

第7章 网络防御

许海燕



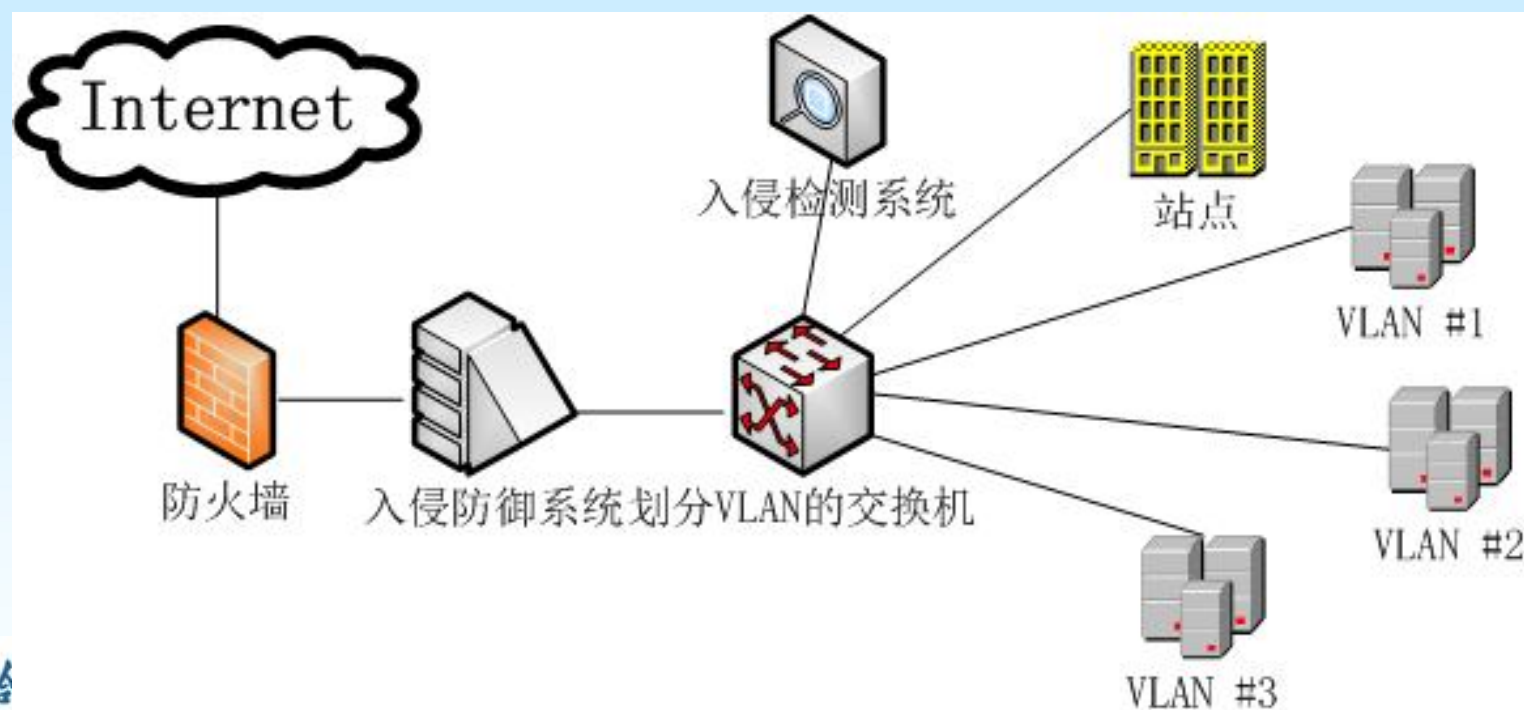
主要内容

- ◆ 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



7.1 概述

- ◆ 网络防御是一个综合性的安全工程，不是几个网络安全产品能够完成的任务。
 - 防御需要解决多层面的问题，除了安全技术之外，安全管理也十分重要，实际上提高用户群的安全防范意识、加强安全管理所能起到效果远远高于应用几个网络安全产品。



哈

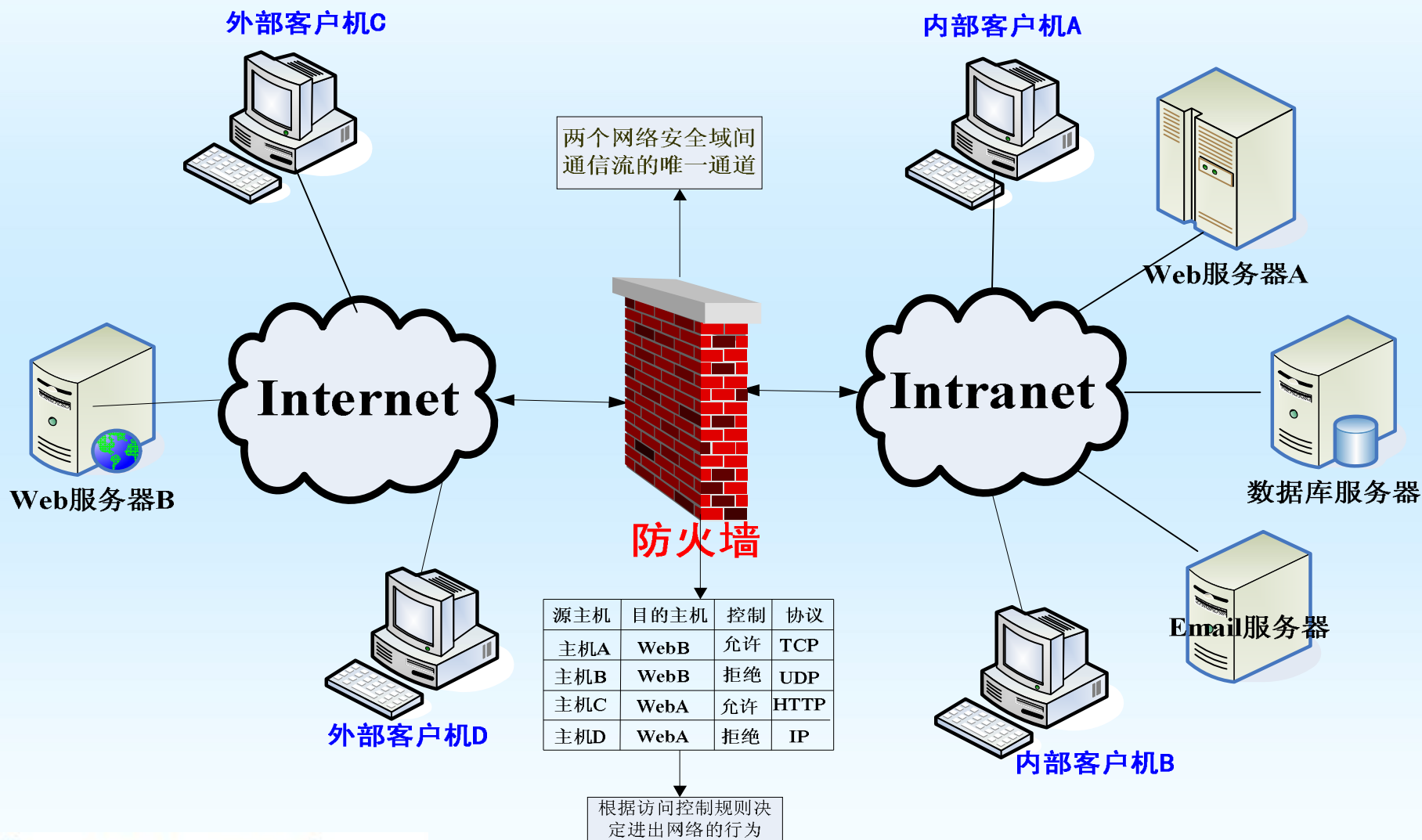
HARBIN INSTITUTE OF TECHNOLOGY AT WEIHAI



7.2 防火墙

- ◆ 防火墙指的是一个由软件和硬件设备组合而成、在内部网络和外部网络之间构造的安全保护屏障，从而保护内部网络免受外部非法用户的侵入。
- ◆ 简单地说，防火墙是位于两个或多个网络之间，**执行访问控制策略的一个或一组系统**，是一类防范措施的总称。

防火墙逻辑位置结构示意图



7.2.1 防火墙概述

◆ 防火墙设计目标是有效地控制内外网之间的网络数据流量，做到御敌于外。

◆ 防火墙的结构和部署考虑：

① 内网和外网之间的所有网络数据流必须经过防火墙；

✓ 阻塞点可以理解为连通两个或多个网络的唯一路径上的点，当这个点被删除后，各网络之间不在连通。

② 只有符合安全政策的数据流才能通过防火墙。

✓ 要求防火墙具有审计和管理的功能，具有可扩展性和健壮性。

分类

- ◆ 从应用对象上，分为企业防火墙和个人防火墙
 - 企业防火墙的主要作用是保护整个企业网络免受外部网络的攻击；
 - 个人防火墙则是保护个人计算机系统的安全。
- ◆ 从存在形式上，可以分为硬件防火墙和软件防火墙
 - 硬件防火墙采用特殊的硬件设备，有较高性能，可做为独立的设备部署，企业防火墙多数是硬件防火墙；
 - 软件防火墙是一套安装在某台计算机系统上来执行防护任务的安全软件，个人防火墙都是软件防火墙。

防火墙主要作用

◆ 网络流量过滤

- 通过在防火墙上进行安全规则配置，可以对流经防火墙的网络流量进行过滤。

◆ 网络监控审计

- 防火墙记录访问并生成网络访问日志，提供网络使用情况的统计数据。

◆ 支持NAT部署

- NAT (Network Address Translation) 是网络地址翻译的缩写，是用来缓解地址空间短缺的主要技术之一

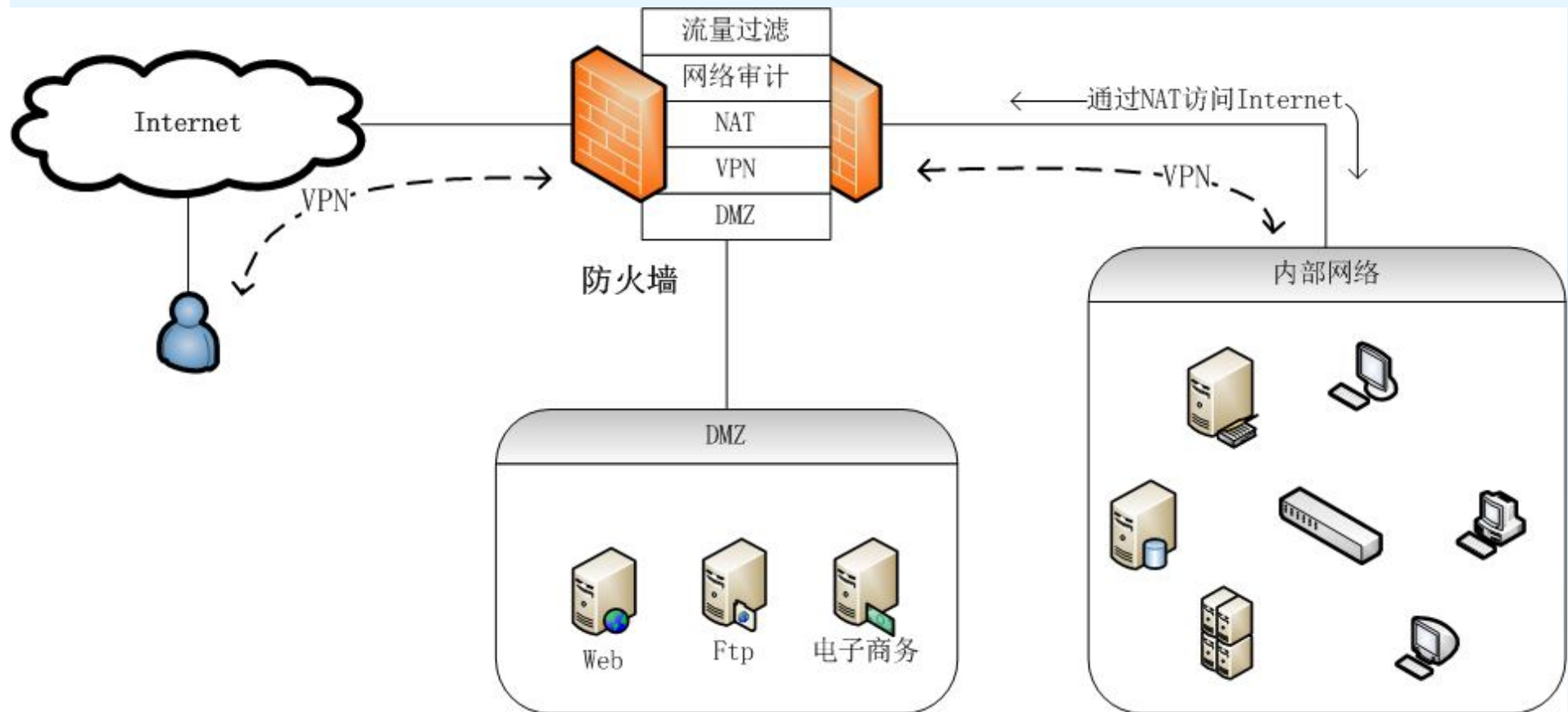
◆ 支持DMZ

- DMZ是英文“Demilitarized Zone”的缩写,它是设立在非安全系统与安全系统之间的缓冲区。

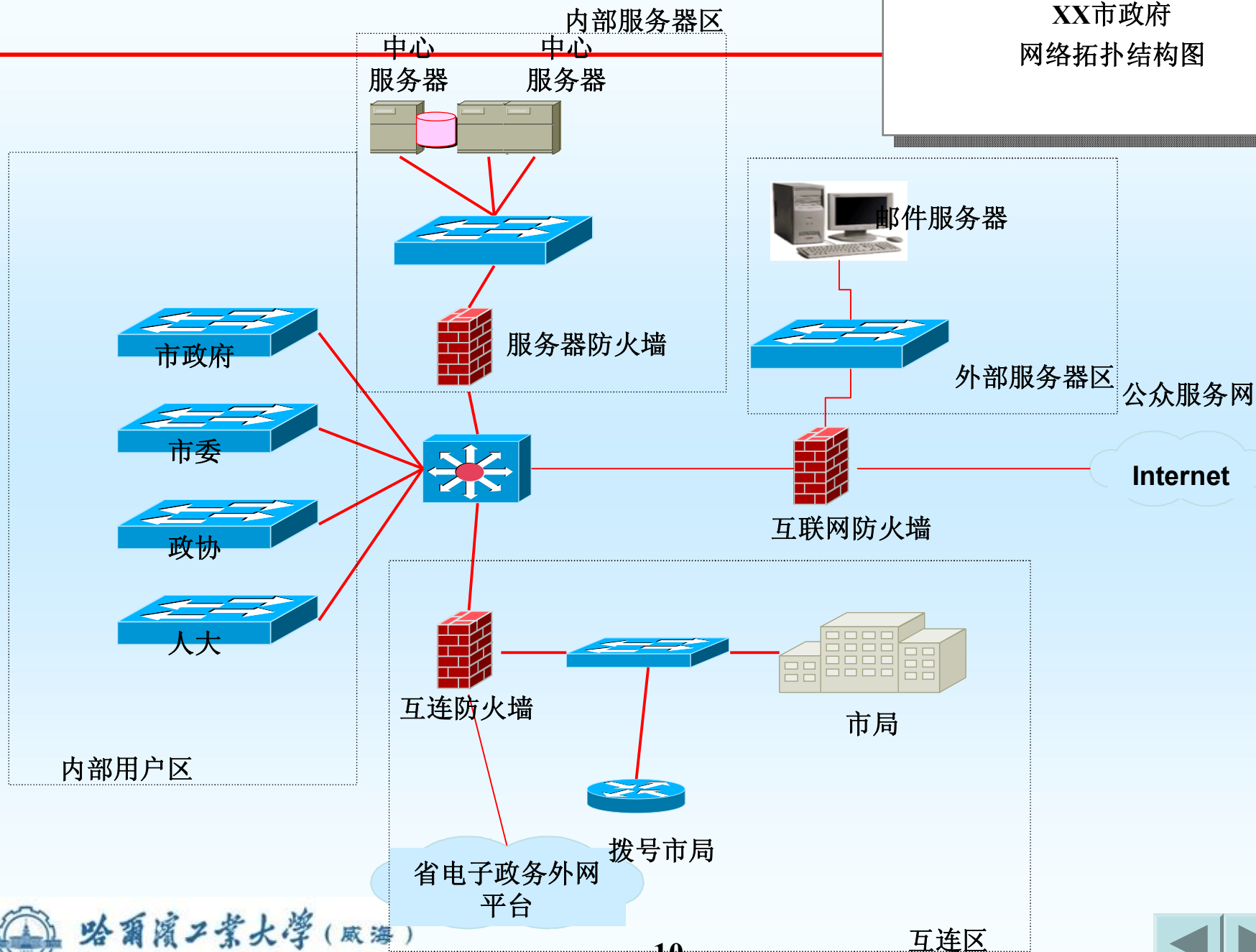
◆ 支持VPN

- 通过VPN，企业可以将分布在各地的局域网有机地连成一个整体。

典型企业防火墙应用



XX市政府
网络拓扑结构图



局限性

- ◆ 防火墙无法检测不经过防火墙的流量，如通过内部提供拨号服务接入公网的流量；
- ◆ 防火墙不能防范来自内部人员恶意的攻击；
- ◆ 防火墙不能阻止被病毒感染的和有害的程序或文件的传递，如木马；
- ◆ 防火墙不能防止数据驱动式攻击，如一些缓冲区溢出攻击。

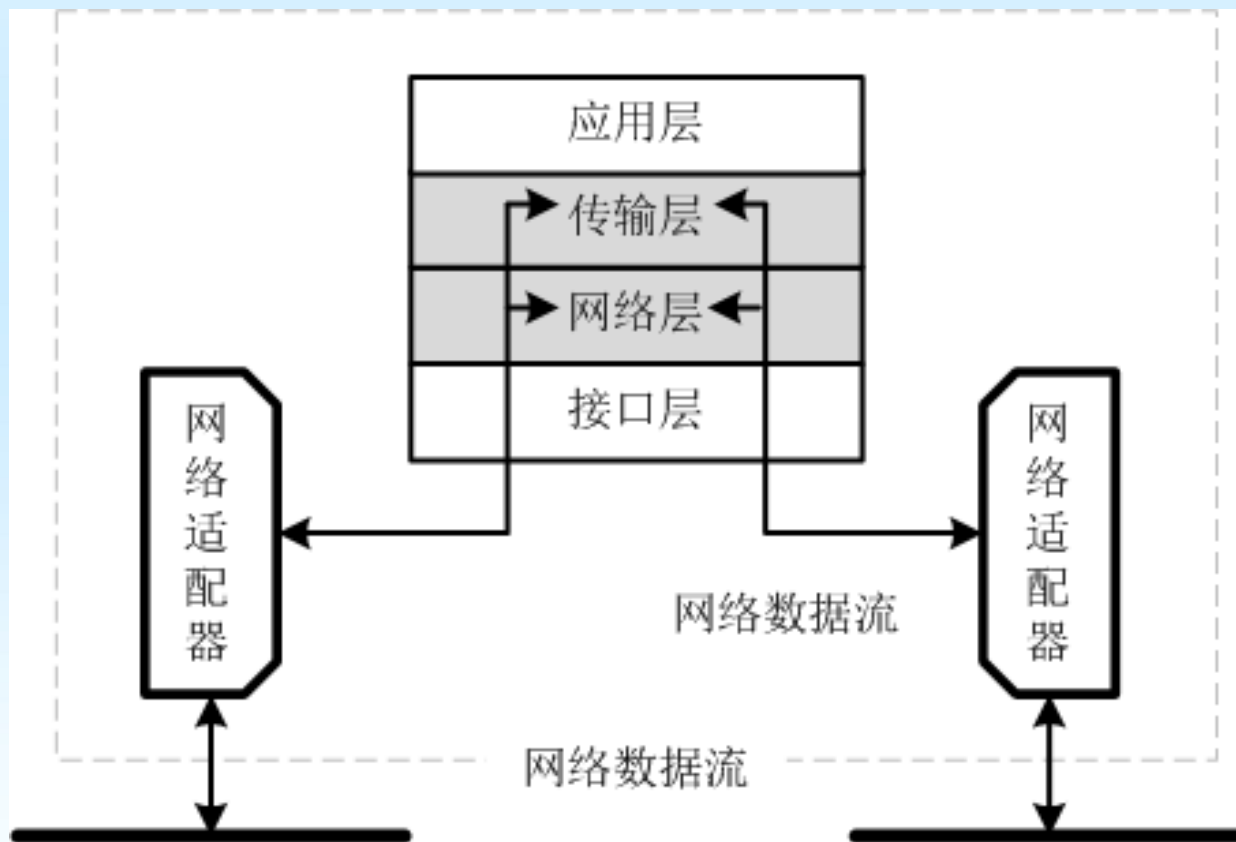
7.2.2 防火墙的主要技术

- ① 包过滤
- ② 代理服务

7.2.2 防火墙的主要技术

◆ 包过滤防火墙

- 面向网络底层数据流进行审计和控管
- 其安全策略主要根据数据包头的源地址、目的地址、端口号和协议类型等标志来制定，可见其主要工作在网络层和传输层。



主要技术简介

◆ 访问控制列表ACL

- Access Control List是允许和拒绝匹配规则的集合。
- 规则告诉防火墙哪些数据包允许通过、哪些被拒绝。

| 顺序 | 方向 | 源地址 | 目的地址 | 协议 | 源端口 | 目的端口 | 是否通过 |
|--------|-----|---------------|---------------|-----|-----|------|--------|
| Rule 1 | out | 192.168.10.11 | *.*.*.* | TCP | any | 80 | deny |
| Rule 2 | out | *.*.*.* | 202.106.85.36 | TCP | any | 80 | accept |



示例：

| Type | Source Addr | Dest Addr | Source Port | Dest Port | Action |
|------|--------------|-----------|-------------|-----------|--------|
| tcp | * | 123.4.5.6 | > 1023 | 23 | permit |
| tcp | * | 123.4.5.7 | > 1023 | 25 | permit |
| tcp | * | 123.4.5.8 | > 1023 | 25 | permit |
| tcp | 129.6.48.254 | 123.4.5.9 | > 1023 | 119 | permit |
| udp | * | 123.4.*.* | > 1023 | 123 | permit |
| * | * | * | * | * | deny |

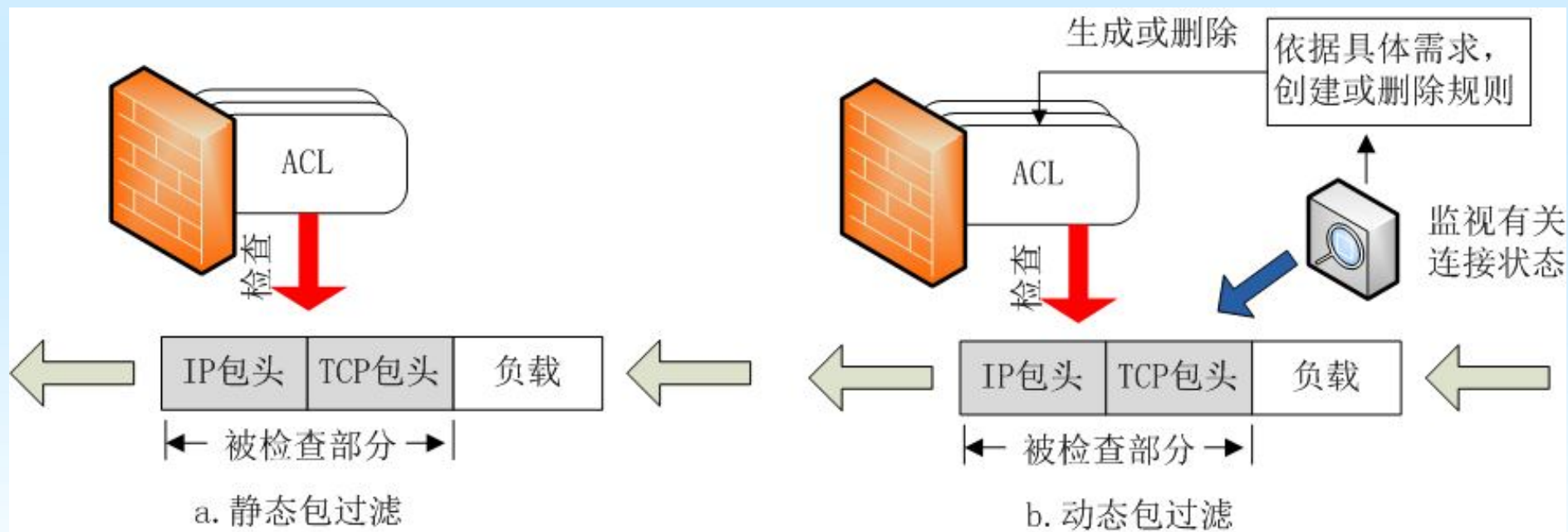
两个默认策略：

默认=丢弃：没有明确允许的就被禁止。

默认=转发：没有明确禁止的就是允许。

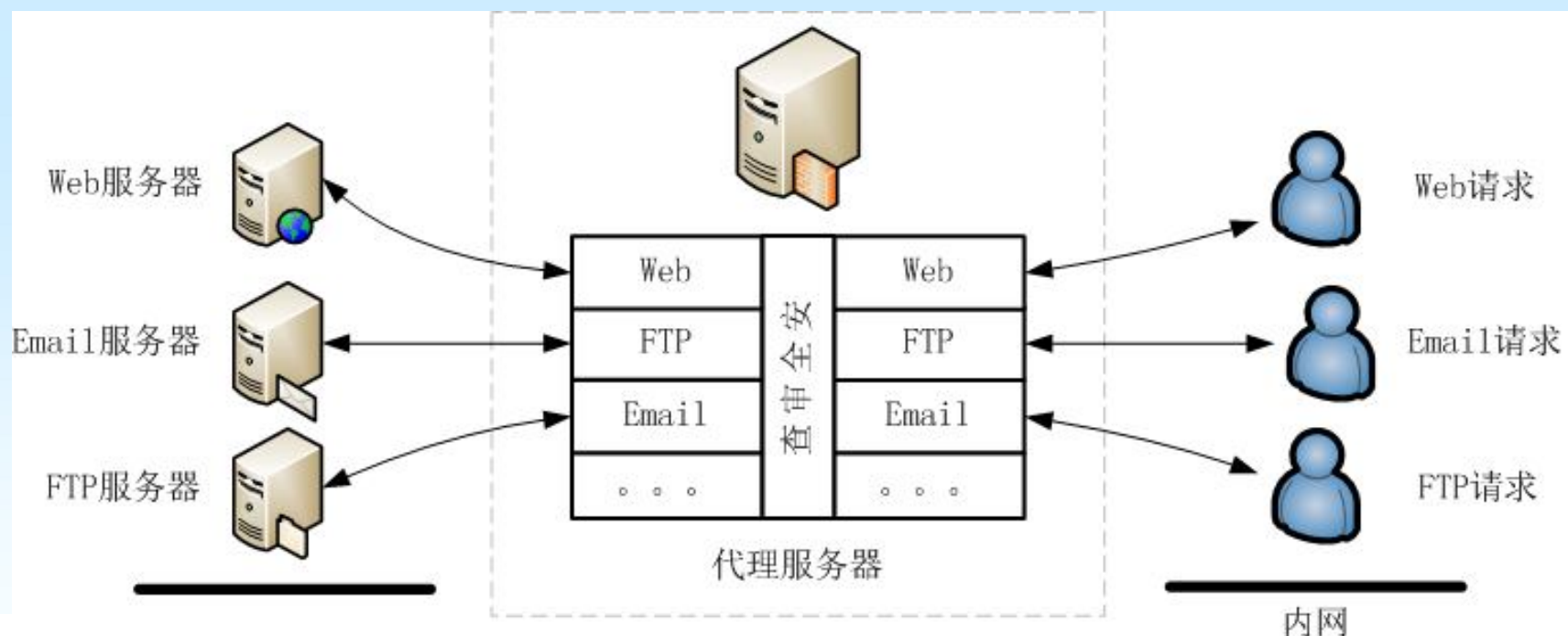
包过滤

- ◆ 静态包过滤是指防火墙根据定义好的包过滤规则审查每个数据包，确定其是否与某一条包过滤规则匹配。
- ◆ 动态包过滤是指防火墙采用动态配置包过滤规则的方法。



代理防火墙

- ◆ 基于代理（Proxy）技术，使防火墙参与到每一个内外网络之间的连接过程
- ◆ 防火墙需要理解用户使用的协议，对内部节点向外部节点请求进行还原审查后，转发给外部服务器；
- ◆ 外部节点发送来的数据也需要进行还原审查，然后封装转发给内部节点。



代理网关

◆ 应用代理网关

- 被认为是最安全的防火墙技术，应用代理网关防火墙彻底隔断内网与外网的直接通信，内网用户对外网的访问变成防火墙对外网的访问，外网返回的消息再由防火墙转发给内网用户

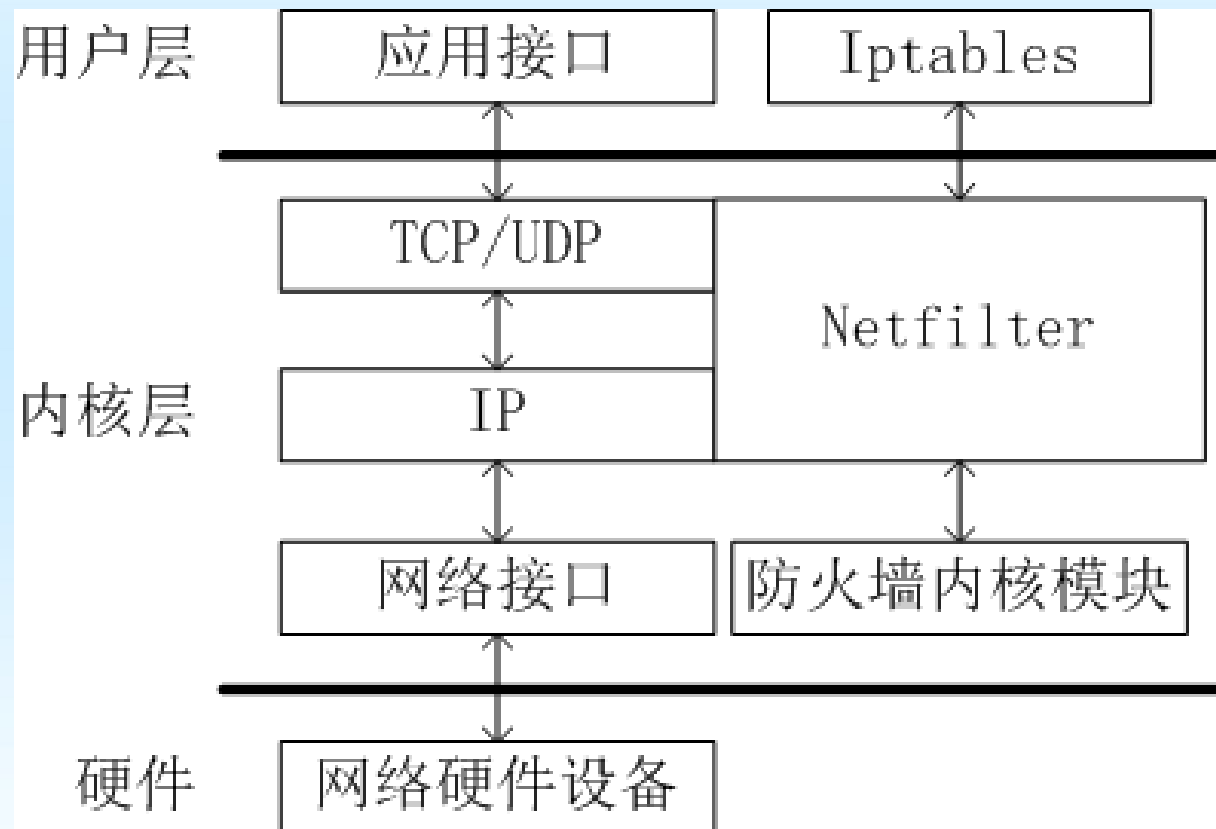
◆ 电路级网关（Circuit Gateway）

- 工作原理与应用代理网关基本相同，代理的协议以传输层为主，在传输层上实施访问控制策略，是在内外网络之间建立一个虚拟电路，进行通信。



7.2.3 Netfilter/IPtables防火墙

- ◆ 2001年，Linux 2.4版内核，Netfilter/IPtables包过滤机制，被业内称为第三代Linux防火墙。



Netfilter通用架构

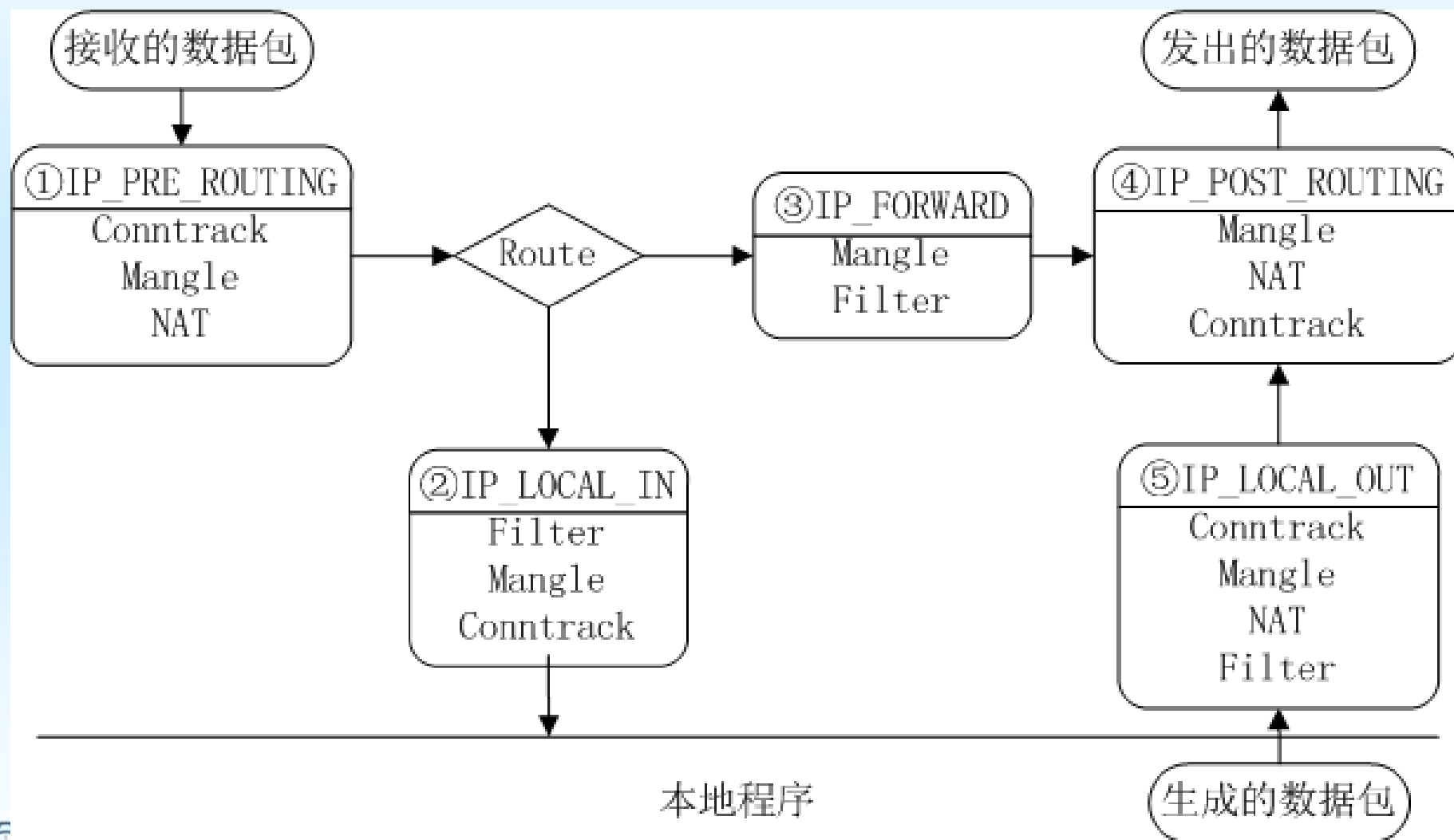
◆ 是嵌入在Linux内核IP协议栈中的一个通用架构。

➤ 它提供了一系列的“表”（tables）

- ✓ 每个表由若干“链”（chains）组成，
- ✓ 每条链中可以有一条或数条规则（rule）。



Netfilter程序流程架构



规则组成

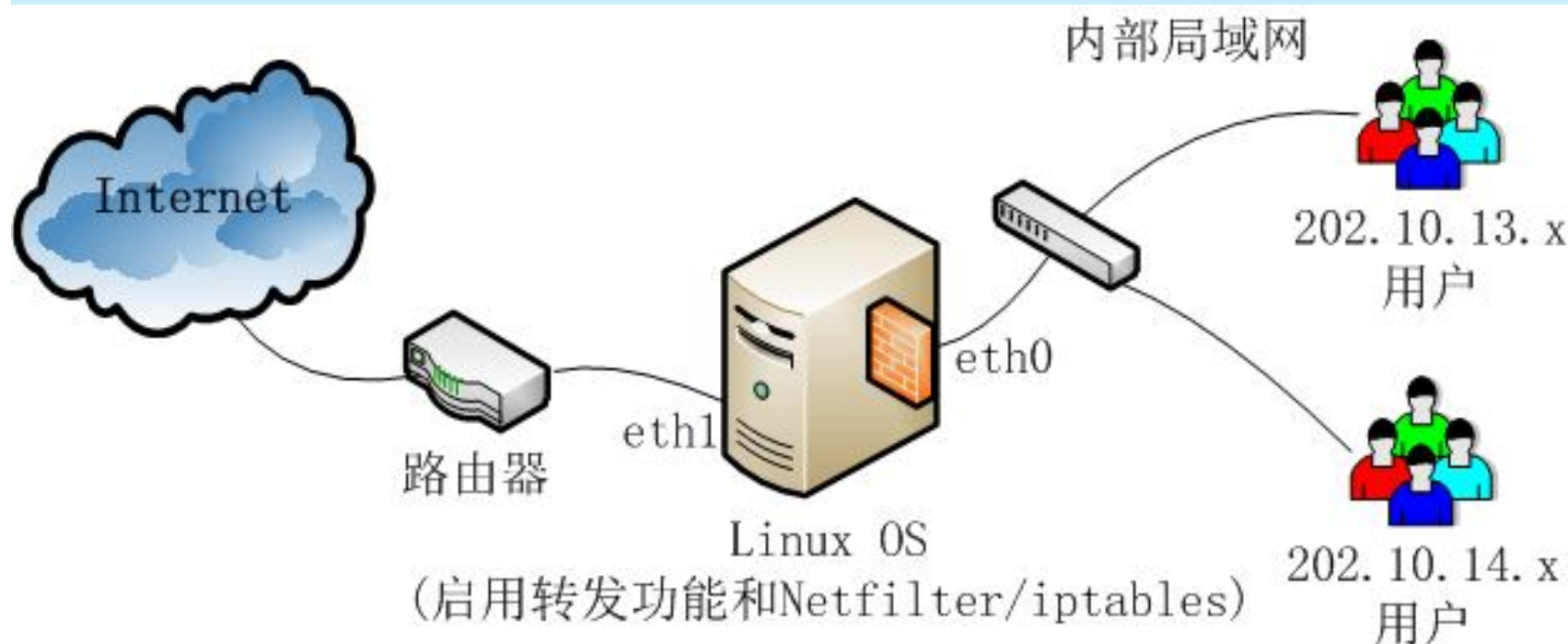
◆ IPtables命令 = 工作表 + 使用链 + 规则操作 + 目标动作 + 匹配条件

- 工作表：指定该命令针对的表，缺省表为filter；
- 使用链：指定表下面的某个链，实际上就是确定哪个钩子点；
- 规则操作：包括添加规则、插入规则、删除规则、替代规则、列出规则；
- 目标动作：有两个，ACCEPT（继续传递数据包），DROP（丢弃数据包）；
- 匹配条件：指过滤检查时，用于匹配数据包头信息的特征信息串，如地址、端口等。



Netfilter/Iptables 例子

- ◆ 目的：内网中只有202.10.13.0/24网段的用户可以访问外网，同时又只能使用TCP。
 - iptables -P FORWARD DROP
 - iptables -A FORWARD -p tcp -s 202.10.13.0/24 -j ACCEPT
 - iptables -A FORWARD -p tcp -d 202.10.13.0/24 -j ACCEPT



7.2.4 防火墙的体系结构

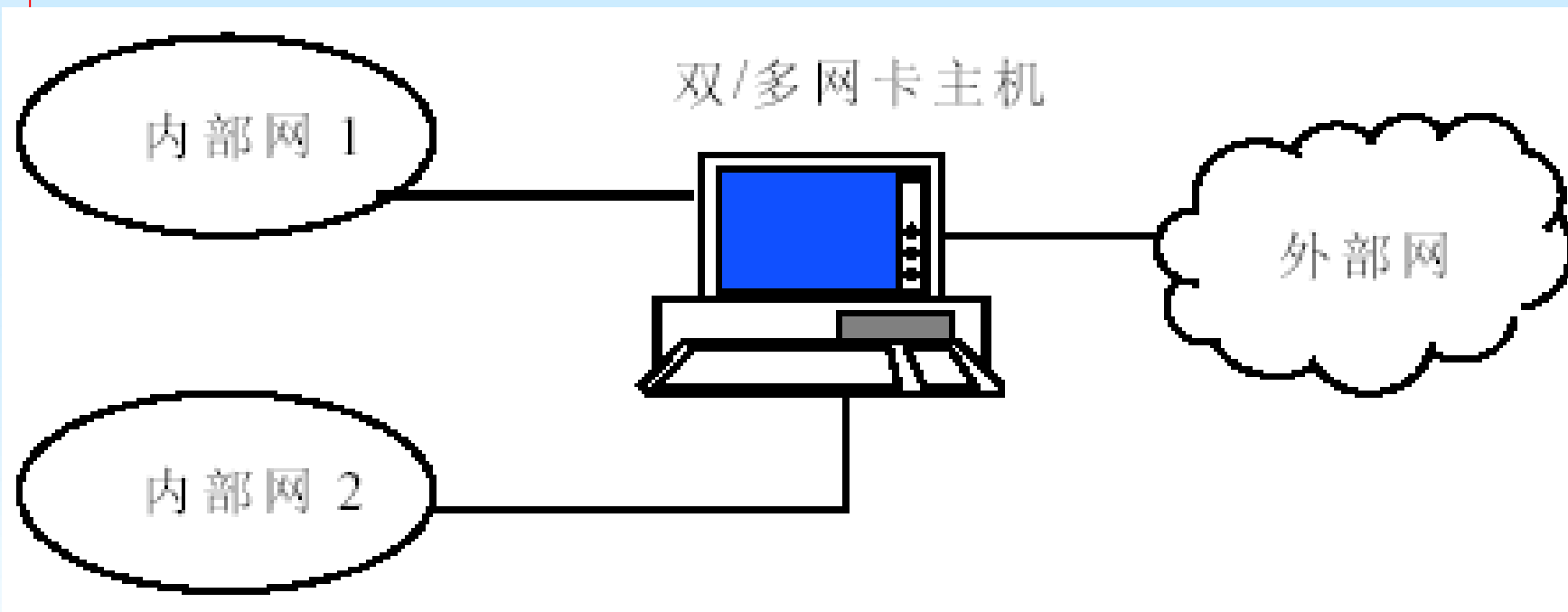
◆ 共有三种体系结构：

1. 双宿/多宿主机模式 (Dual-Homed /Multi-Homed Host Firewall)
2. 屏蔽主机模式(Screened Host Firewall)
3. 屏蔽子网模式(Screened Subnet mode)



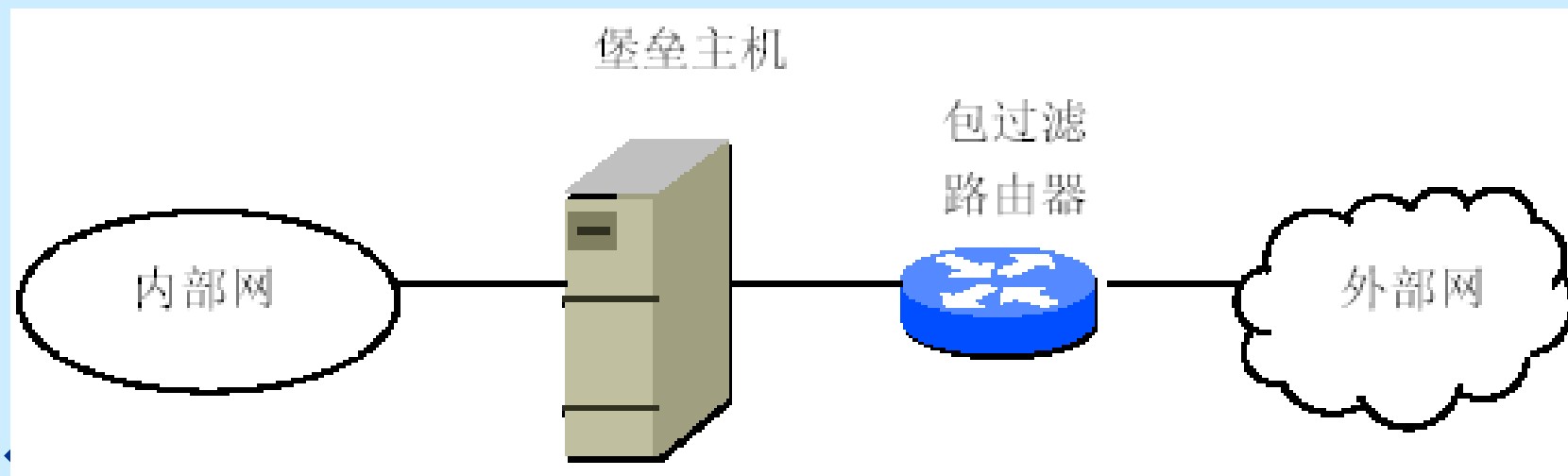
1. 双宿/多宿主机模式

- 它是一种拥有两个或多个连接到不同网络上的网络接口的防火墙。
- 通常用一台装有两块或多块网卡的堡垒主机做防火墙。



2. 屏蔽主机模式

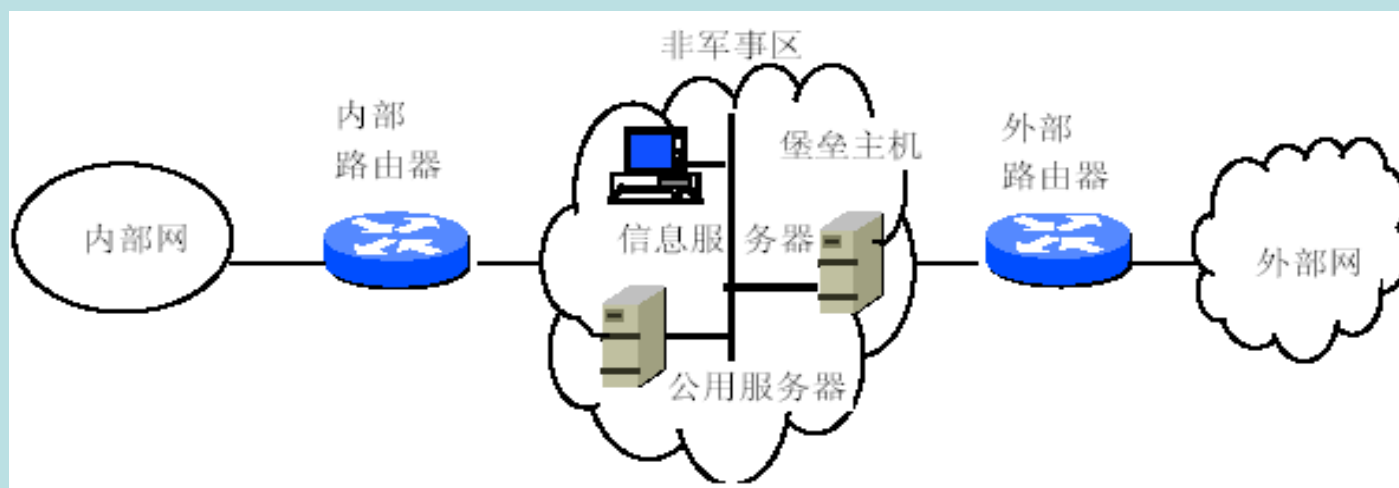
- ◆ 屏蔽主机防火墙由包过滤路由器和堡垒主机组成。



- ◆ 在这种方式的防火墙中，堡垒主机安装在内部网络上，
- ◆ 通常在路由器上设立过滤规则，并使这个堡垒主机成为从外部网络唯一可直接到达的主机，这确保了内部网络不受未被授权的外部用户的攻击。
- ◆ 屏蔽主机防火墙实现了网络层和应用层的安全，因而比单独的包过滤或应用网关代理更安全。
- ◆ 在这一方式下，过滤路由器是否配置正确是这种防火墙安全与否的关键，如果路由表遭到破坏，堡垒主机就可能被越过，使内部网完全暴露。

3. 屏蔽子网模式

- ◆ 采用了两个包过滤路由器和一个堡垒主机，在内外网络之间建立了一个被隔离的子网，定义为“非军事区（de-militarized zone）”网络，有时也称作周边网（perimeter network）。



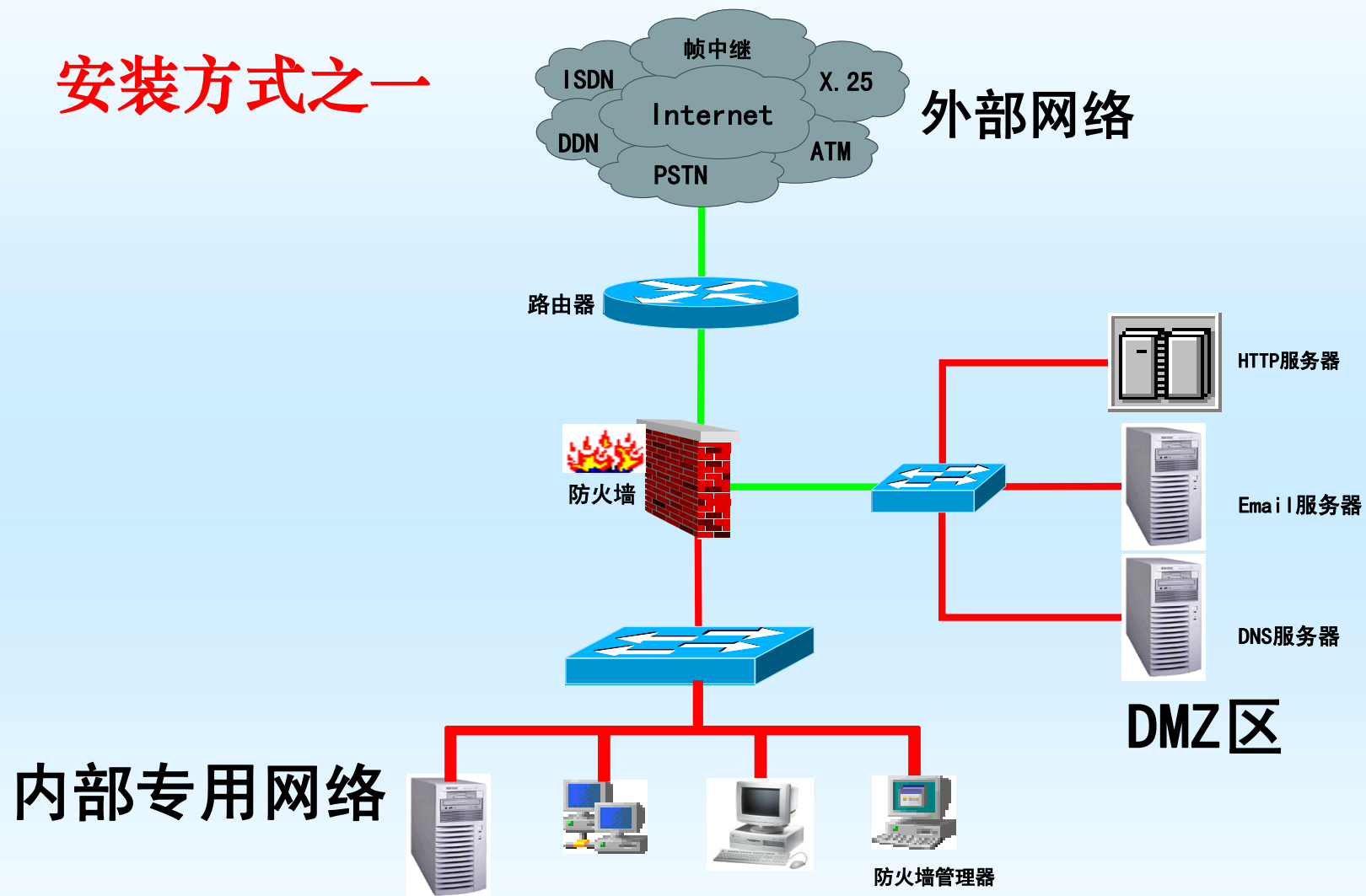
- ◆ 屏蔽子网模式特点：
- ◆ 网络管理员将堡垒主机，WEB服务器、Mail服务器等公用服务器放在非军事区网络中。
- ◆ 内部网络和外部网络均可访问屏蔽子网，但禁止它们穿过屏蔽子网通信。
- ◆ 在这一配置中，即使堡垒主机被入侵者控制，内部网仍受到内部包过滤路由器的保护。
- ◆ 堡垒主机运行各种代理服务。

防火墙体系结构的组合形式

1. 最少服务、最小特权原则
2. 使用多堡垒主机
3. 合并内部路由器与外部路由器
4. 合并堡垒主机与外部路由器
5. 合并堡垒主机与内部路由器
6. 使用多台内部路由器
7. 使用多台外部路由器
8. 使用多个周边网络
9. 使用双重宿主主机与屏蔽子网



安装方式之一



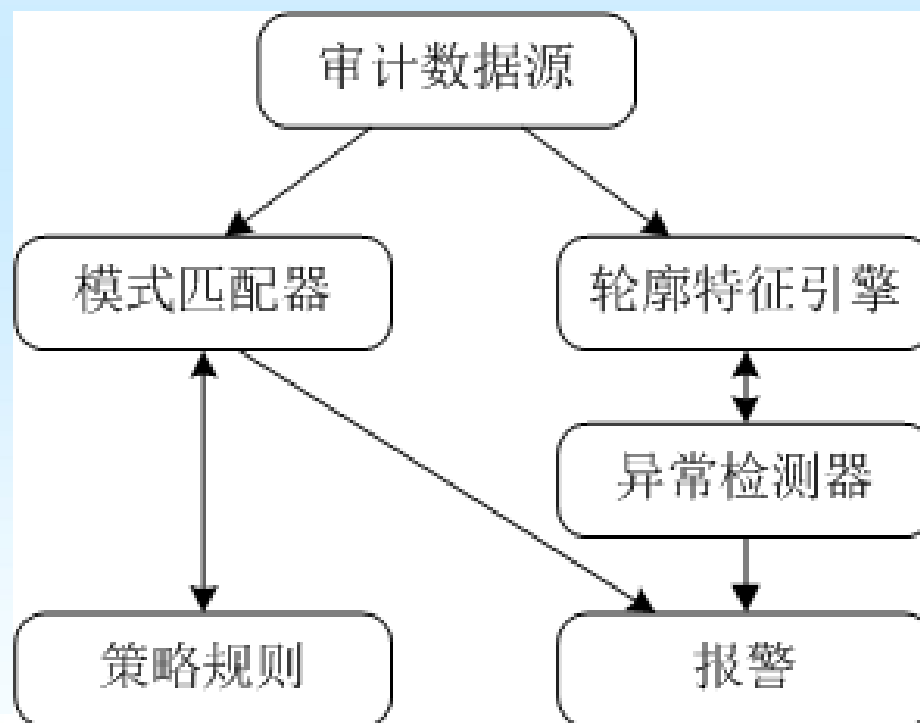
7.3 入侵检测系统

◆ IDS (Intrusion Detection System)

- 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。

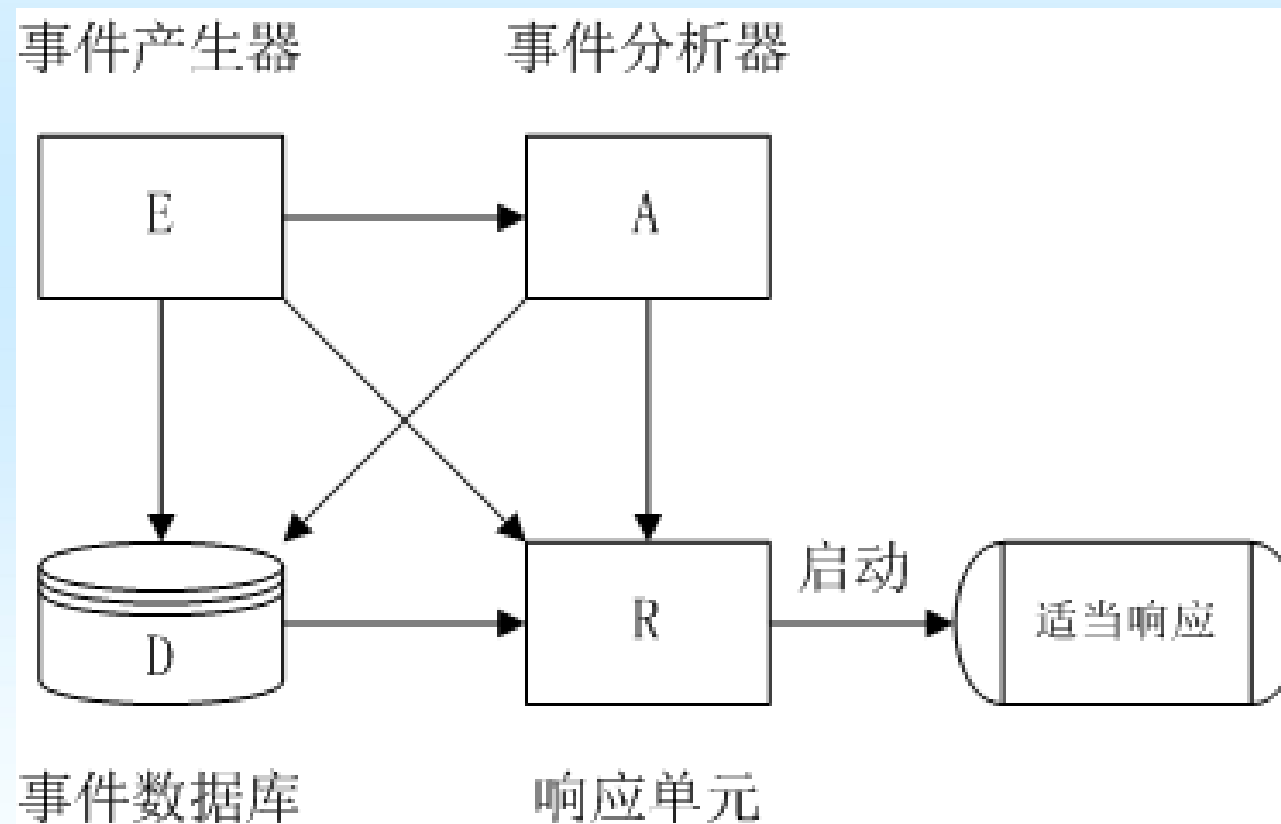
7.3.1 入侵检测概述

- ◆ 1980年，James P. Anderson，《Computer Security Threat Monitoring and Surveillance》此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)



入侵检测系统工作过程

◆ 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。如可以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

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



入侵检测几个重要概念

◆ 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的造成威胁的一类行为。

◆ 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。

◆ 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：

- 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。

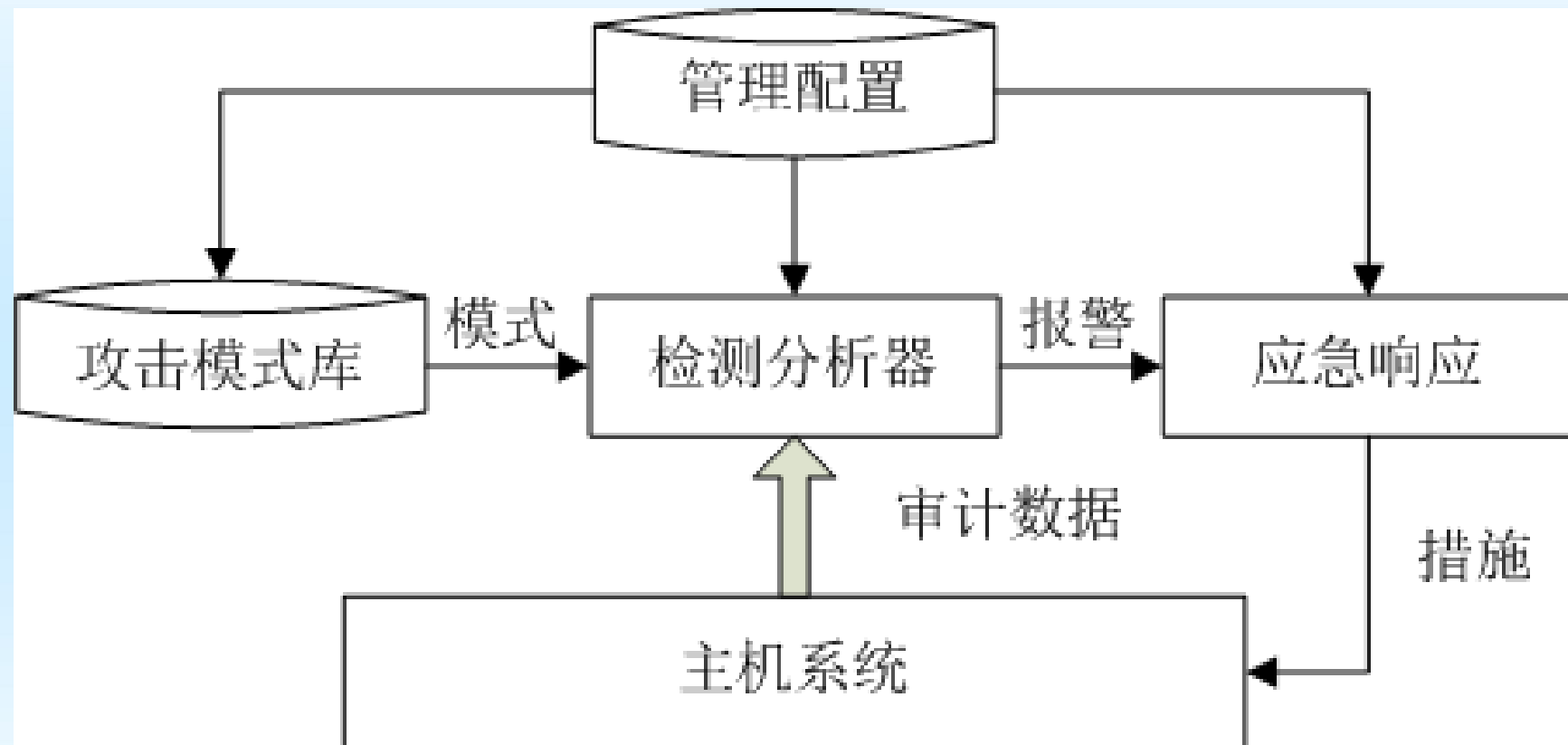
7.3.2 入侵检测系统分类

◆ 以数据源为分类标准

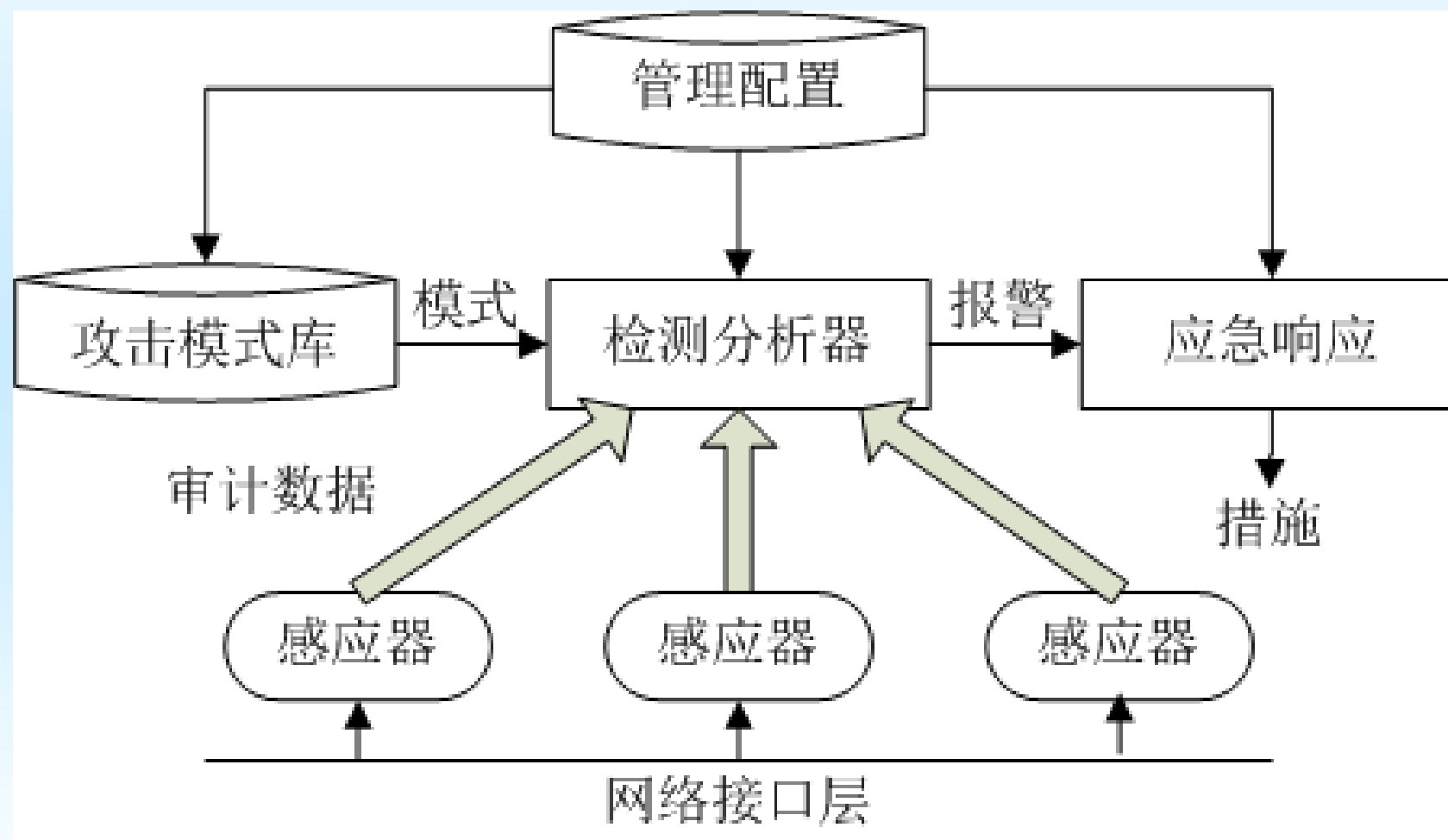
- 主机型入侵检测系统HIDS (Host-based Intrusion Detection System)
- 网络型入侵检测系统NIDS (Network-based Intrusion Detection System)。



主机型入侵检测系统

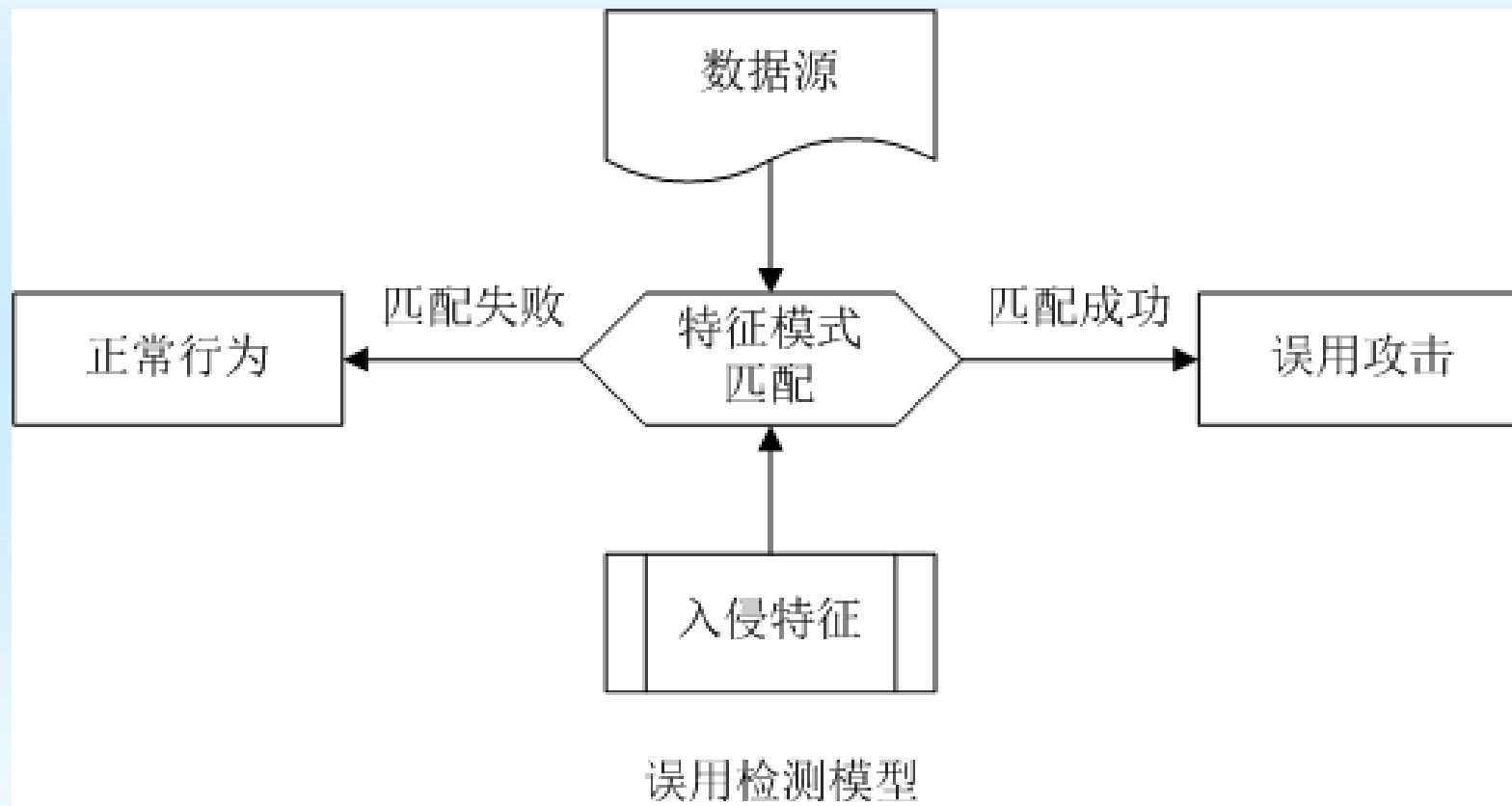


网络型入侵检测系统

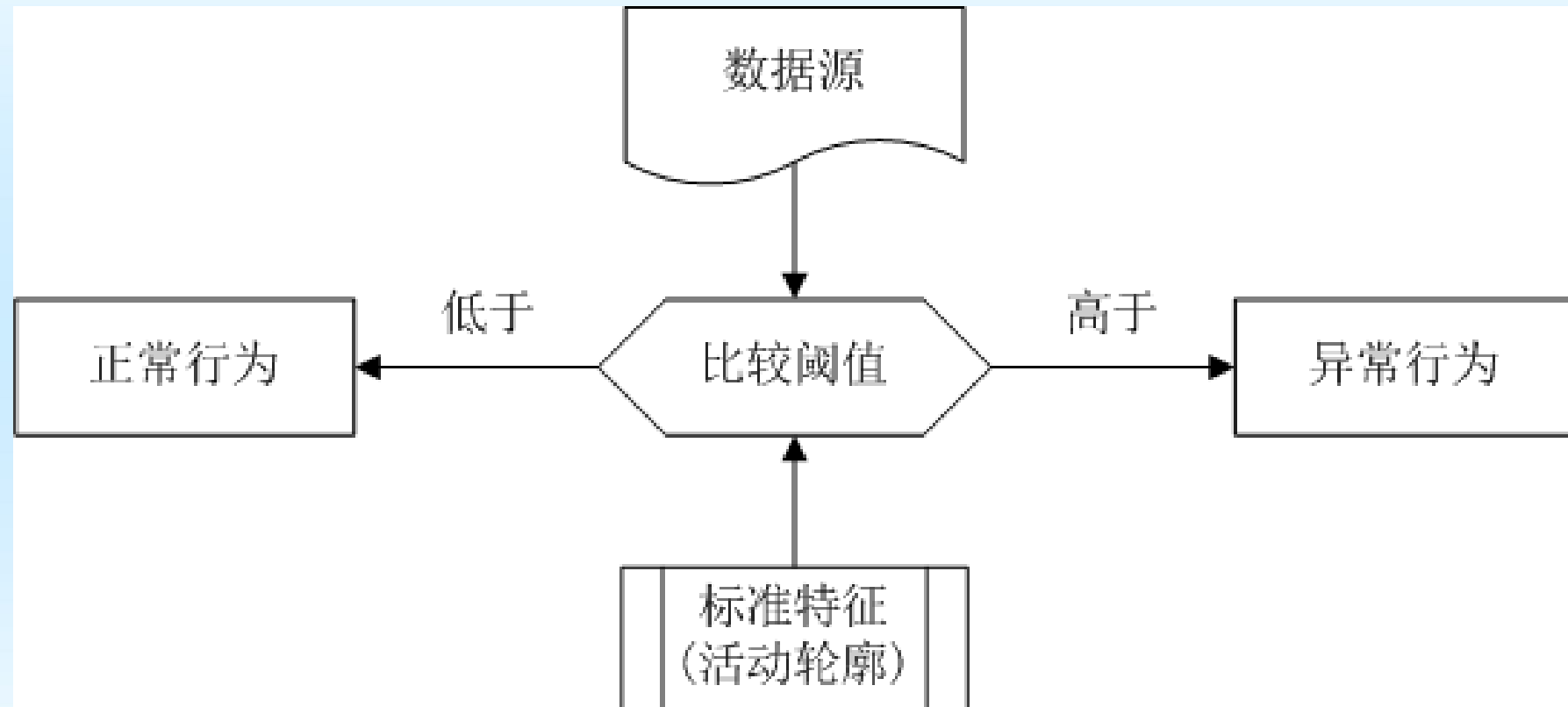


以检测技术为分类标准

◆ 基于误用检测（ Misuse Detection ）的IDS



基于异常检测 (Anomaly Detection) 的IDS



7.3.3 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。
- ◆ 从误用检测、异常检测、诱骗和响应等四个方面分析一下入侵检测的主要技术方法。
- ◆ 误用检测技术
 - 专家系统
 - 特征分析
 - 模型推理
 - 状态转换分析
 - 完整性校验等



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。



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。
- ◆ 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”技术的起源(1)

入侵检测系统能够对网络和系统的活动情况进行监视,及时发现并报告异常现象。但是,入侵检测系统在使用中存在着难以检测新类型黑客攻击方法,可能漏报和误报的问题。

蜜罐使这些问题有望得到进一步的解决,通过观察和记录黑客在蜜罐上的活动,人们可以了解黑客的动向、黑客使用的攻击方法等有用信息。如果将蜜罐采集的信息与IDS采集的信息联系起来,则有可能减少IDS的漏报和误报,并能用于进一步改进IDS的设计,增强IDS的检测能力。

“蜜罐”技术的起源(2)

- “蜜罐”的思想最早是由Clifford Stoll 于1988 年5 月提出。该作者在跟踪黑客的过程中，利用了一些包含虚假信息文件作为黑客“诱饵”来检测入侵，这就是蜜罐的基本构想，但他并没有提供一个专门让黑客攻击的系统。
- 蜜罐正式出现是 Bill Cheswick 提到采用**服务仿真**和**漏洞仿真**技术来吸引黑客。
 - 服务仿真技术是蜜罐作为应用层程序打开一些常用服务端口监听，仿效实际服务器软件的行为响应黑客请求。例如，提示访问者输入用户名和口令，从而吸引黑客进行登录尝试。
 - 漏洞仿真是指返回黑客的响应信息会使黑客认为该服务器上存在某种漏洞，从而引诱黑客继续攻击。

蜜罐技术的发展历程

◆ 蜜罐 (Honeypot)

- 物理蜜罐
- 虚拟蜜罐工具: DTK, Honeyd
- 专用蜜罐工具: mwcollect, nepenthes

◆ 蜜网 (Honeynet)

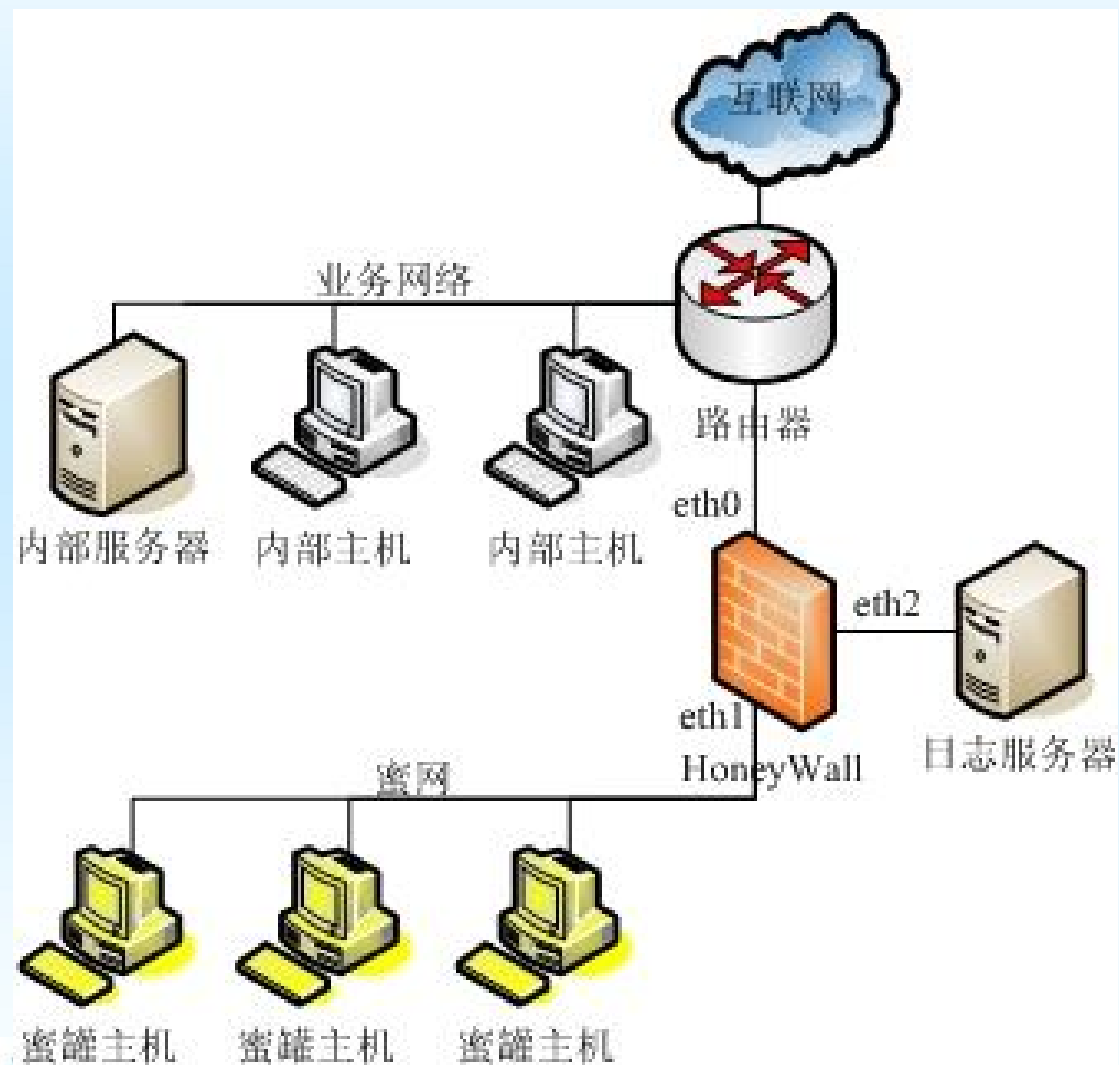
- The Honeynet Project
- Gen 1 / Gen 2 / Gen 3 Honeynet
- Research Purpose

◆ 蜜场 (Honeyfarm)

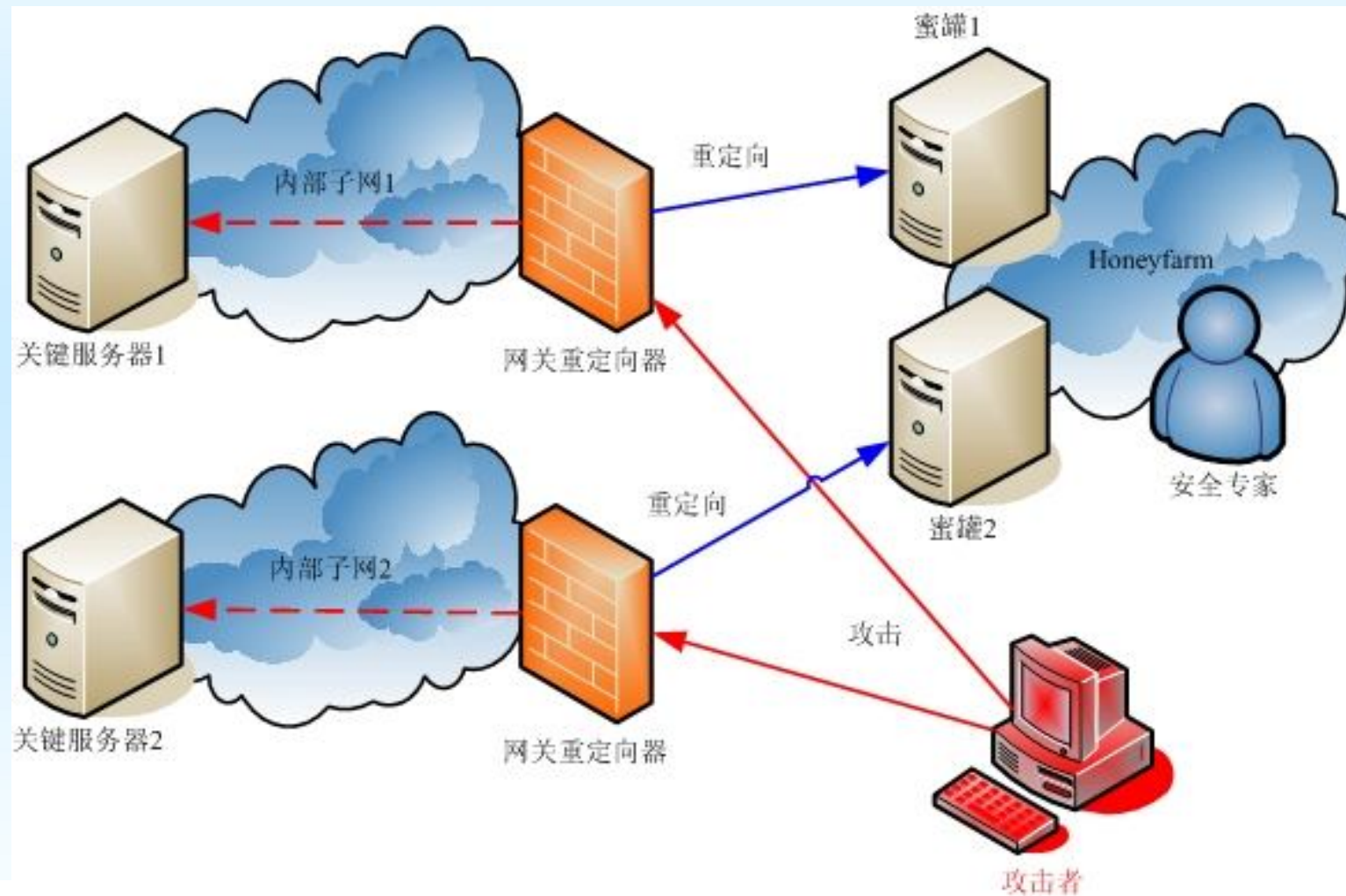
- 蜜罐技术如何有效地对一个大型网络提供防护功能？
- 外/内部安全威胁的发现、重定向、跟踪



蜜网的体系框架

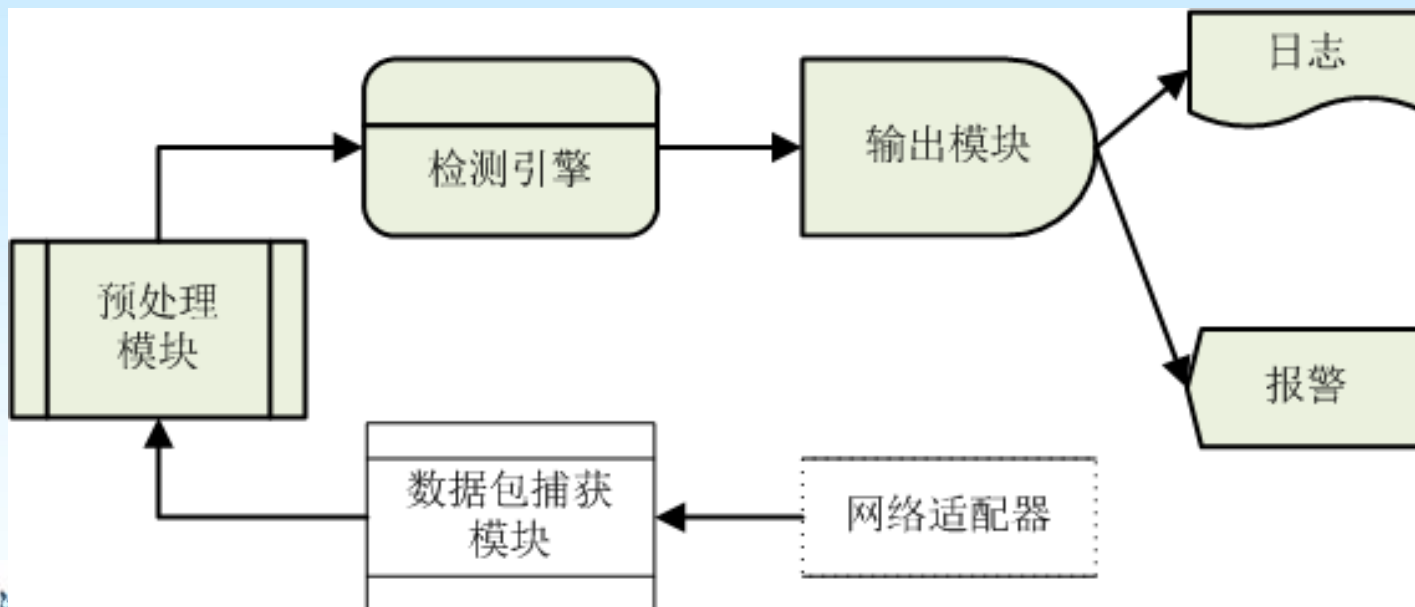


蜜场



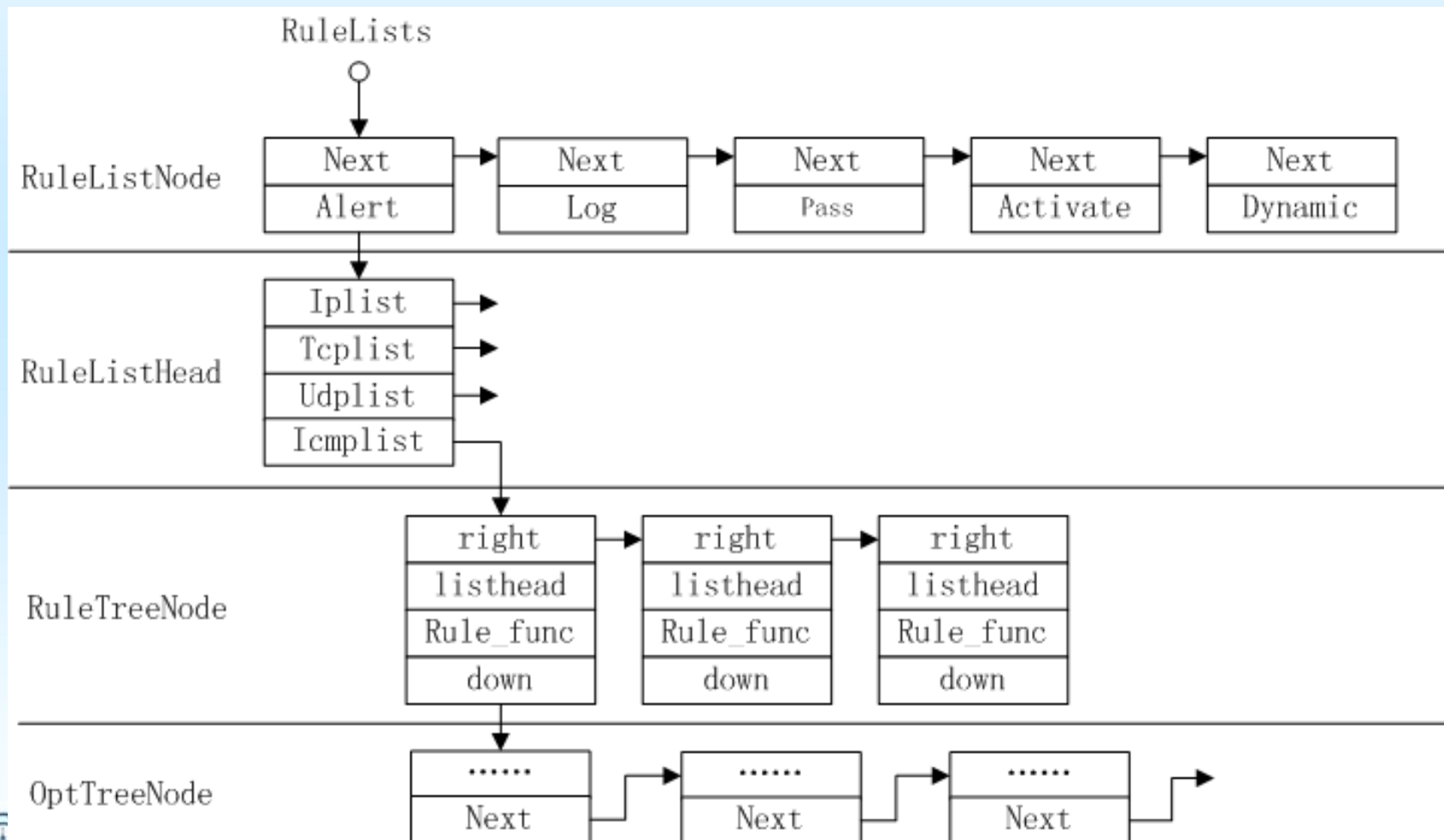
7.3.4 Snort系统

- ◆ 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规则库

- ◆ 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。



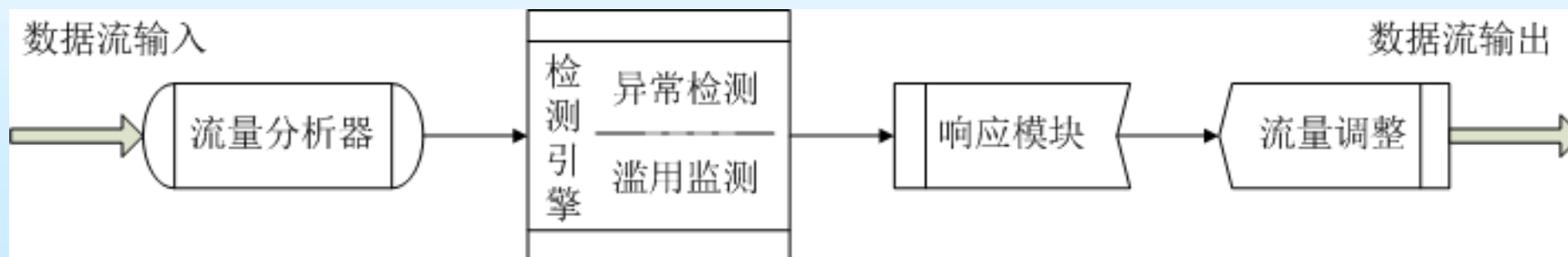
Snort规则例子

- ◆ 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。Snort定义了五种可选的行为：
 - Alert：使用设定的警告方法生成警告信息，并记录这个数据报文；
 - Log：使用设定的记录方法来记录这个数据报文；
 - Pass：忽略这个数据报文；
 - Activate：进行alert，然后激活另一个dynamic规则。
 - Dynamic：等待被一个activate规则激活，被激活后就作为一条log规则执行。



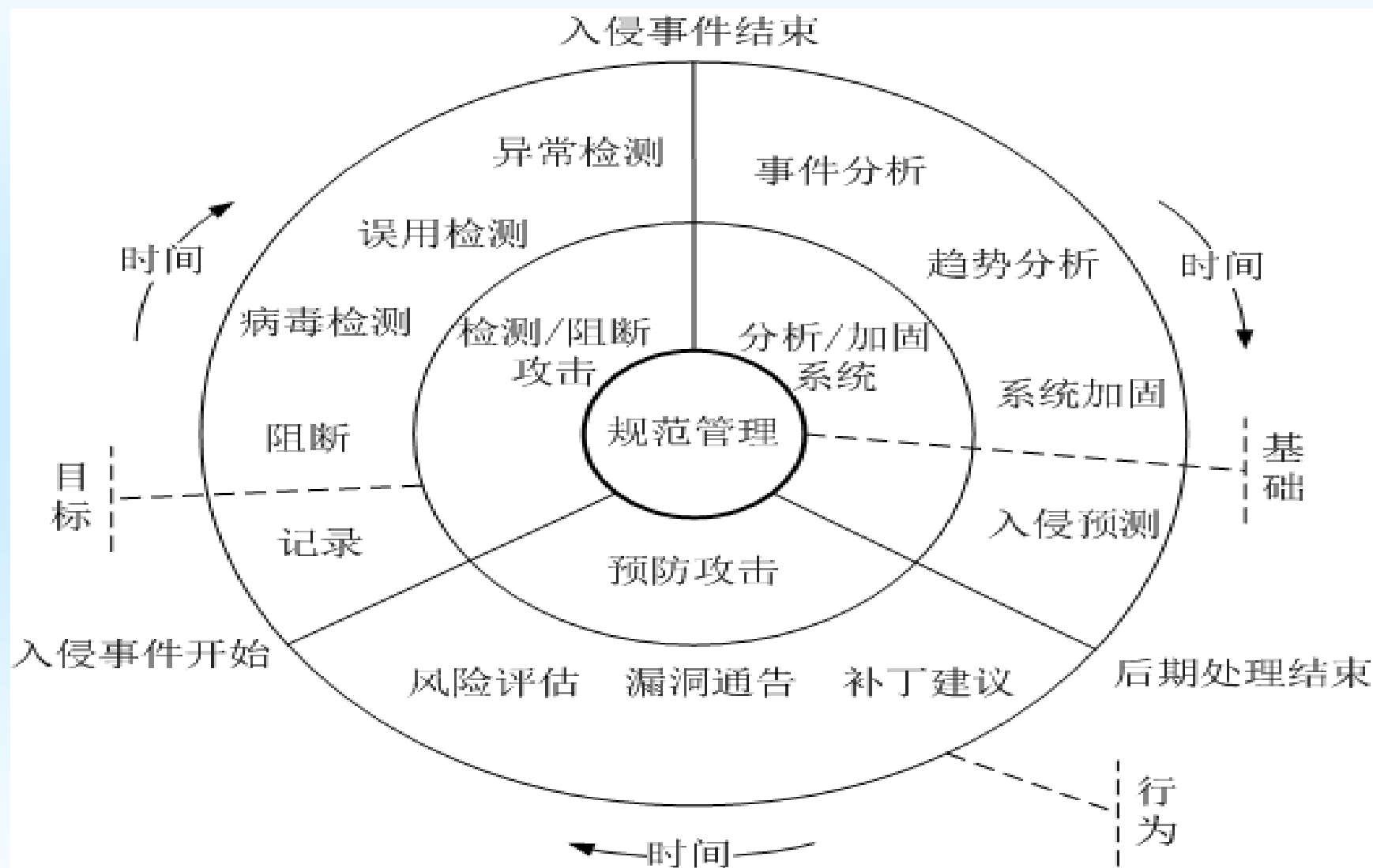
7.4 网络防御的新技术

◆ 入侵防御系统IPS (Intrusion Prevention System)



- 具备检测和防御功能。
- 可检测到IDS检测不到的攻击行为。
- 黑客较难破坏入侵攻击数据。
- 具有双向检测防御功能。

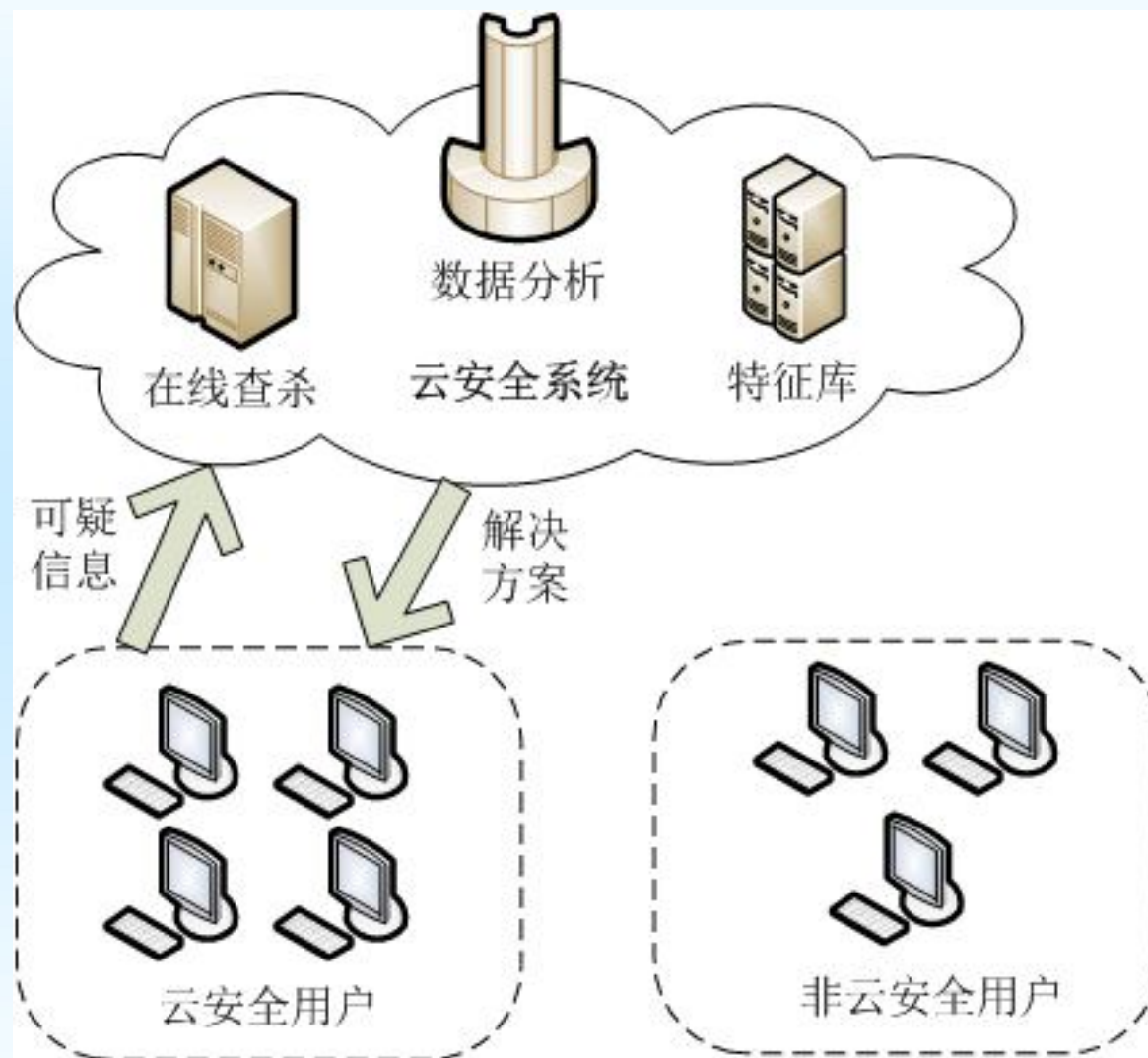
入侵管理系统IMS (Intrusion Management System)



云安全

- ◆ “云”是近几年来出现的概念，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。

云安全示意图



Any question?

