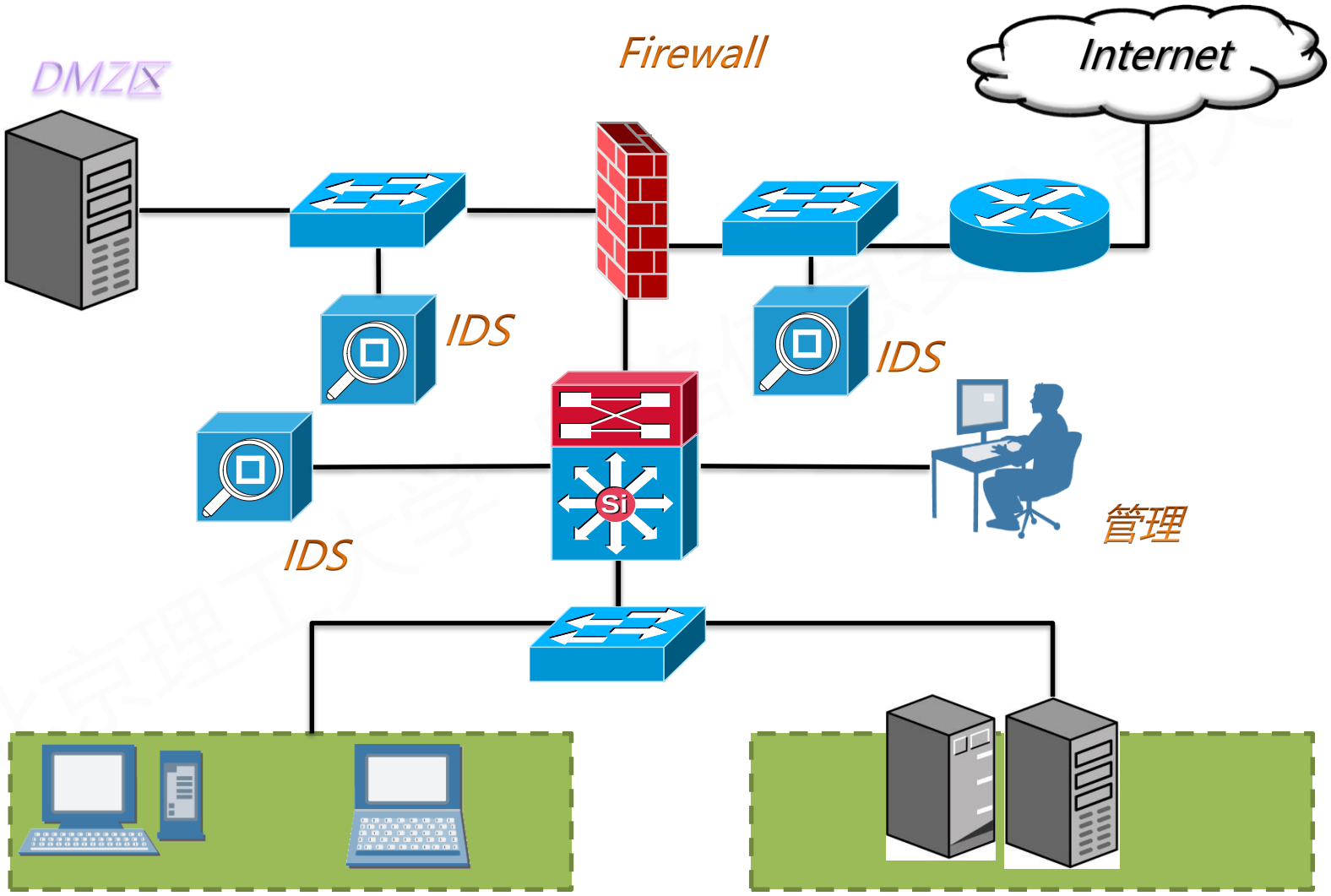
入侵检测/防御的部署

- **NIDS的部署要求**
  - **不同于防火墙，IDS入侵检测系统是一个监听设备**
  - **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。**

入侵检测/防御的部署


控制台
企业内部网络
服务器子网
CISCO
PIX
防火墙
VPN加密通道
Internet
移动用户
WinRC
Unix
Server
Win2000
Server
Win NT
Server
图例说明
管理控制台
基于网络的
入侵检测系统
主机安全评估点
网络安全评估点
主机入侵检测

入侵检测/防御的部署



入侵检测/防御的部署

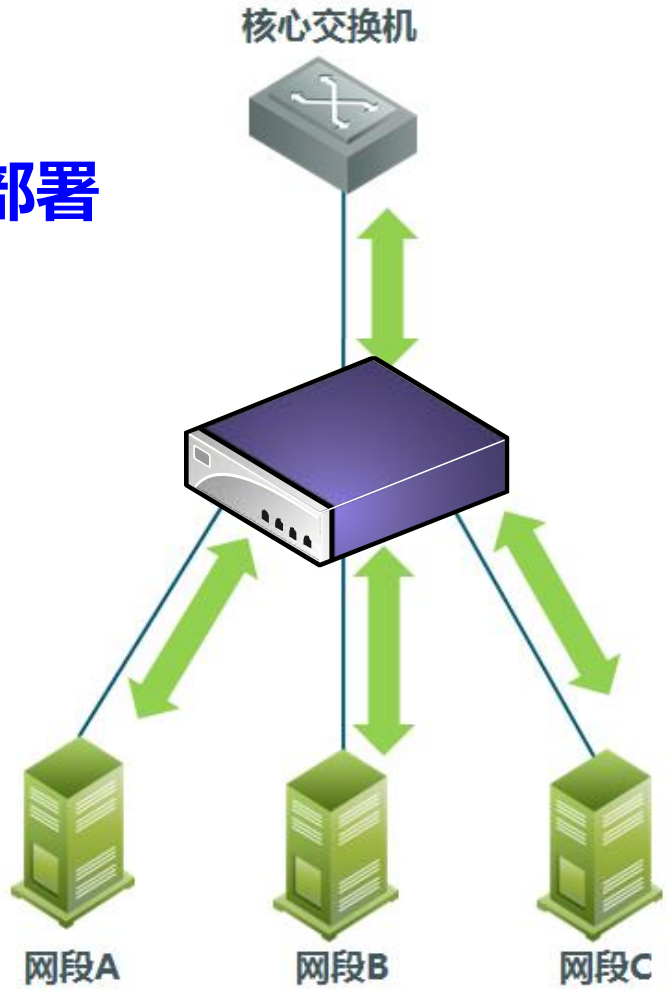
- **NIPS（网络入侵防御系统）的部署要求**
  - **网络入侵防御系统是一种在线部署的产品**
  - **提供主动的、实时的防护，其设计目标旨在准确监测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是简单地发出告警**
  - **IPS是通过直接串联到网络链路中而实现这一功能的**

入侵检测/防御的部署

- **NIDS和NIPS的区别**
  - **功能上：NIPS能够及时阻止入侵**
  - **性能上：NIPS性能更为敏感**
  - **实现上：NIPS需要维护流表，NIDS不需要，开销不同**

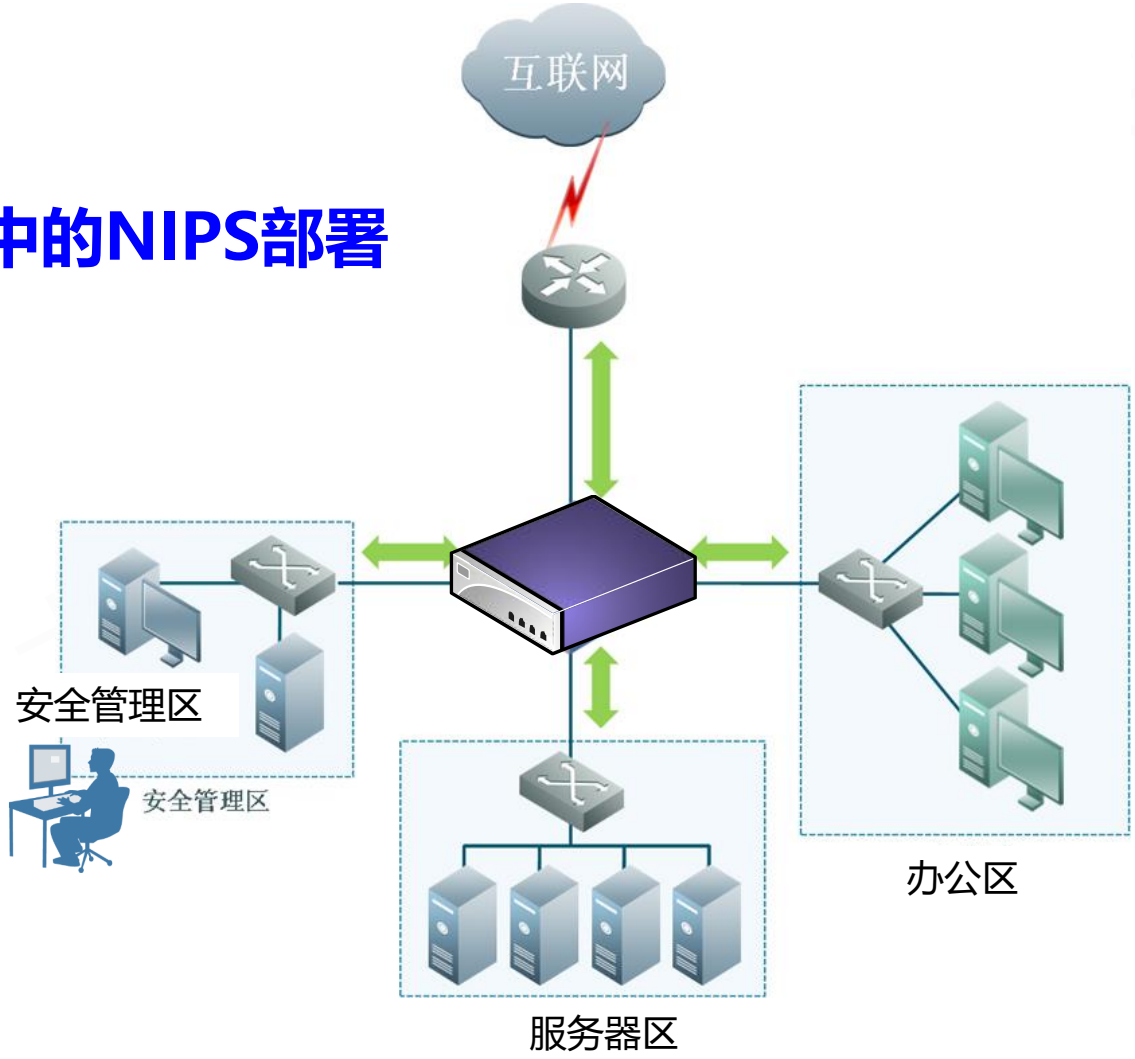
入侵检测/防御的部署

- **一般网络环境中的NIPS部署**



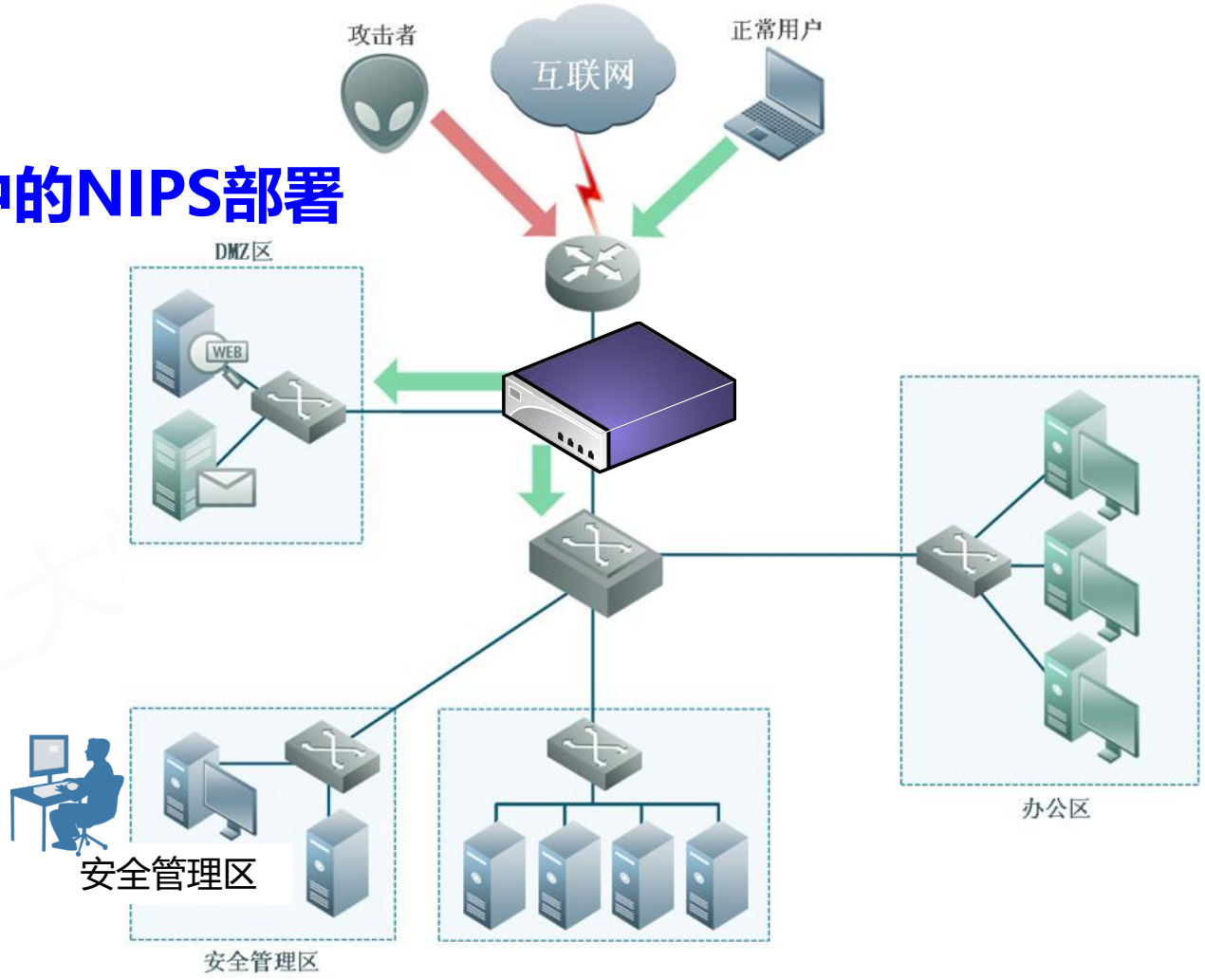
入侵检测/防御的部署

- **复杂网络环境中的NIPS部署**



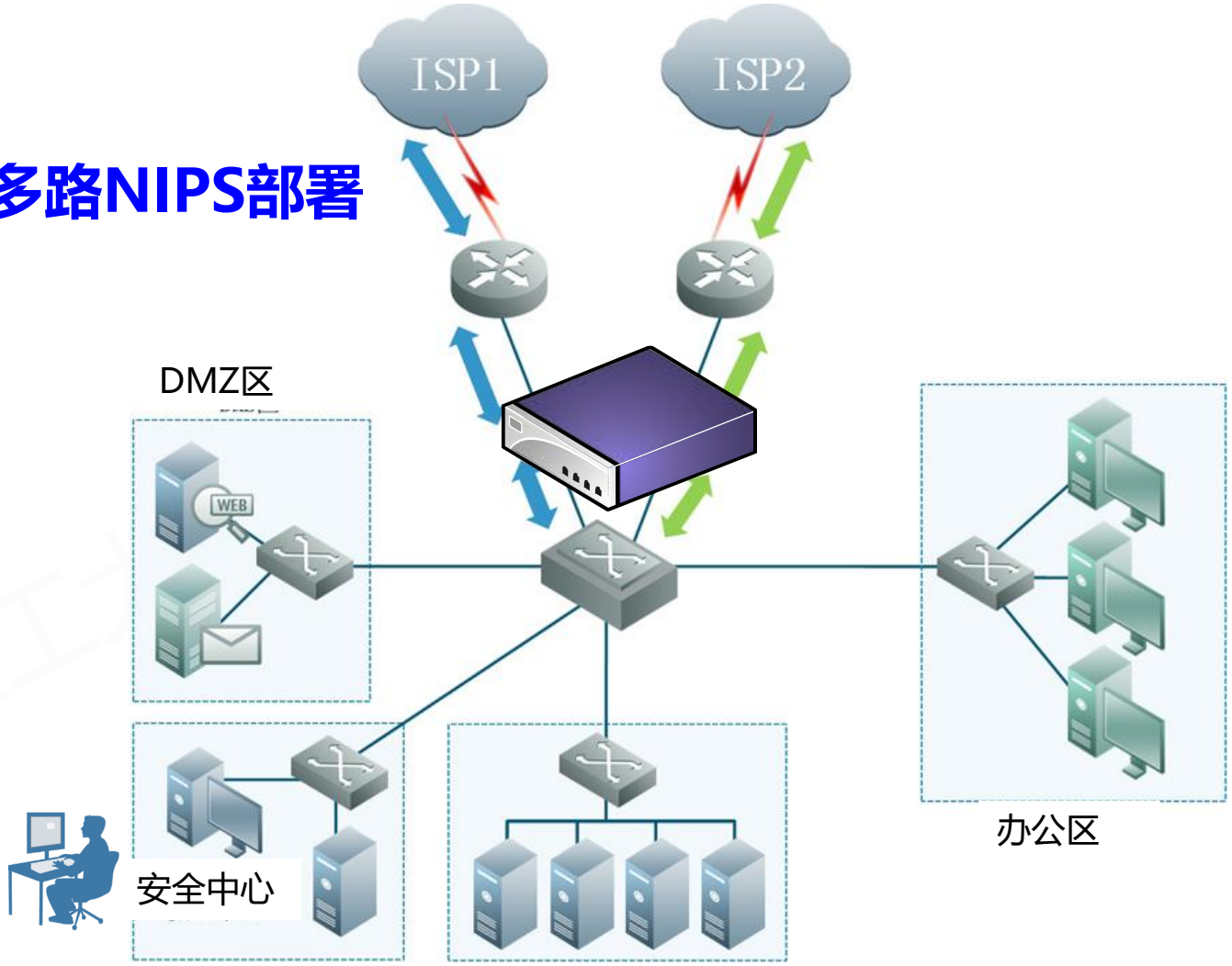
入侵检测/防御的部署

- **复杂网络环境中的NIPS部署**



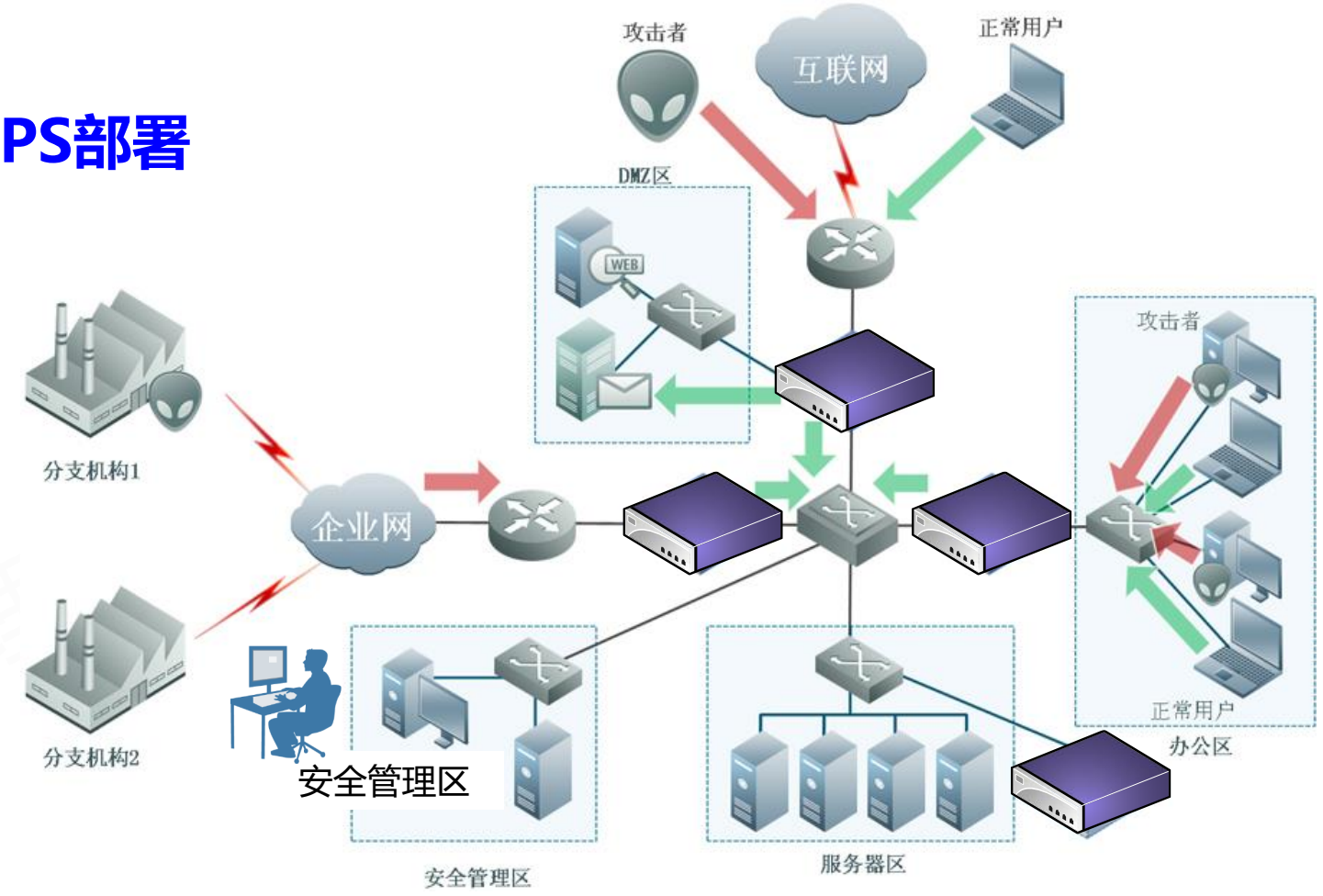
入侵检测/防御的部署

- **独立部署的多路NIPS部署**



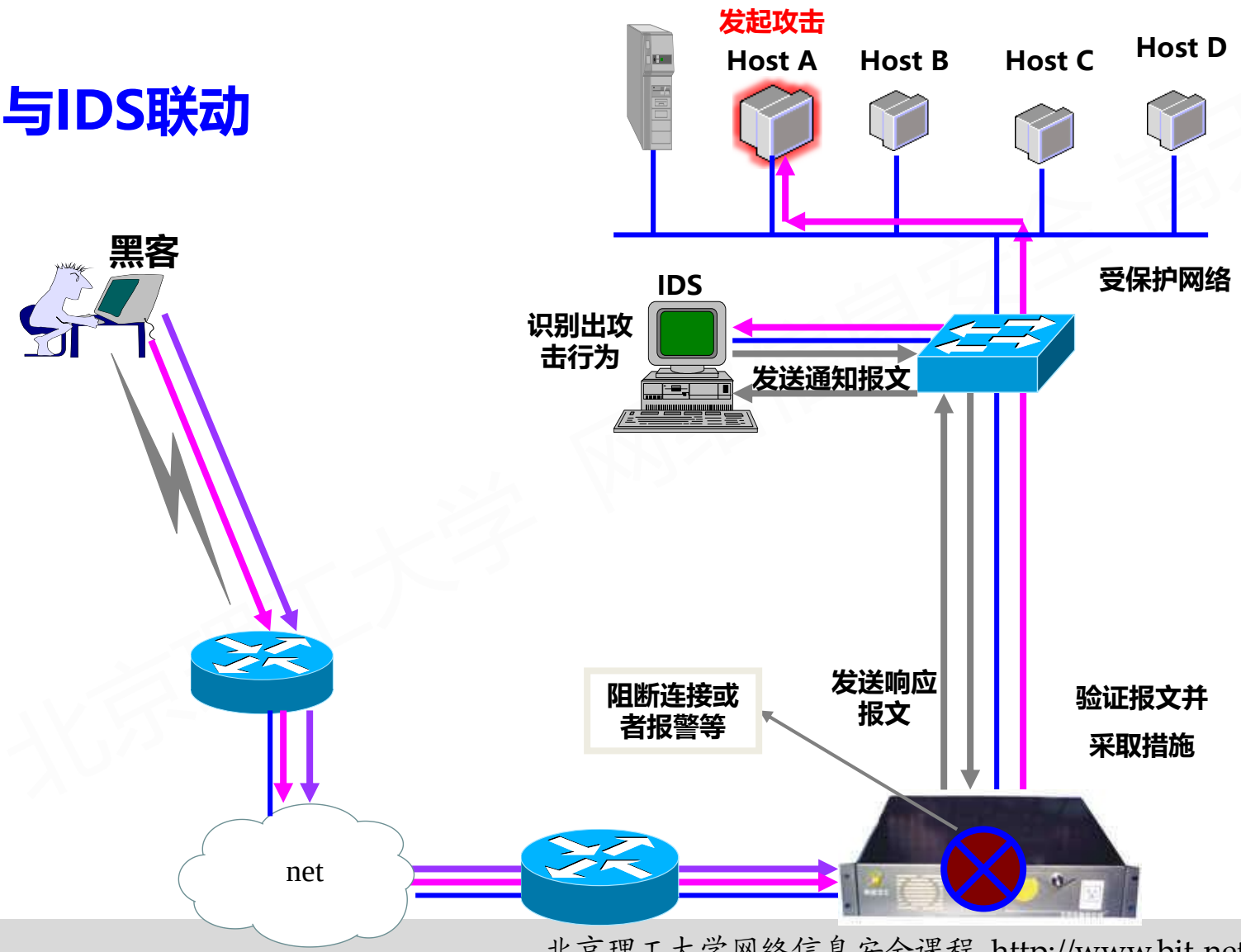
入侵检测/防御的部署

- **分布式NIPS部署**



与防火墙联动

- 与IDS联动



本节总结

- **经过本节的学习，我们知道**
  - **网络入侵检测基本模型**
  - **网络入侵检测系统概念、类型**
  - **误用检测和异常检测**
  - **入侵检测系统的部署**