信息安全概论

网络防御

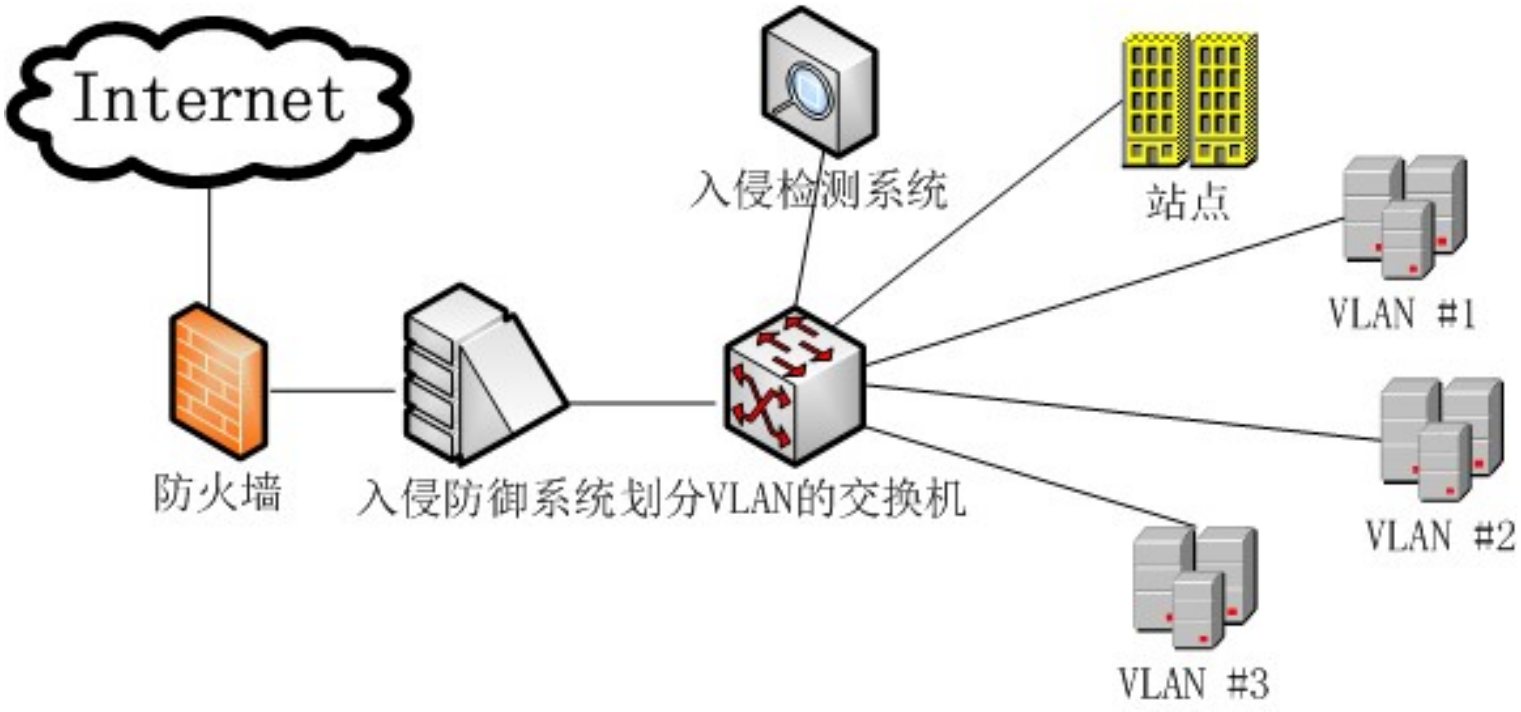
刘亚维

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。



7.2 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。

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。

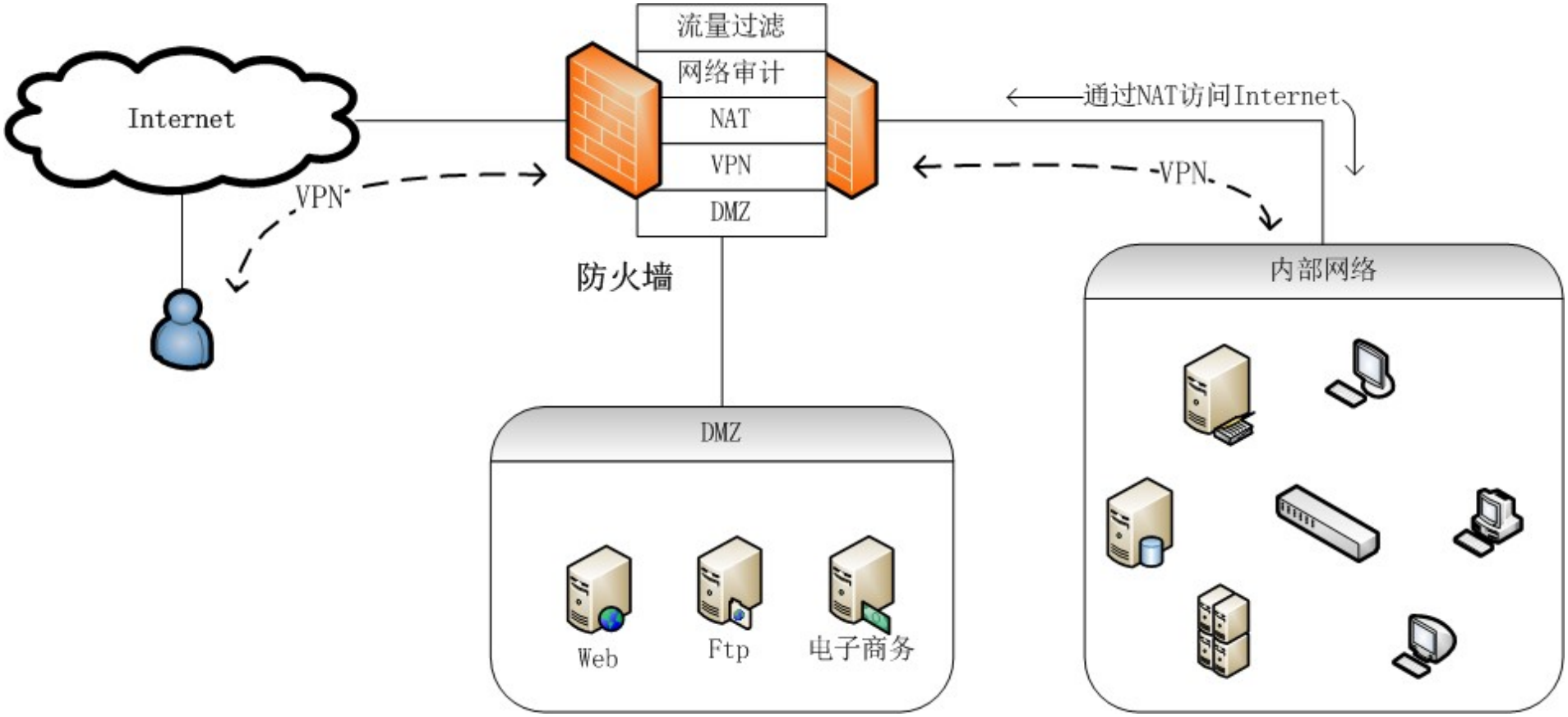
分类

- 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

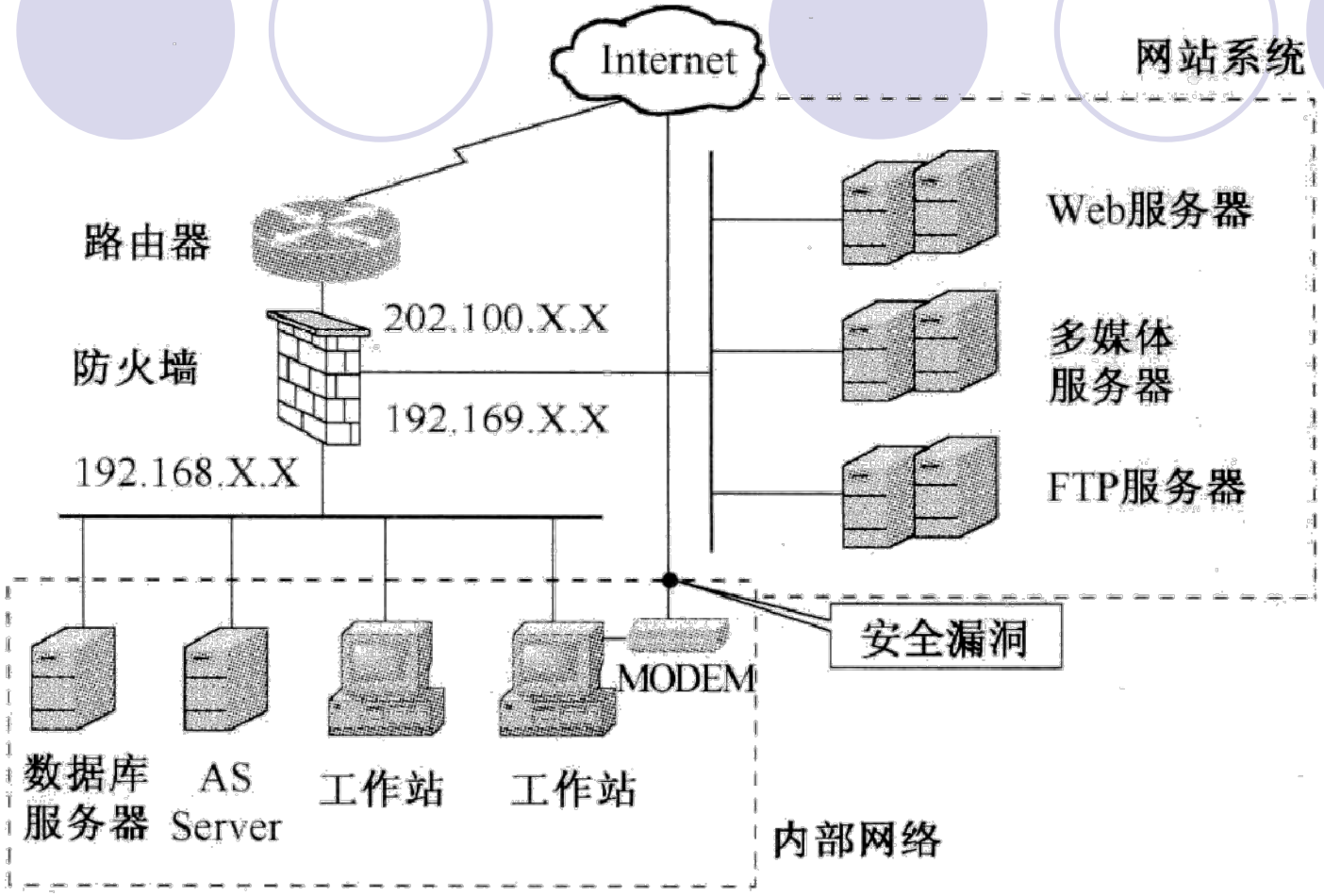
- 网络流量过滤
  - 通过在防火墙上进行安全规则配置，可以对流经防火墙的网络流量进行过滤。
- 网络监控审计
  - 防火墙记录访问并生成网络访问日志，提供网络使用情况的统计数据。
- 支持NAT部署
  - NAT（Network Address Translation）是网络地址翻译的缩写，是用来缓解地址空间短缺的主要技术之一
- 支持DMZ
  - DMZ是英文“Demilitarized Zone”的缩写,它是设立在非安全系统与安全系统之间的缓冲区。
- 支持VPN
  - 通过VPN，企业可以将分布在各地的局域网有机地连成一个整体。

典型企业防火墙应用


流量过滤
网络审计
NAT
VPN
DMZ
防火墙
Internet
VPN
通过NAT访问Internet
VPN
内部网络
DMZ
Web
Ftp
电子商务

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。


Internet
网站系统
路由器
Web服务器
202.100.X.X
防火墙
多媒体
服务器
192.169.X.X
FTP服务器
192.168.X.X
安全漏洞
MODEM
数据库
服务器
AS
Server
工作站
工作站
内部网络

防火墙的后门

7.2.2 防火墙技术

- 防火墙技术是一种综合技术，主要包括：包过滤技术、网络地址转换技术和代理技术。

包过滤技术

- 包过滤原理
  - 包过滤是最早应用到防火墙当中的技术之一。
  - 针对网络数据包由信息头和数据信息两部分组成这一特点而设计。
  - 防火墙通过对信息头的检测就可以决定是否将数据包发往目的地址，从而达到对进入和流出网络的数据进行监测和限制的目的。

包过滤技术

- 包过滤技术
  - 数据包过滤功能的实现依赖于包过滤规则，有时人们也称之为访问控制列表(ACL，Access Control List)。
  - 只有满足访问控制列表的数据才被转发，其余数据则被从数据流中删除。
  - 为了保证所有流入和流出网络的数据包都被监控和检测，包过滤器必须放置在网络单点访问点的位置。

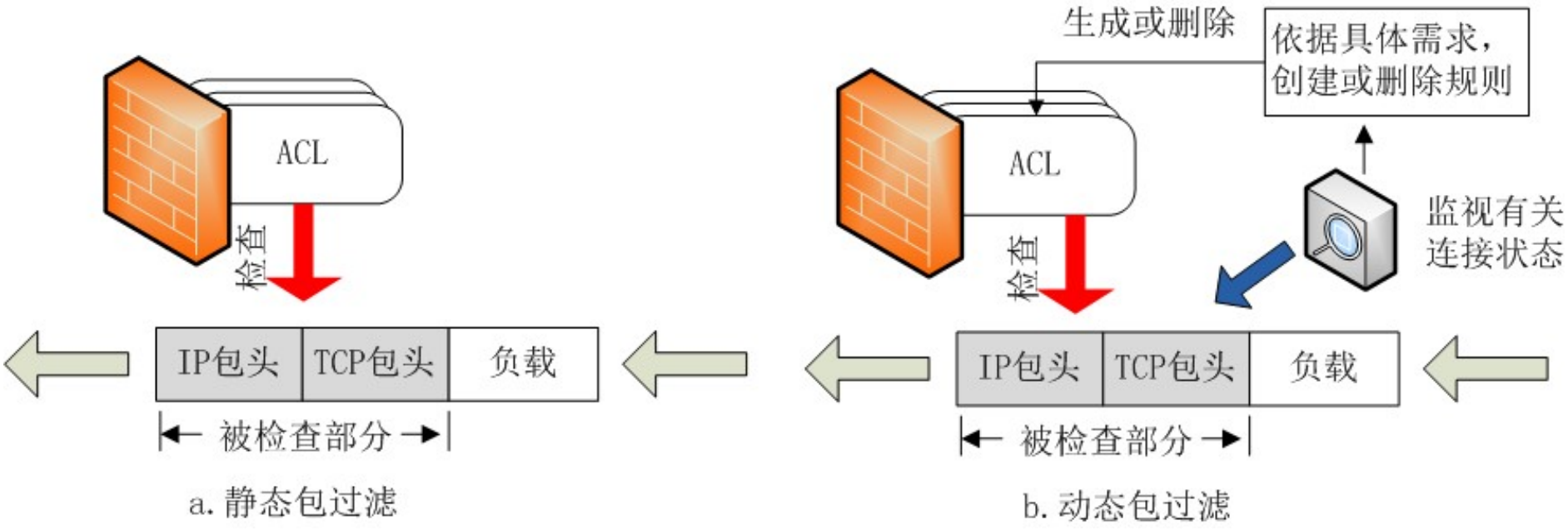
访问控制列表ACL

- 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

静态与动态包过滤

- 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。



网络地址翻译技术

- NAT(Network Address Translation，网络地址翻译)
- 最初设计目的
  - 增加私有组织的可用地址空间
  - 解决将现有的私有TCP／IP网络连接到互联网上的IP地址编号问题。

网络地址翻译技术

- 网络地址翻译技术通过地址映射保证了使用私有IP地址的内部主机或网络能够连接到公用网络。
  - 私有IP地址只能作为内部网络号，不在互联网主干网上使用。
  - NAT网关被安放在网络末端区域(内部网络和外部网络之间的边界点上)，并且在源自内部网络的数据包发送到外部网络之前把数据包的源地址转换为惟一的IP地址。

网络地址翻译技术

- 静态网络地址翻译技术
  - NAT网关位于内部和外部网络接口卡之间，只有在内部和外部网络接口之间传输的数据包才进行转换。
  - 如果网络地址翻译技术完全依赖于手工指定内部局部地址和内部全局地址之间映射关系来运行，我们称之为静态网络地址翻译技术

IPv4私有地址

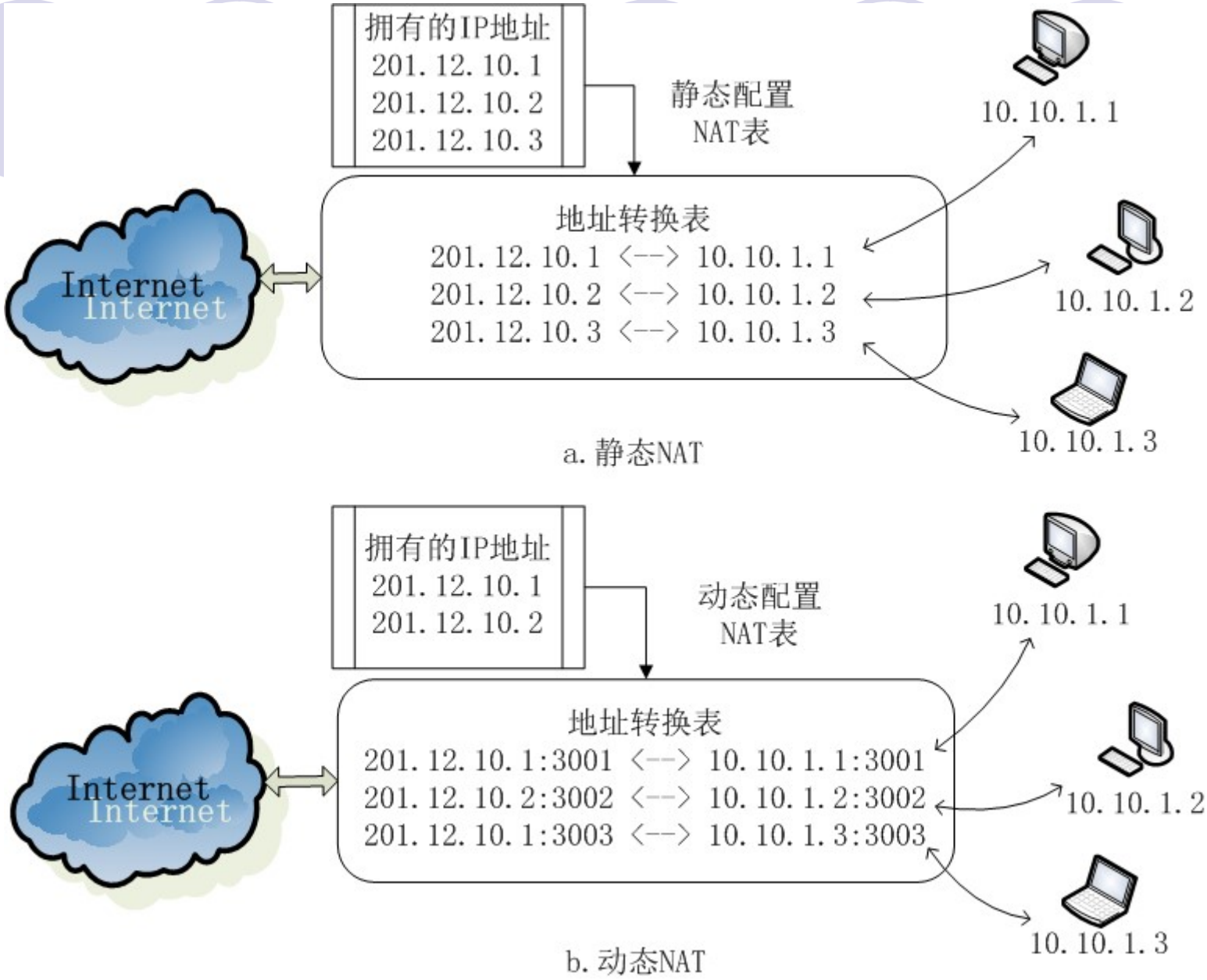
RFC1918 规定区块名	IP地址区段	IP数量
24位区块	10.0.0.0 – 10.255.255.255	16,777,216
20位区块	172.16.0.0 – 172.31.255.255	1,048,576
16位区块	192.168.0.0 – 192.168.255.255	65,536

网络地址翻译技术

动态网络地址翻译技术

- NAT映射表由防火墙动态建立，对网络管理员和用户透明。
- 网络地址翻译技术允许将多个内部IP地址映射成为一个外部IP地址。
  - 从本质上讲网络地址映射并不是简单的IP地址之间的映射，而是网络套接字映射，网络套接字由IP地址和端口号共同组成。当多个不同的内部局部地址映射到同一个内部全局地址时，可以使用不同端口号来区分它们

NAT（Network Address Translation）



网络地址翻译技术

依然存在一些问题难以解决：

- 一些应用层协议的工作特点导致了它们无法使用网络地址翻译技术
- 静态和动态网络地址映射安全问题
- 对内部主机的引诱和特洛伊木马攻击
- 状态表超时问题

网络代理技术

- 应用层代理
  - 包过滤技术在网络层实现数据包的拦截、分析和过滤等应用
  - 代理(Proxy)技术针对每一个特定应用进行实现，在应用层实现网络数据流保护功能
    - 具有状态性
      - 能够提供部分与传输有关的状态
    - 能完全提供与应用相关的状态部分传输信息
    - 代理也能够处理和管理信息。

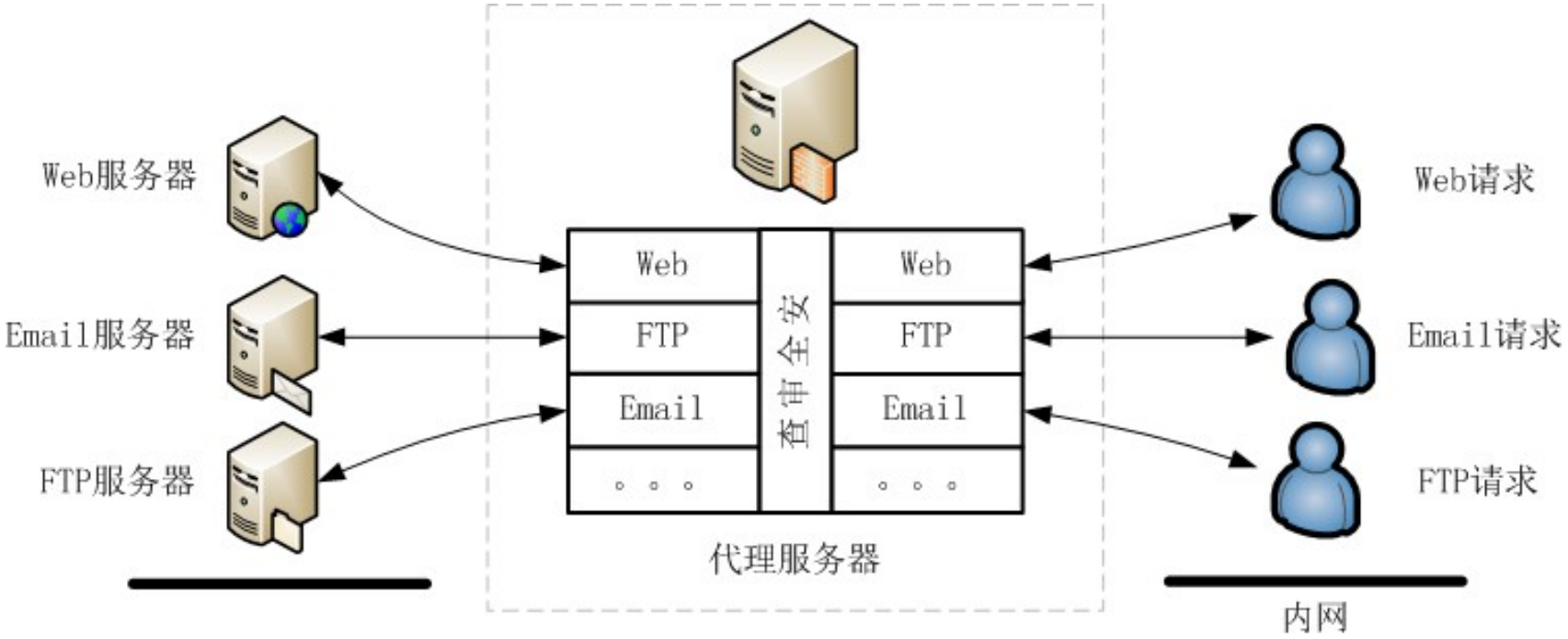
应用层代理

- 应用层代理服务器起到了内部网络向外部网络申请服务时的中间转接作用
  - 对外部网来说，外部网所见到的只是代理服务器，
    - 它收到的请求都是从代理服务器来的
  - 对内部网来说，客户机所能直接访问的只是代理服务器
    - 请求首先是发给了代理服务器。

应用层代理

- 外部网络主机通过应用层代理访问内部网络主机
- 内部网络主机只接受应用层代理提出的服务请求，拒绝外部网络节点的直接请求

网络代理技术



INTERNET客户通过应用层代理访问内部网络主机

电路级代理

- 电路级代理(电路级网关)
  - 也是一种代理
  - 只是建立起一个回路，对数据包只起转发的作用。
  - 电路级网关依赖于TCP连接，并不进行任何附加的包处理或过滤。

应用层代理

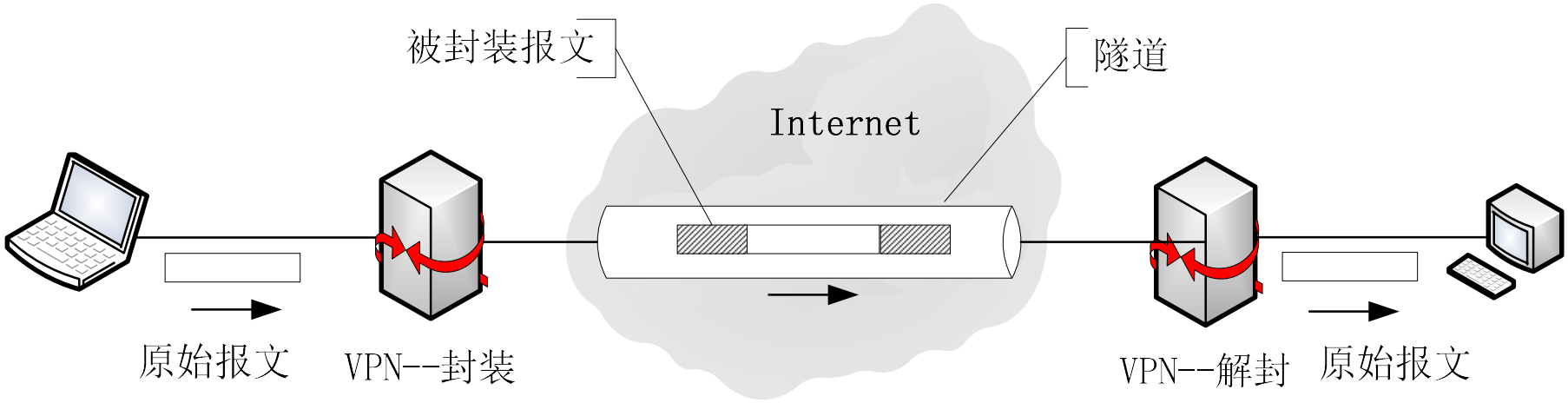
- *为一种特定的服务(如FTP，Telnet等)提供代理服务，它不但转发流量而且对应用层协议做出解释。*

电路级代理

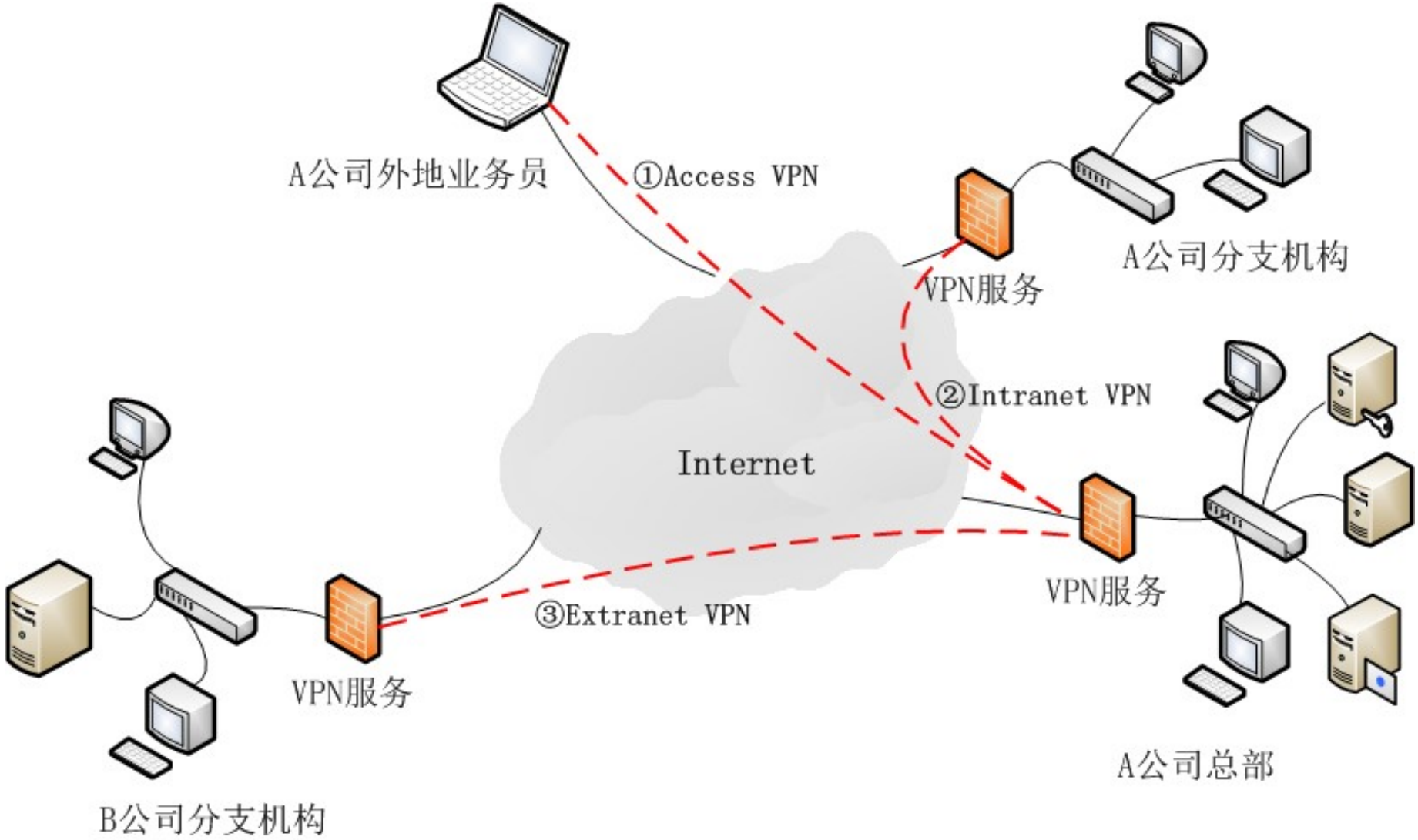
- 电路级网关只用来在两个通信终点之间转接数据包
  - 数据包被提交给应用层来处理。
  - 只是将简单的字节复制
  - 由于连接似乎是起源于防火墙，其隐藏了受保护网络的有关信息
- 电路级网关对外像一个代理，而对内则是一个过滤路由器

VPN（Virtual Private Network）

- VPN：虚拟的企业内部专线，也称虚拟私有网。
- VPN是通过一个公用网络（通常是Internet）建立一个临时的、安全的连接，
  - 可以理解为一条穿过公用网络的安全、稳定的隧道，两台分别处于不同网络的机器可以通过这条隧道进行连接访问，就像在一个内部局域网一样。

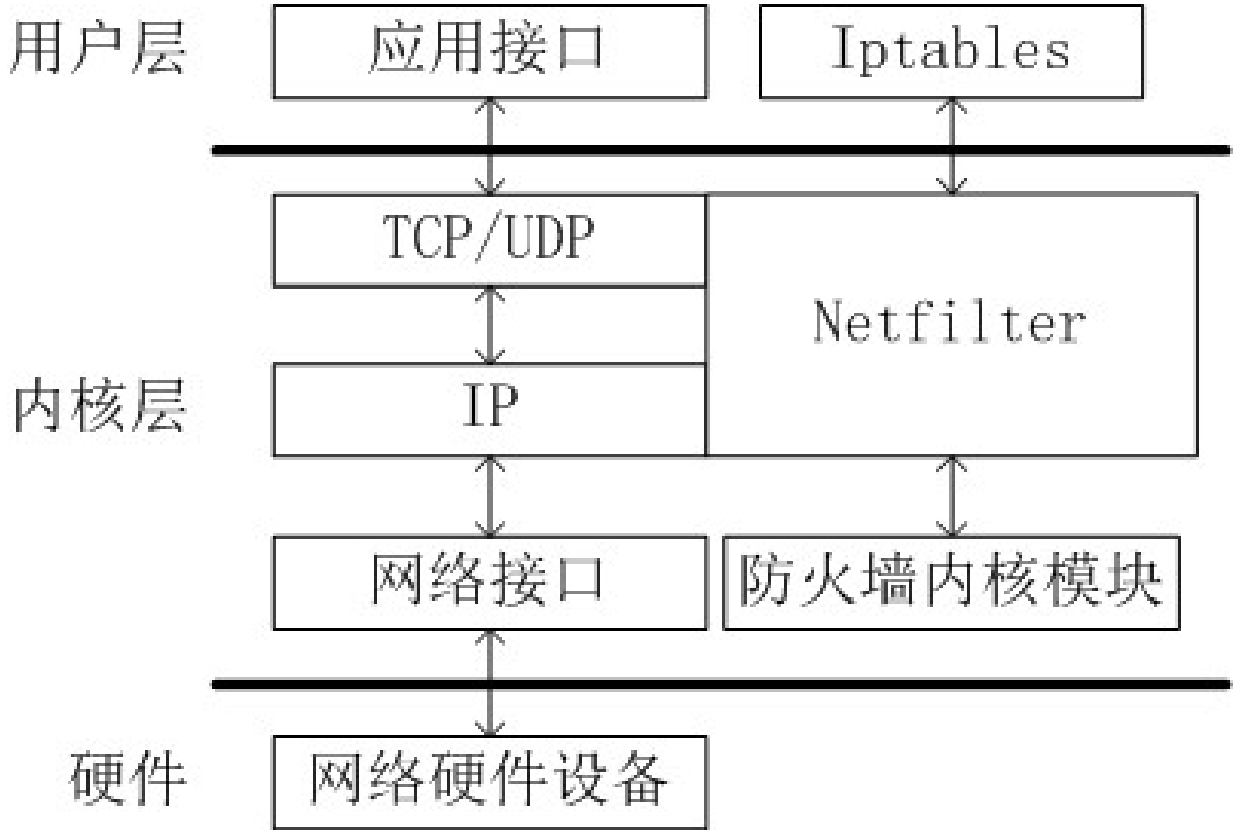


VPN典型应用


A公司外地业务员
①Access VPN
A公司分支机构
VPN服务
②Intranet VPN
Internet
VPN服务
③Extranet VPN
VPN服务
A公司总部
B公司分支机构

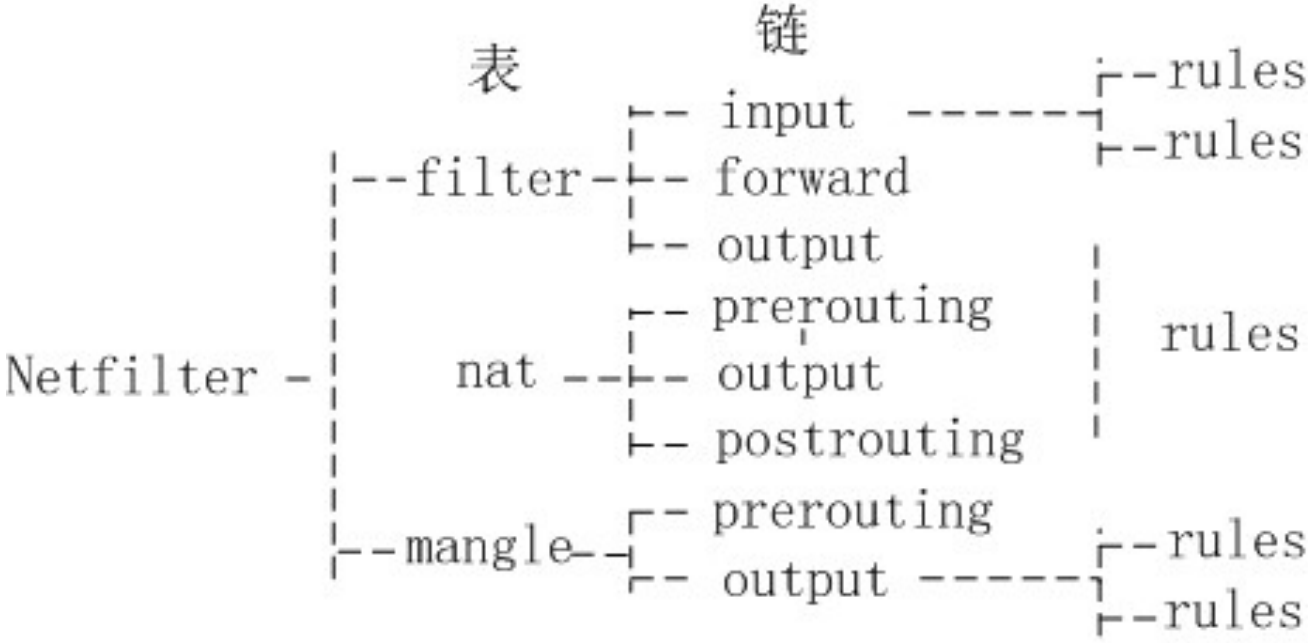
7.2.4 Netfilter/IPtables防火墙

- 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。

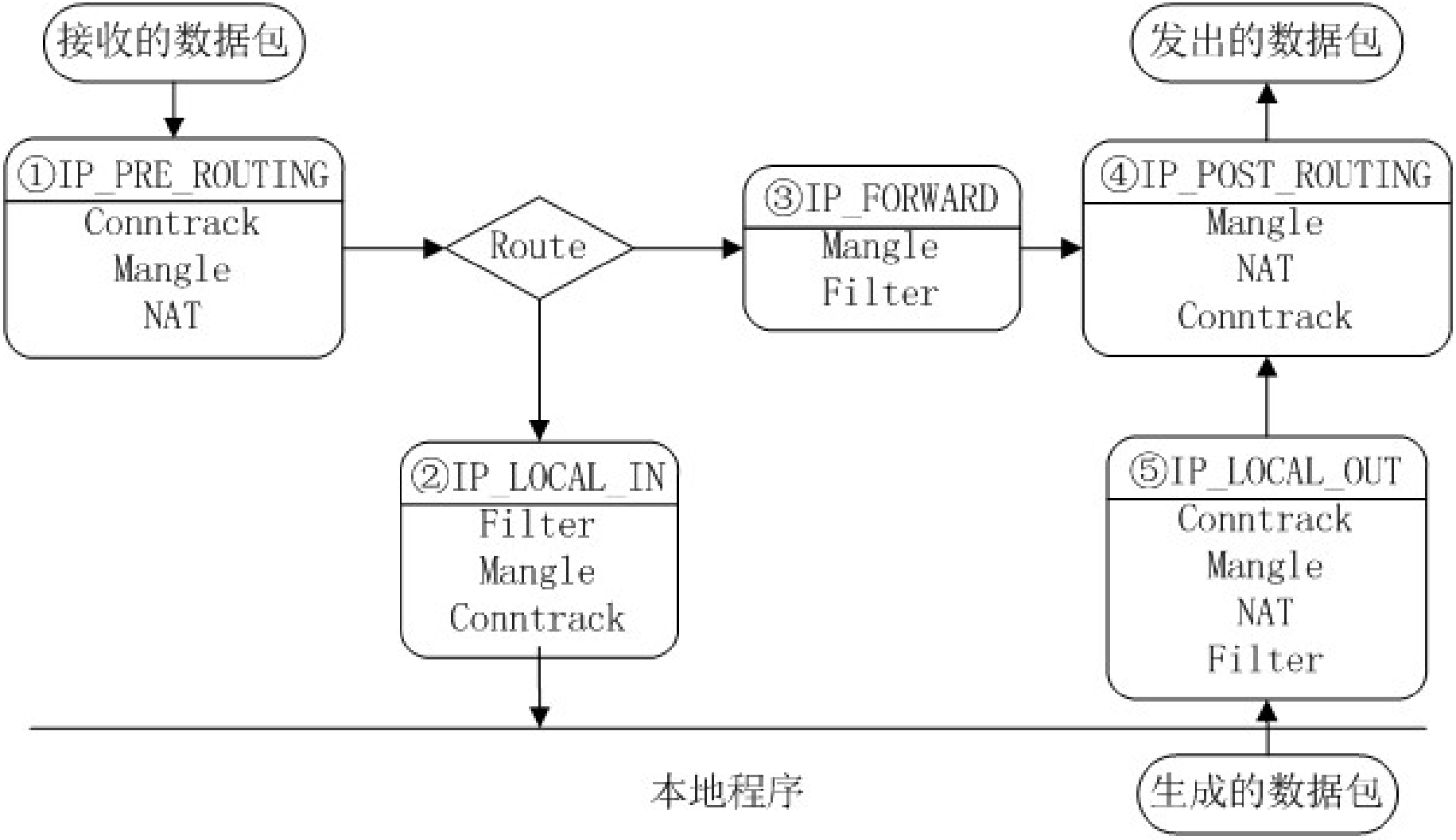


Netfilter通用架构

- 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

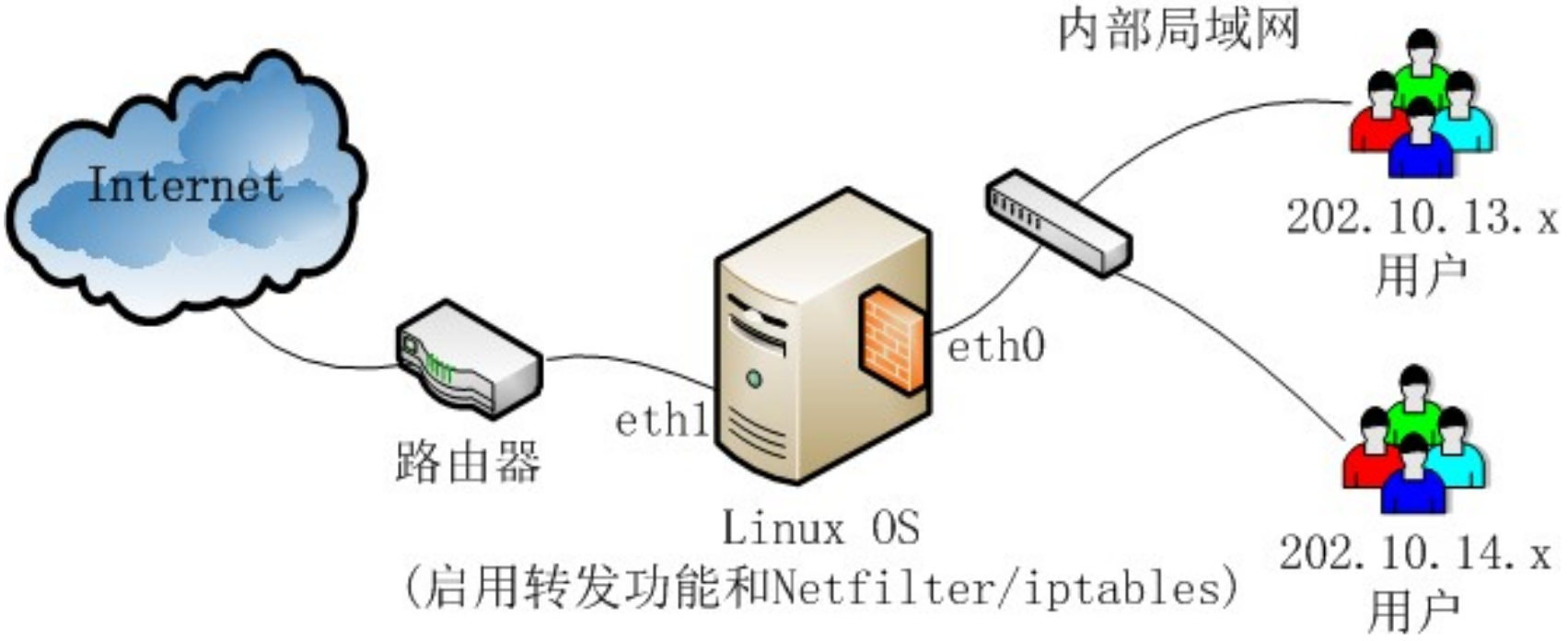


规则组成

- 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



7.3 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

- 为什么需要**IDS**
  - 关于防火墙
    - 网络边界的设备
    - 自身可以被攻破
    - 对某些攻击保护很弱
    - 不是所有的威胁来自防火墙外部
  - 入侵行为的普遍性
    - 各种入侵教程
    - 各种黑客工具

入侵（ **Intrusion** ）

- Intrusion : Attempting to break into or misuse your system.
- Intruders may be from outside the network or legitimate users of the network.
- Intrusion can be a physical, system or remote intrusion.

入侵检测

- 入侵检测（Intrusion Detection）是对入侵行为的发觉。
  - 它通过从计算机网络或计算机系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象
  - 传统的信息安全方法采用严格的访问控制和数据加密策略来防护，但在复杂系统中，这些策略是不充分的。
    - 它们是系统安全不可缺的部分但不能完全保证系统的安全

入侵检测的定义

- 对系统的运行状态进行监视，发现各种攻击企图、攻击行为或者攻击结果，以保证系统资源的机密性、完整性和可用性

- 进行入侵检测的软件与硬件的组合便是入侵检测系统
  - IDS ： Intrusion Detection System

入侵检测的起源（1）

- 审计技术
  - 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

入侵检测的起源（2）

- 1980年4月，James P. Anderson，《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
  - 计算机系统威胁分类: 外部渗透、内部渗透和不法行为
  - 提出了利用审计跟踪数据监视入侵活动的思想

这份报告被公认为是入侵检测的开山之作

入侵检测的起源（3）

- 从**1984**年到**1986**年，乔治敦大学的**Dorothy Denning**，**SRI/CSL**的**Peter Neumann**
- 研究出了一个实时入侵检测系统模型**—IDES**（入侵检测专家系统）

入侵检测的起源（4）

- 1990，加州大学戴维斯分校的L. T. Heberlein等人开发出了NSM（Network Security Monitor）
  - 第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异种主机
- 入侵检测系统发展史翻开了新的一页，两大阵营正式形成：
  - 基于网络的IDS
  - 基于主机的IDS

IDS基本结构

入侵检测系统包括三个功能部件

- 信息收集
- 信息分析
- 结果处理

信息收集

- 收集来源
  - 系统或网络的日志文件
  - 网络流量
  - 系统目录和文件的异常变化
  - 程序执行中的异常行为
- 收集位置
  - 在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息
  - 尽可能扩大检测范围
  - 从一个源来的信息有可能看不出疑点

信息分析

- 分析技术
  - 模式匹配
  - 统计分析
  - 完整性分析，往往用于事后分析

模式匹配

- 将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。
  - 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（如利用正规的数学表达式来表示安全状态的变化）

统计分析

- 创建一个统计描述
  - 针对系统对象（如用户、文件、目录和设备等），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）
  - 测量属性的平均值和偏差将被用来与网络、系统的行为进行比较
- 判断入侵
  - 任何观察值在正常值范围之外时

完整性分析

- 主要关注某个文件或对象是否被更改
  - 包括文件和目录的内容及属性
  - 在发现被更改的、被安装木马的应用程序方面特别有效

入侵检测性能关键参数

- 误报(false positive)：如果系统错误地将异常活动定义为入侵

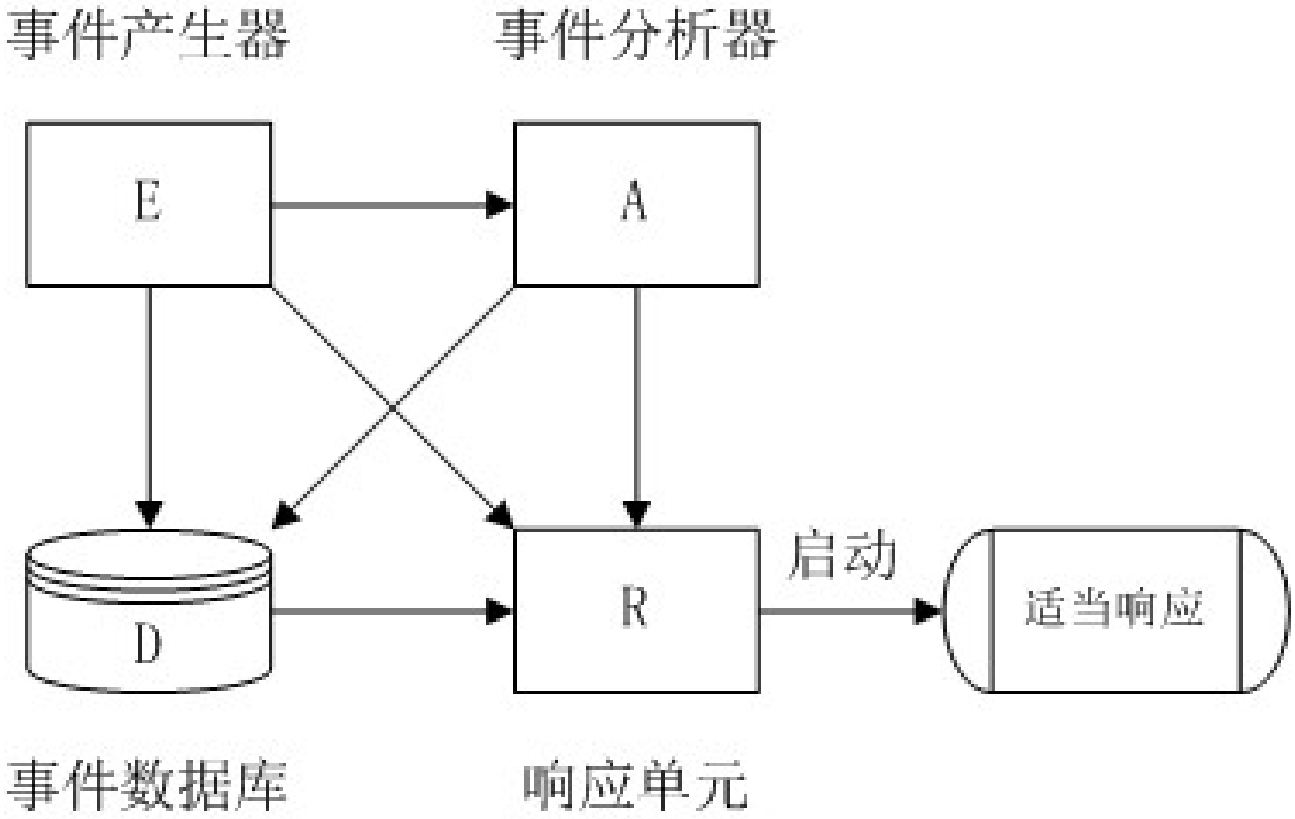
- 漏报(false negative)：如果系统未能检测出真正的入侵行为

CIDF通用模型

- 为了更高效地开发入侵检测系统，有必要制定IDS标准。
  - 大部分入侵检测系统大部分是基于各自的需求和设计独立开发的。
  - 不同系统间缺乏操作性和互用性，这对入侵检测系统的发展造成了障碍。

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。

入侵检测几个重要概念（续）

- 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。

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。

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）。

黑客入侵的过程和阶段

Phase 1:
Discover & Map

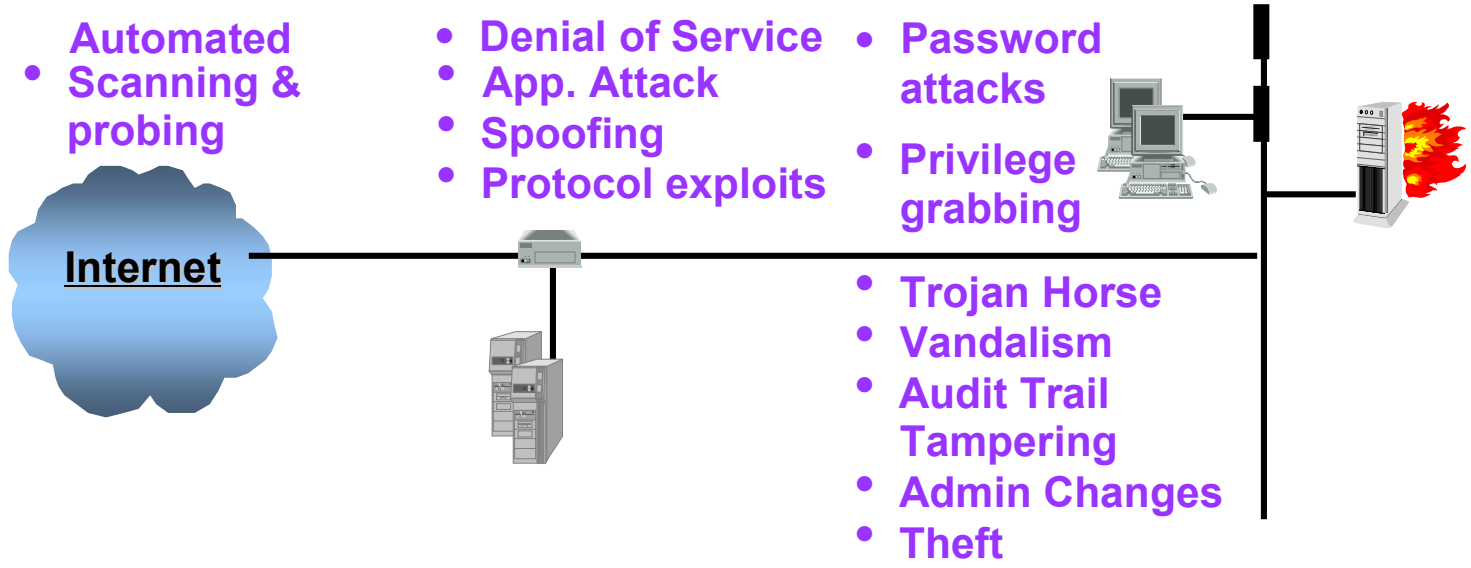
- Automated Scanning & probing

Phase 2:
Penetrate Perimeter

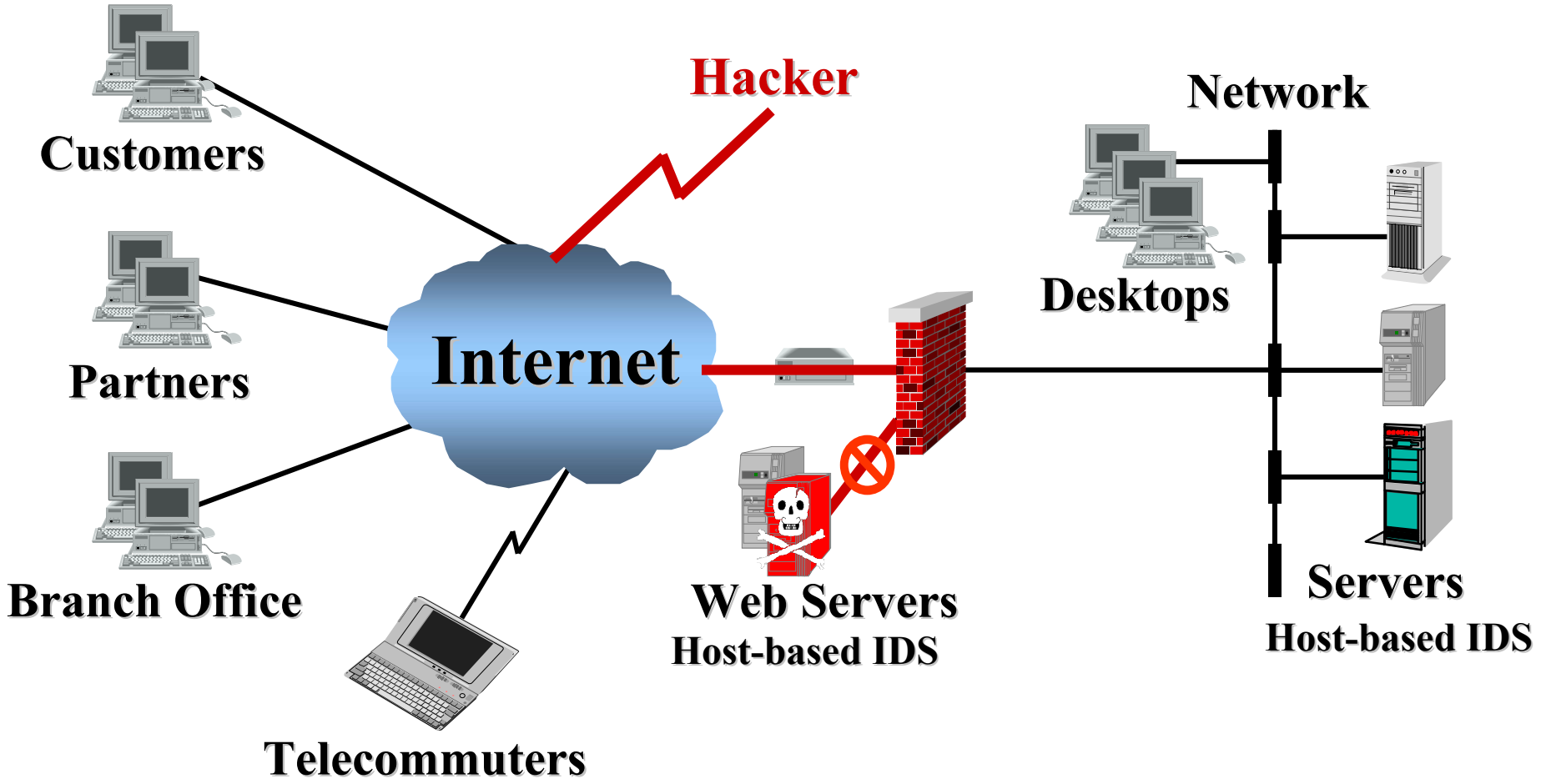
- Denial of Service
- App. Attack
- Spoofing
- Protocol exploits

Phase 3:
Attack/Control Resources

- Password attacks
- Privilege grabbing
- Trojan Horse
- Vandalism
- Audit Trail Tampering
- Admin Changes
- Theft



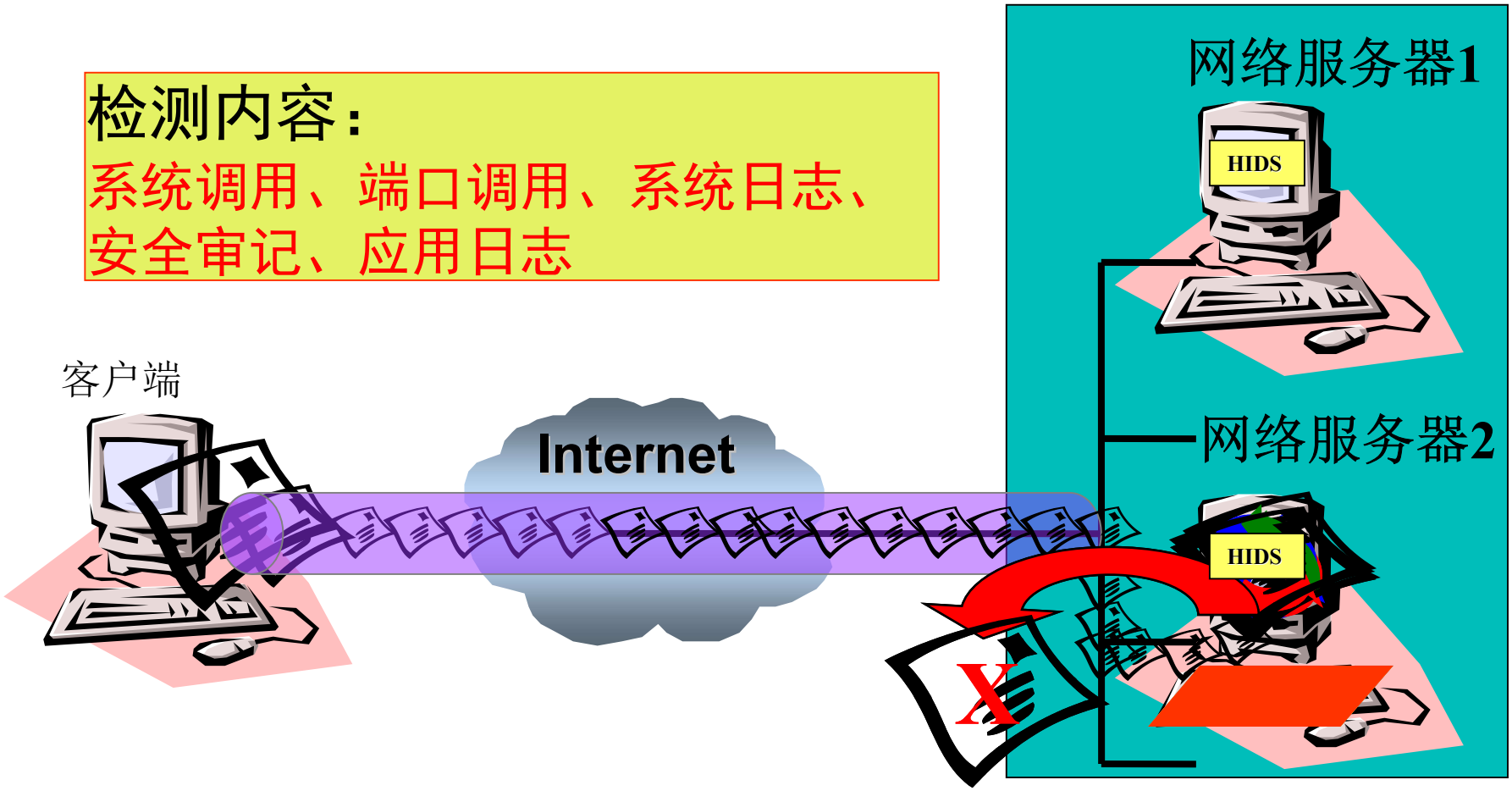
HIDS


Customers
Partners
Branch Office
Telecommuters
Hacker
Internet
Web Servers
Host-based IDS
Network
Desktops
Servers
Host-based IDS

基于主机入侵检测系统工作原理

检测内容：

系统调用、端口调用、系统日志、安全审记、应用日志



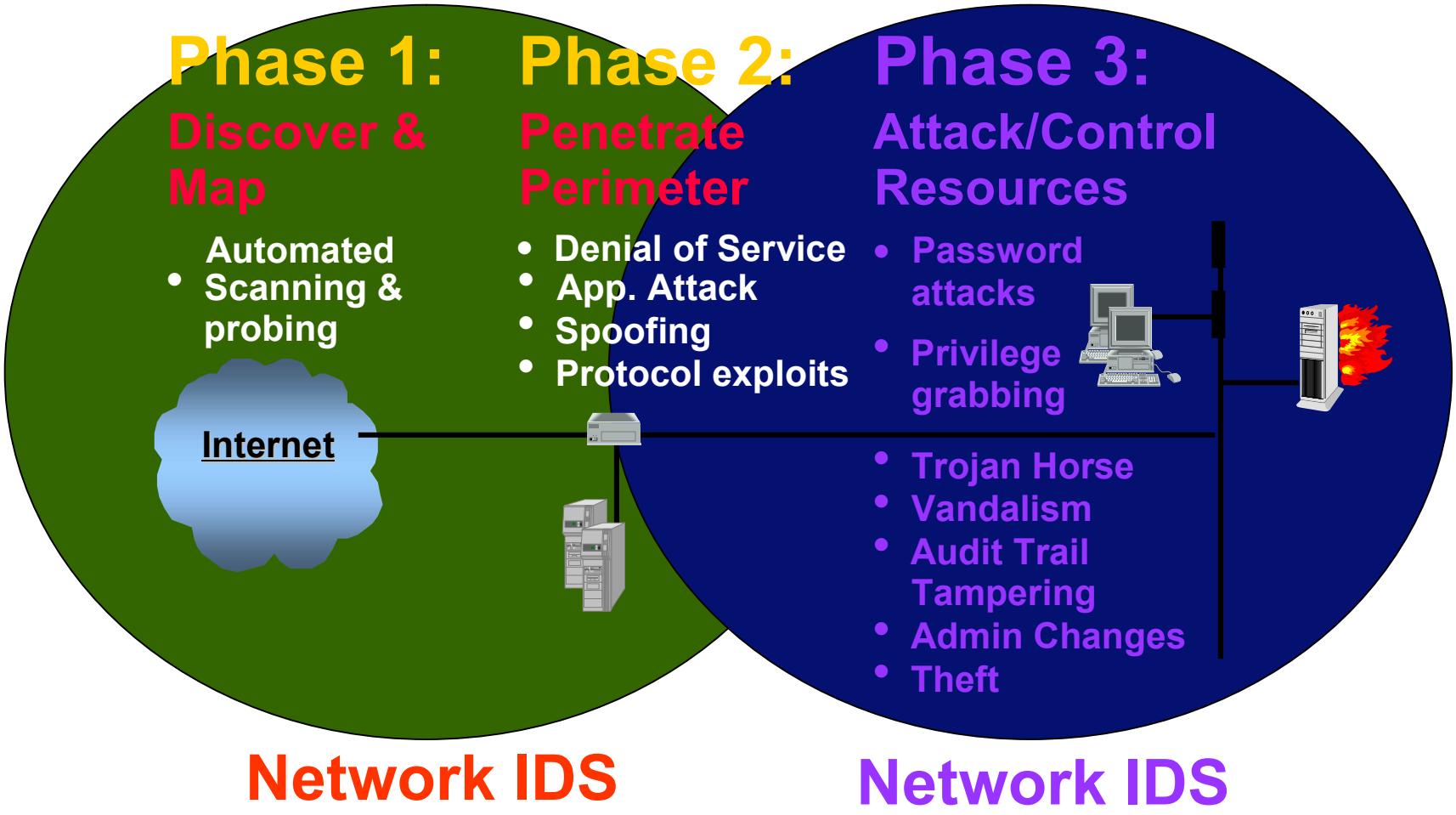
HIDS

- 监视与分析主机的审计记录
- 可以不运行在监控主机上
- 能否及时采集到审计记录
- 如何保护作为攻击目标主机审计子系统

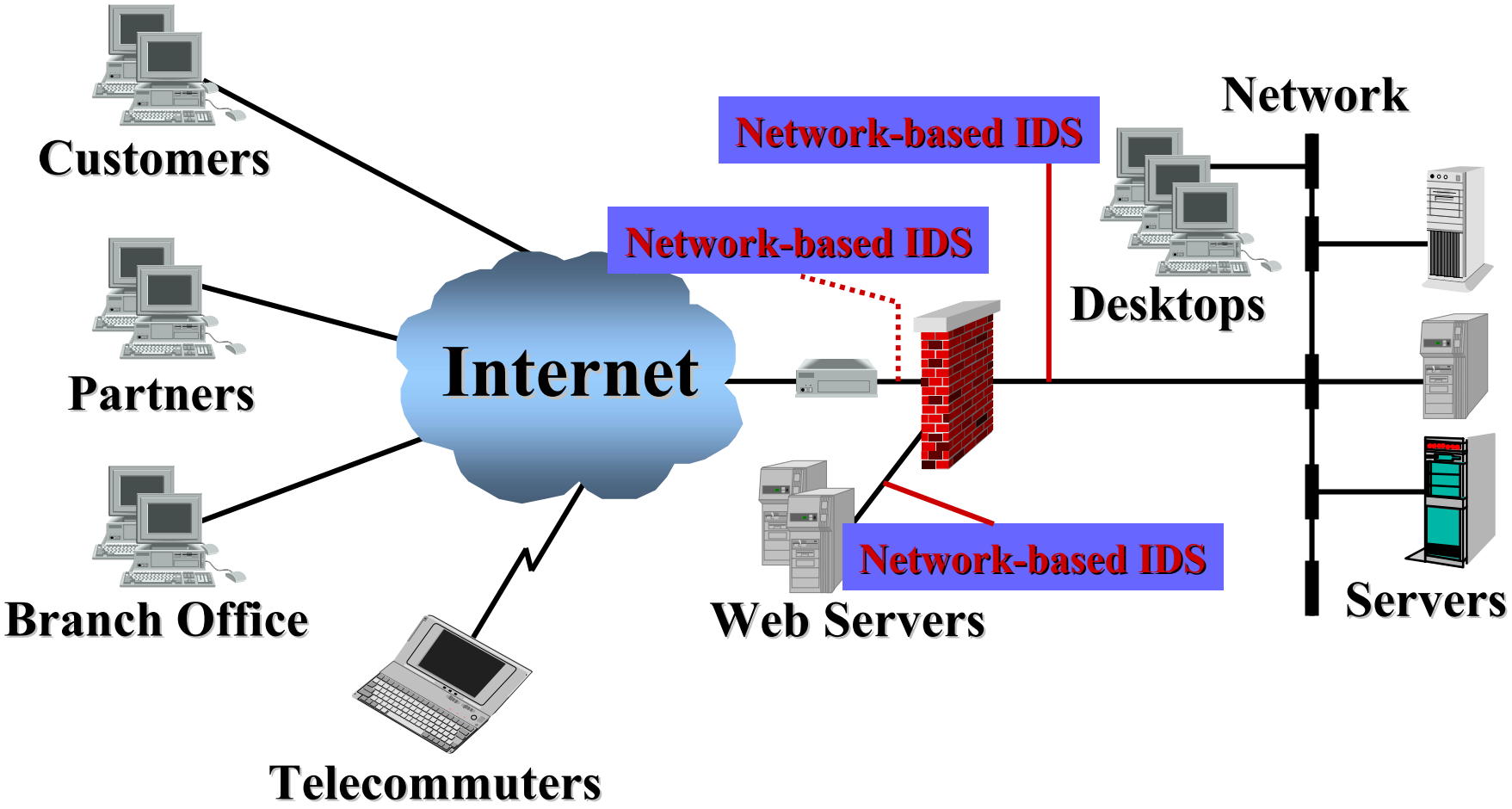
NIDS

- 在共享网段上对通信数据进行侦听采集数据
- 主机资源消耗少
- 提供对网络通用的保护
- 如何适应高速网络环境
- 非共享网络上如何采集数据

❖ 黑客入侵的过程和阶段

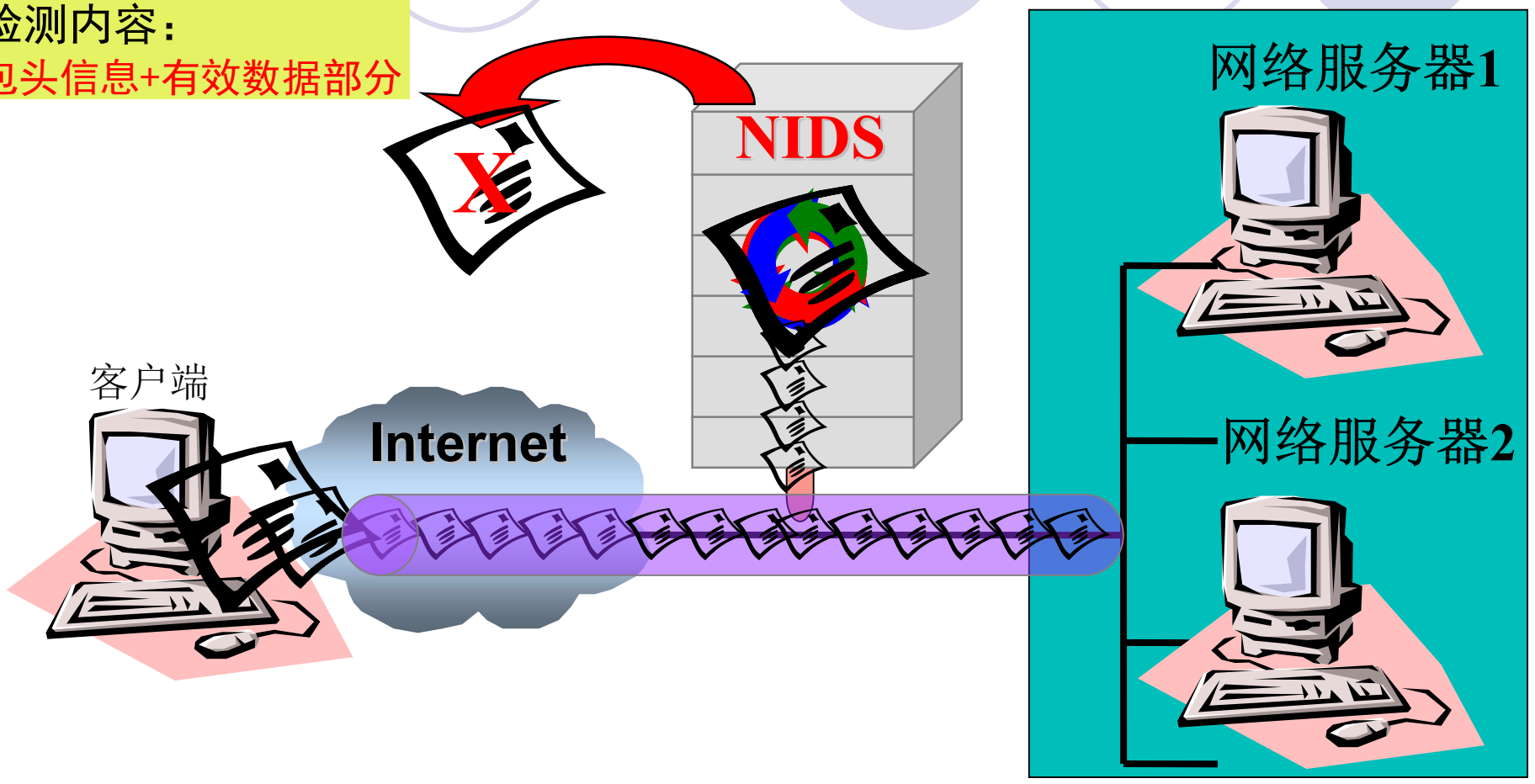

Phase 1:
Discover & Map
Automated Scanning & probing
Phase 2:
Penetrate Perimeter
Denial of Service
App. Attack
Spoofing
Protocol exploits
Phase 3:
Attack/Control Resources
Password attacks
Privilege grabbing
Trojan Horse
Vandalism
Audit Trail Tampering
Admin Changes
Theft
Internet
Network IDS
Network IDS

NIDS


Customers
Partners
Branch Office
Telecommuters
Internet
Network-based IDS
Network-based IDS
Network-based IDS
Web Servers
Network
Desktops
Servers

基于网络入侵检测系统工作原理

检测内容：
包头信息+有效数据部分

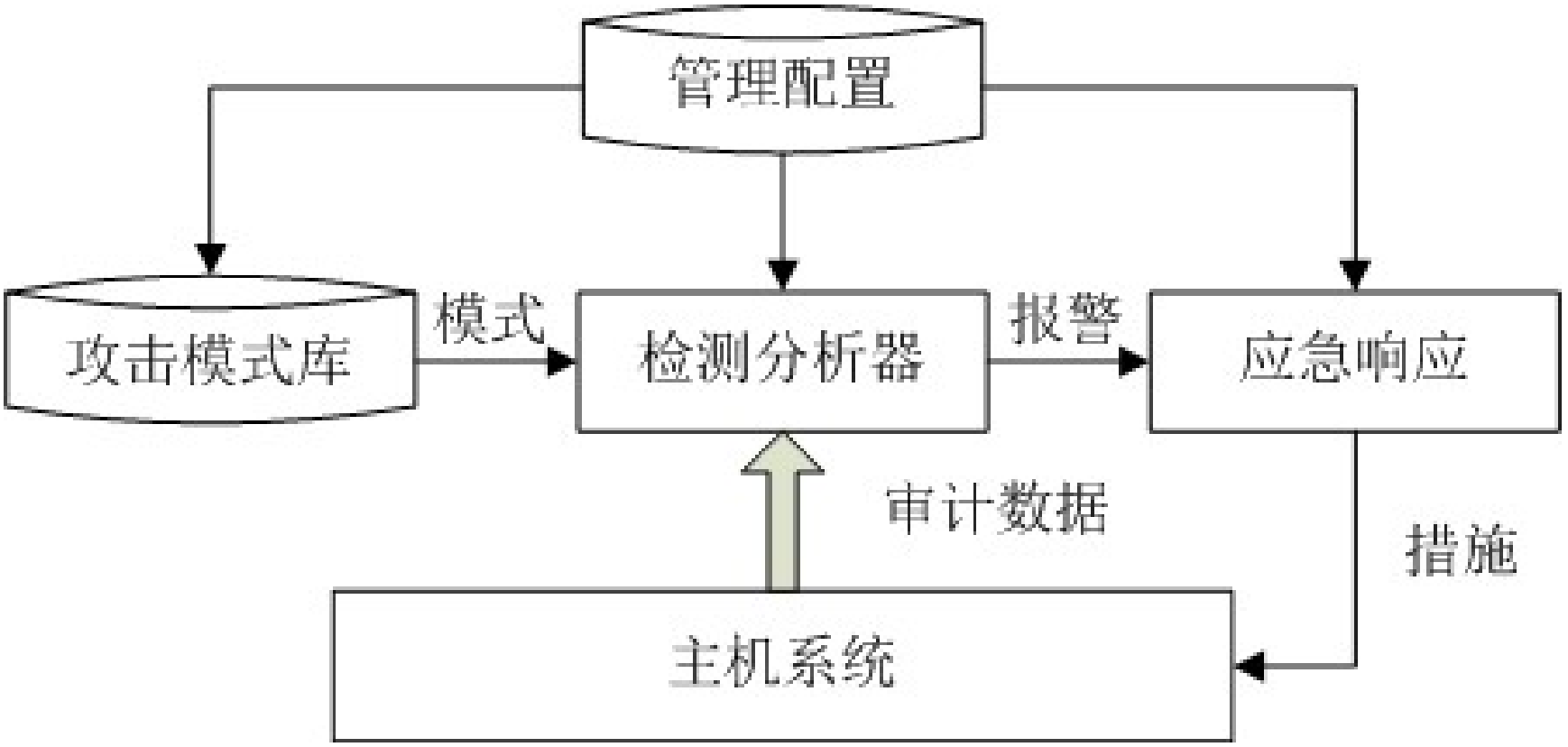


数据包=包头信息+有效数据部分

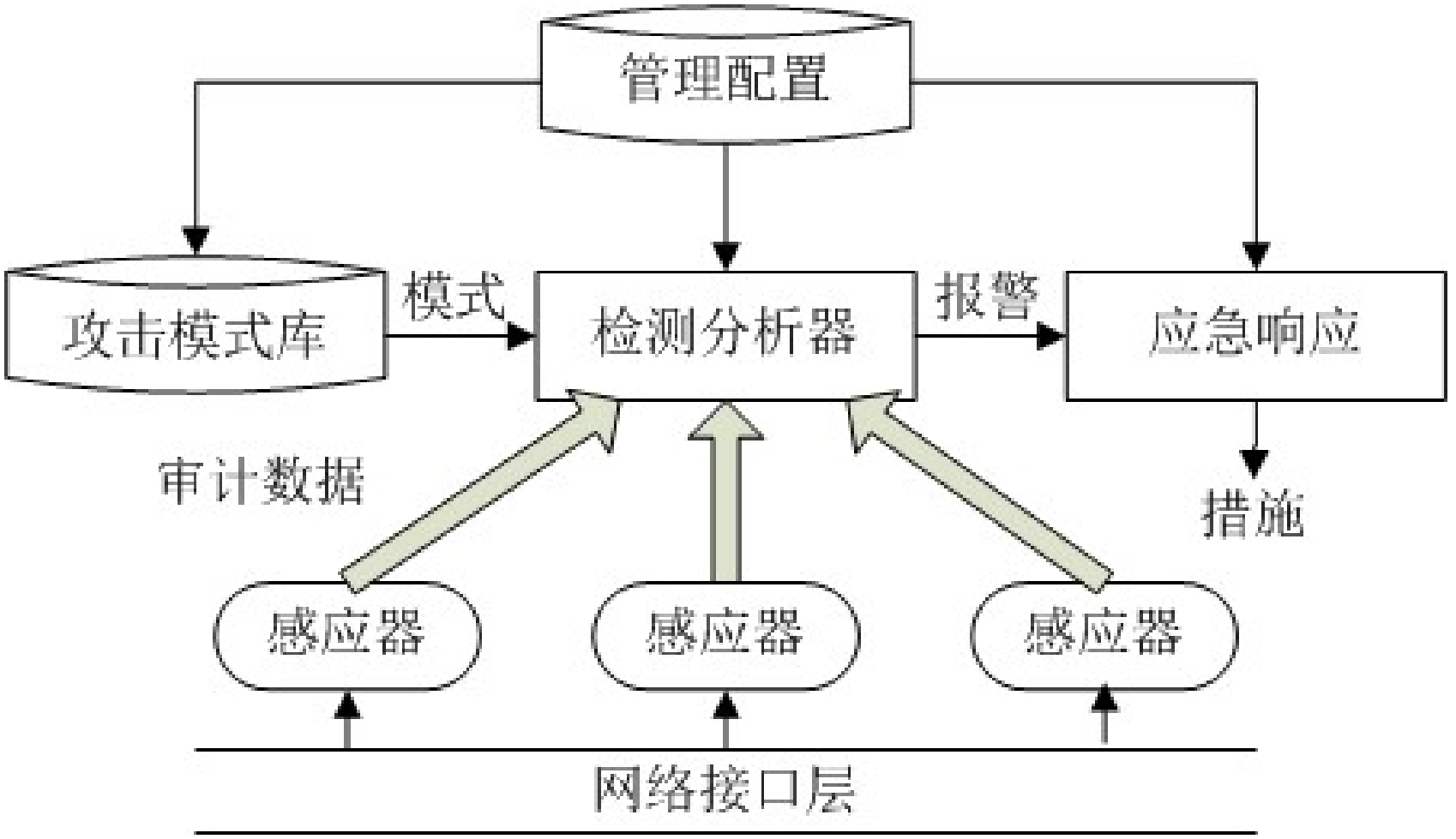
两类IDS监测软件

- 网络IDS
  - 侦测速度快
  - 隐蔽性好
  - 视野更宽
  - 较少的监测器
  - 占资源少
- 主机IDS
  - 视野集中
  - 易于用户自定义
  - 保护更加周密
  - 对网络流量不敏感

主机型入侵检测系统



网络型入侵检测系统

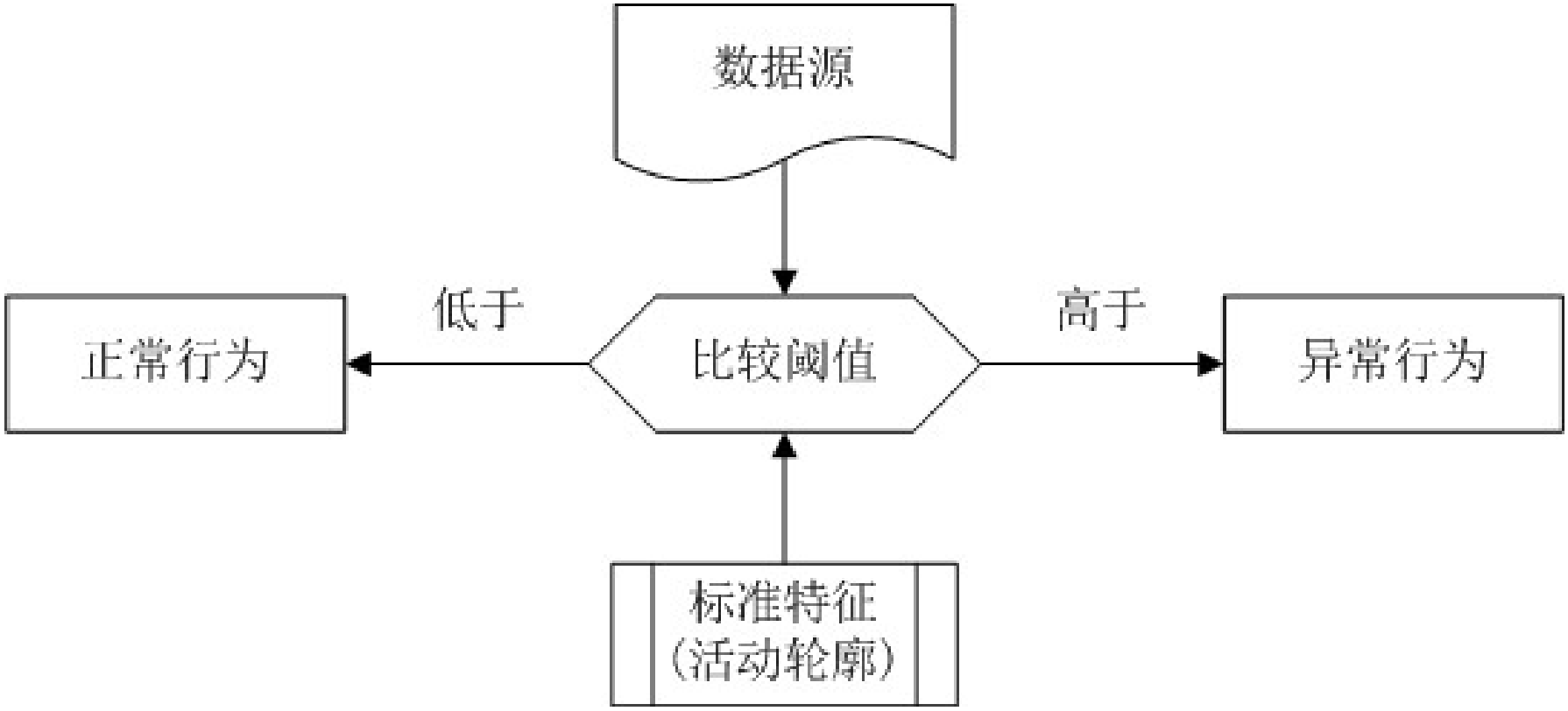


以检测技术为分类标准（分类2）

- 异常检测模型（**Anomaly Detection):**首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵。

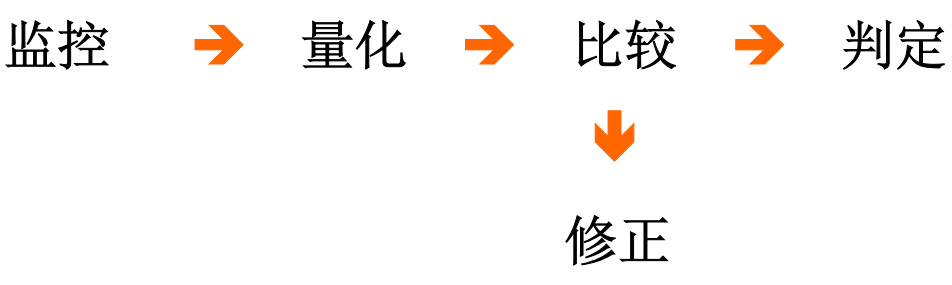
- 误用检测模型（**Misuse Detection)**：收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵 。

基于异常检测（Anomaly Detection）的IDS



基于异常检测（Anomaly Detection）的IDS

1. 前提：入侵是异常活动的子集
2. 用户轮廓(Profile)：通常定义为各种行为参数及其阀值的集合，用于描述正常行为范围
3. 过程

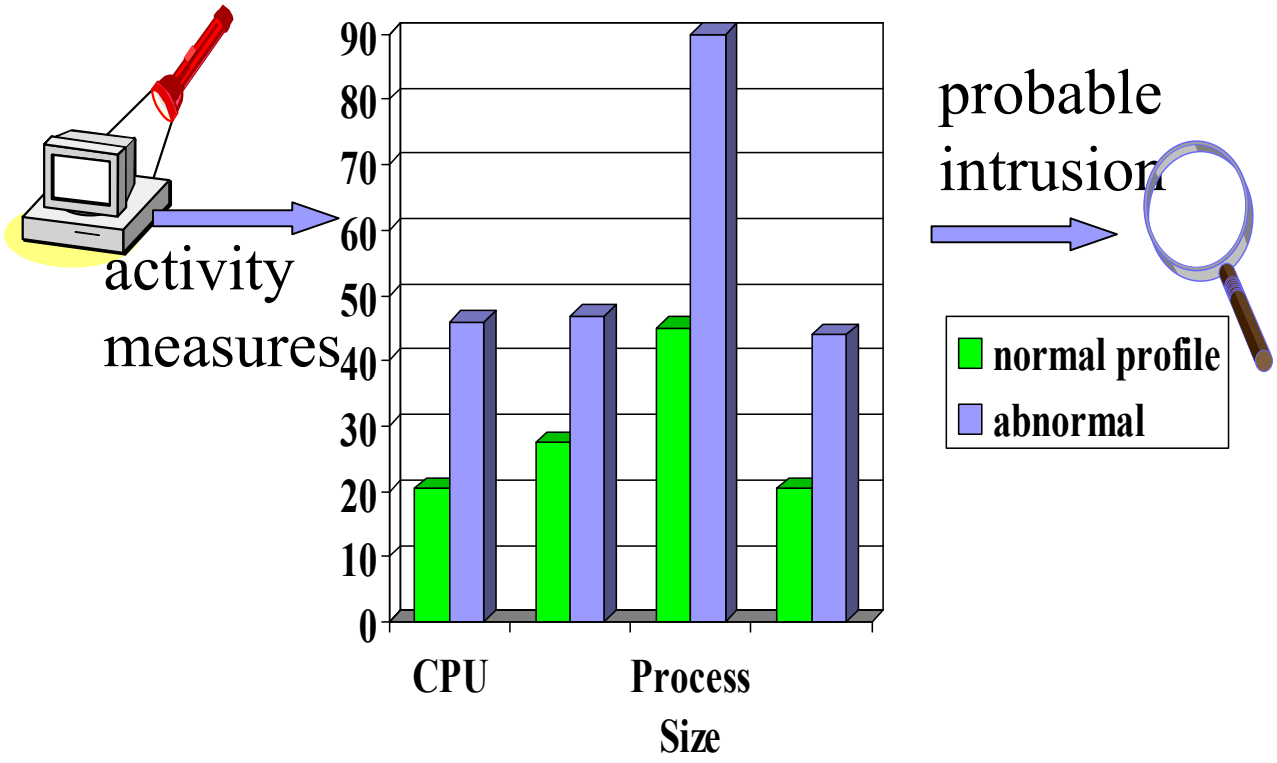


4. 指标:漏报率低,误报率高

异常检测特点

- 异常检测系统的效率取决于用户轮廓的完备性和监控的频率
- 因为不需要对每种入侵行为进行定义，因此能有效检测未知的入侵
- 系统能针对用户行为的改变进行自我调整和优化，但随着检测模型的逐步精确，异常检测会消耗更多的系统资源

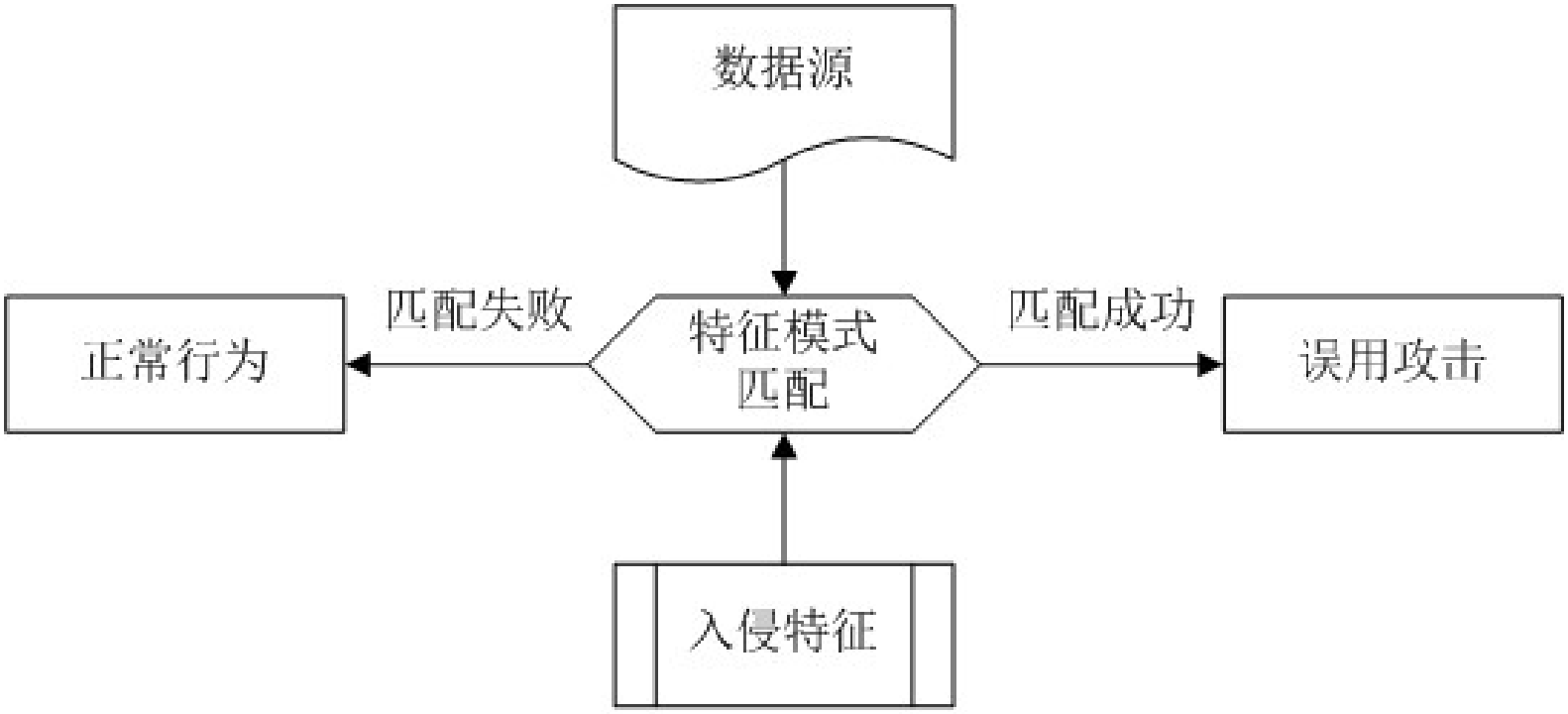
Anomaly Detection



Relatively high false positive rate -
anomalies can just be new normal activities.

以检测技术为分类标准（分类2）

- 基于误用检测（Misuse Detection）的IDS



误用检测模型

以检测技术为分类标准（分类2）

1. 前提：所有的入侵行为都有可被检测到的特征
2. 攻击特征库：当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵
3. 过程

   监控 → 特征提取 → 匹配 → 判定

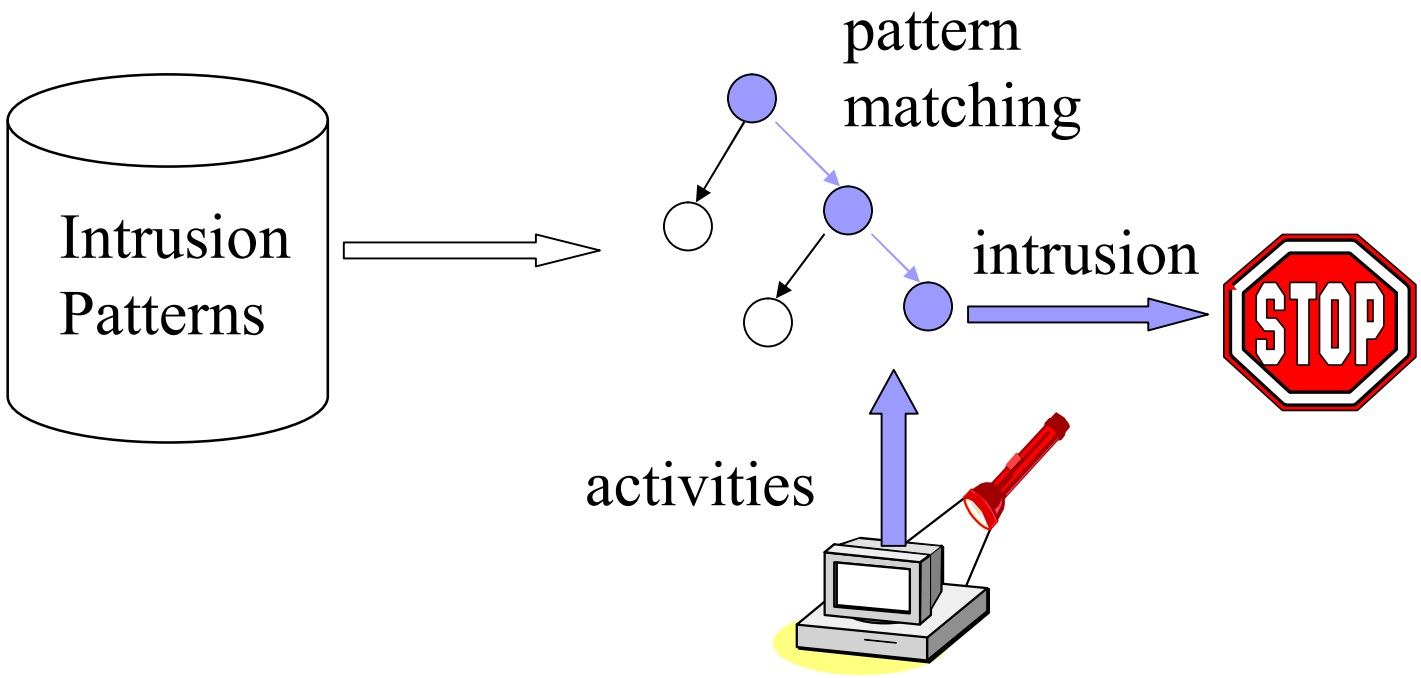
4. 指标:误报低、漏报高

误用检测模型

- 如果入侵特征与正常的用户行能匹配，则系统会发生误报；
- 如果没有特征能与某种新的攻击行为匹配，则系统会发生漏报

- 特点：
  - 采用特征匹配，滥用模式能明显降低错报率，但漏报率随之增加。
  - 攻击特征的细微变化，会使得滥用检测无能为力

Misuse Detection



Example: ***if*** (src_ip == dst_ip) ***then*** “land attack”

Can’t detect new attacks

入侵检测的分类（3）

- 按系统各模块的运行方式
  - 集中式：系统的各个模块包括数据的收集分析集中在一台主机上运行。
  - 分布式：系统的各个模块分布在不同的计算机和设备上。

入侵检测的分类（4）

- 根据时效性
  - 脱机分析：行为发生后，对产生的数据进行分析
  - 联机分析：在数据产生的同时或者发生改变时进行分析

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。
- 入侵检测的主要技术方法
  - 误用检测
  - 异常检测
  - 诱骗
  - 响应
  - 等

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
- ……

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。

异常检测技术

- 统计分析
- 预测模型
- 系统调用监测
- 基于人工智能的异常检测技术
- ……

入侵诱骗技术

- 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。

响应技术

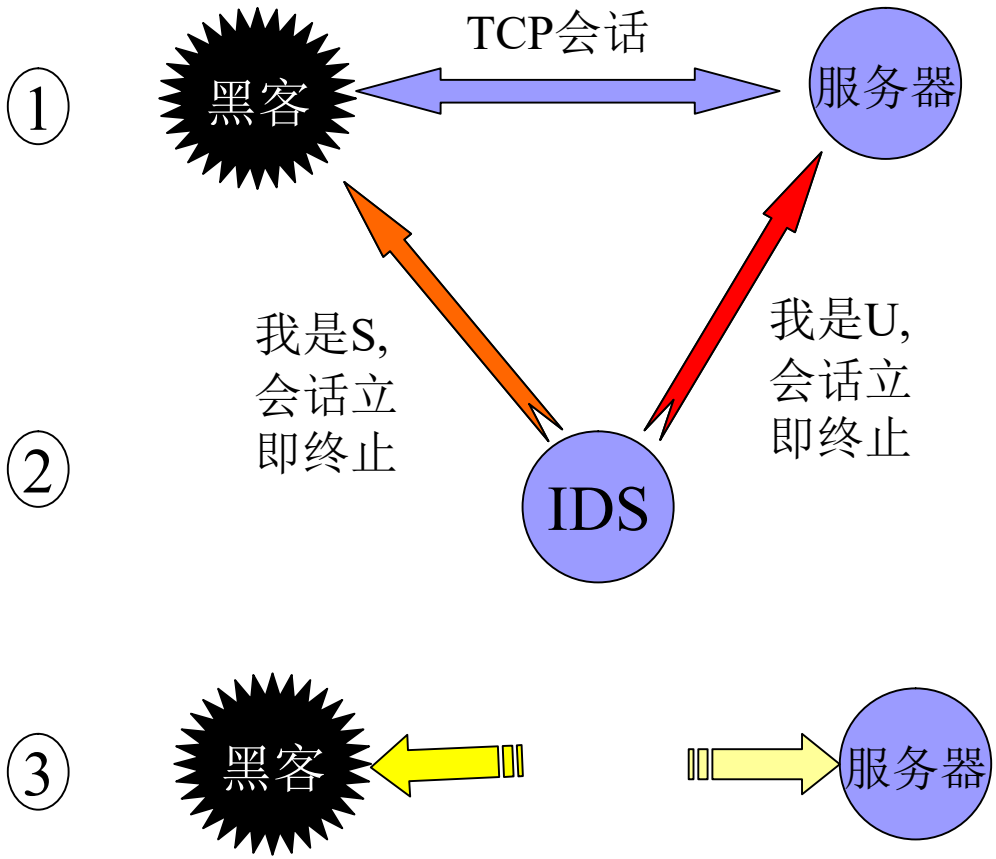
- 入侵检测系统的响应技术可以分为主动响应和被动响应。
  - 主动响应是系统自动阻断攻击过程或以其他方式影响攻击过程；
  - 被动响应是报告和记录发生的事件。

响应策略

- 弹出窗口报警
- E-mail通知
- 切断TCP连接
- 执行自定义程序
- 与其他安全产品交互
  - Firewall
  - SNMP Trap

NIDS技术—响应方法（1）

切断连接



NIDS技术—响应方法（2）

- 显示与记录
  - 记录到文件或者数据库中
  - 显示到控制台屏幕
  - 利用网络或者其他设备显示到呼机或者手机
- 发送电子邮件
  - 给指定的管理员发送电子邮件，附带警报部分内容

NIDS技术—响应方法（3）

- 配置防火墙
  - 向防火墙提交进行恶意攻击的IP地址及其他相关信息
  - 防火墙动态添加规则，禁止该地址通过或者访问特定主机的服务。
- 发送SNMP Trap信息
  - 向SNMP Trap代理发送保护警报信息的事件，以便通知基于snmp的管理平台。

7.4 网络防御的新技术

- **7.4.1 VLAN技术**
  - VLAN（Virtual Local Area Network）的中文名为“虚拟局域网”
  - 1999年IEEE颁布的802.1Q协议标准草案
    - 定义为：虚拟局域网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。

VLAN的划分方式

- 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

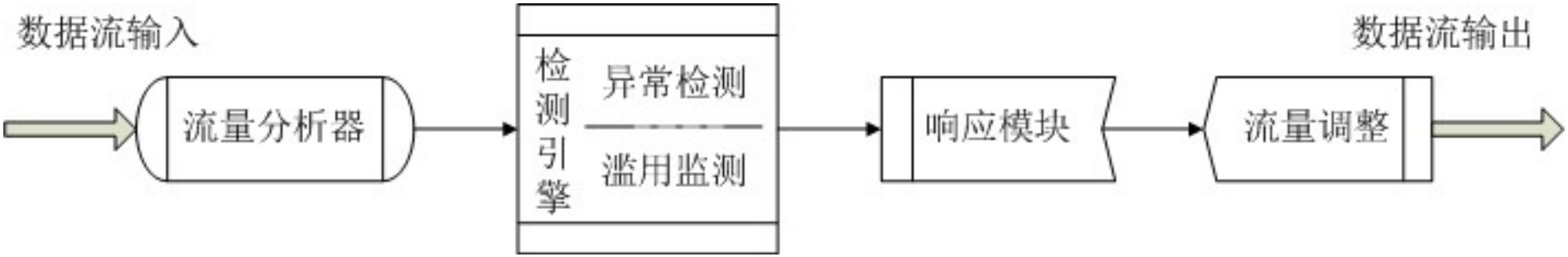
- 广播风暴防范
  - 广播风暴的控制：物理网络分段和VLAN的逻辑分段，同一VLAN处于相同的广播域，通过VLAN的划分可以有效地阻隔网络广播，缩小广播域，控制广播风暴。
- 信息隔离
  - 同一个VLAN内的计算机之间便可以直接通信，不同VLAN间的通信则要通过路由器进行路由选择、转发，这样就能隔离基于广播的信息，防止非法访问，
- 控制IP地址盗用
  - 该VLAN内任何一台计算机的IP地址都必须在分配给该VLAN的IP地址范围内，否则将无法通过路由器的审核，也就不能进行通信，

VLAN存在的问题

- 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，所以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。

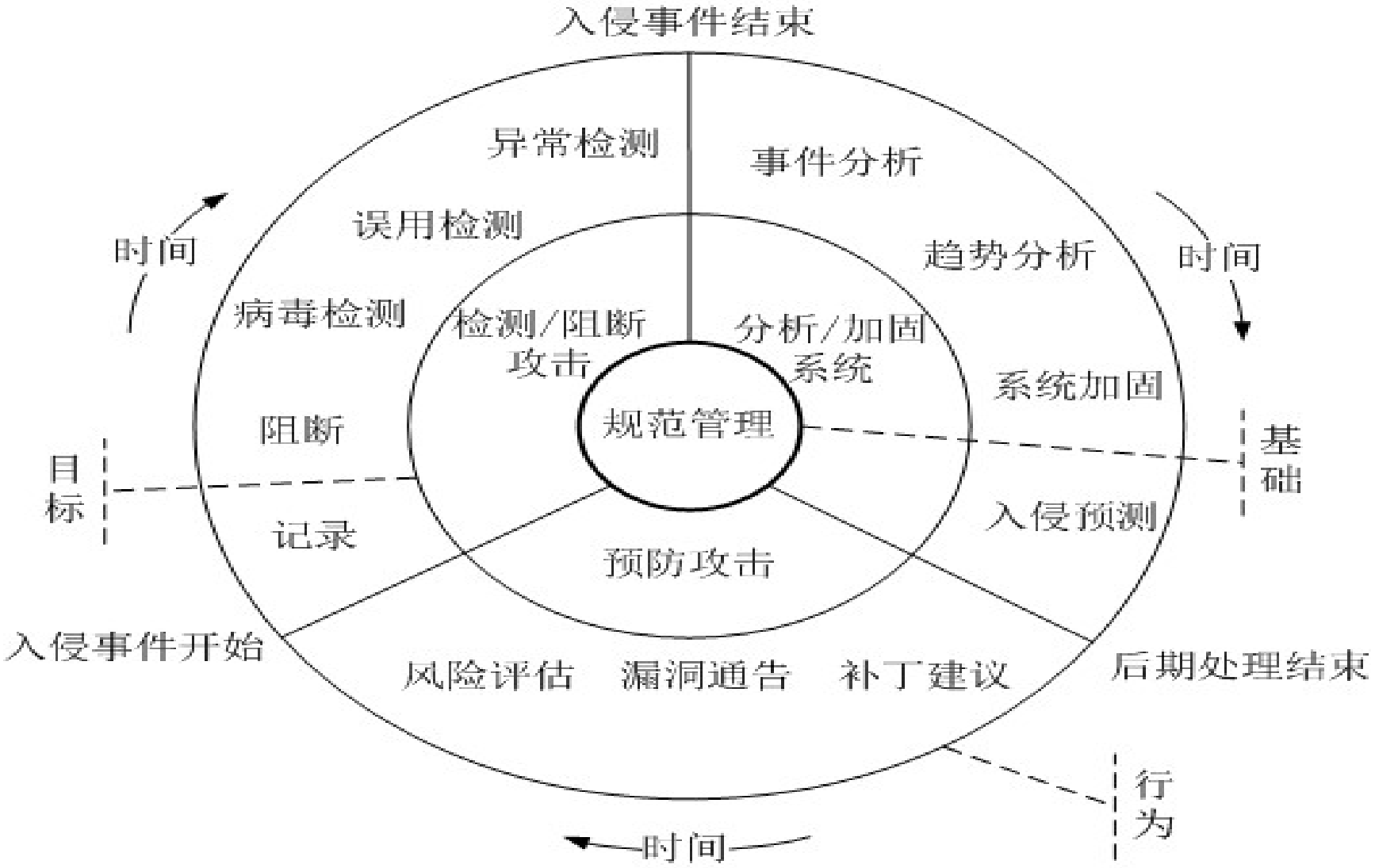
7.4.2 IPS与IMS

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



- IPS与IDS相比具有许多先天优势。
  - 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）



IMS模型示意图

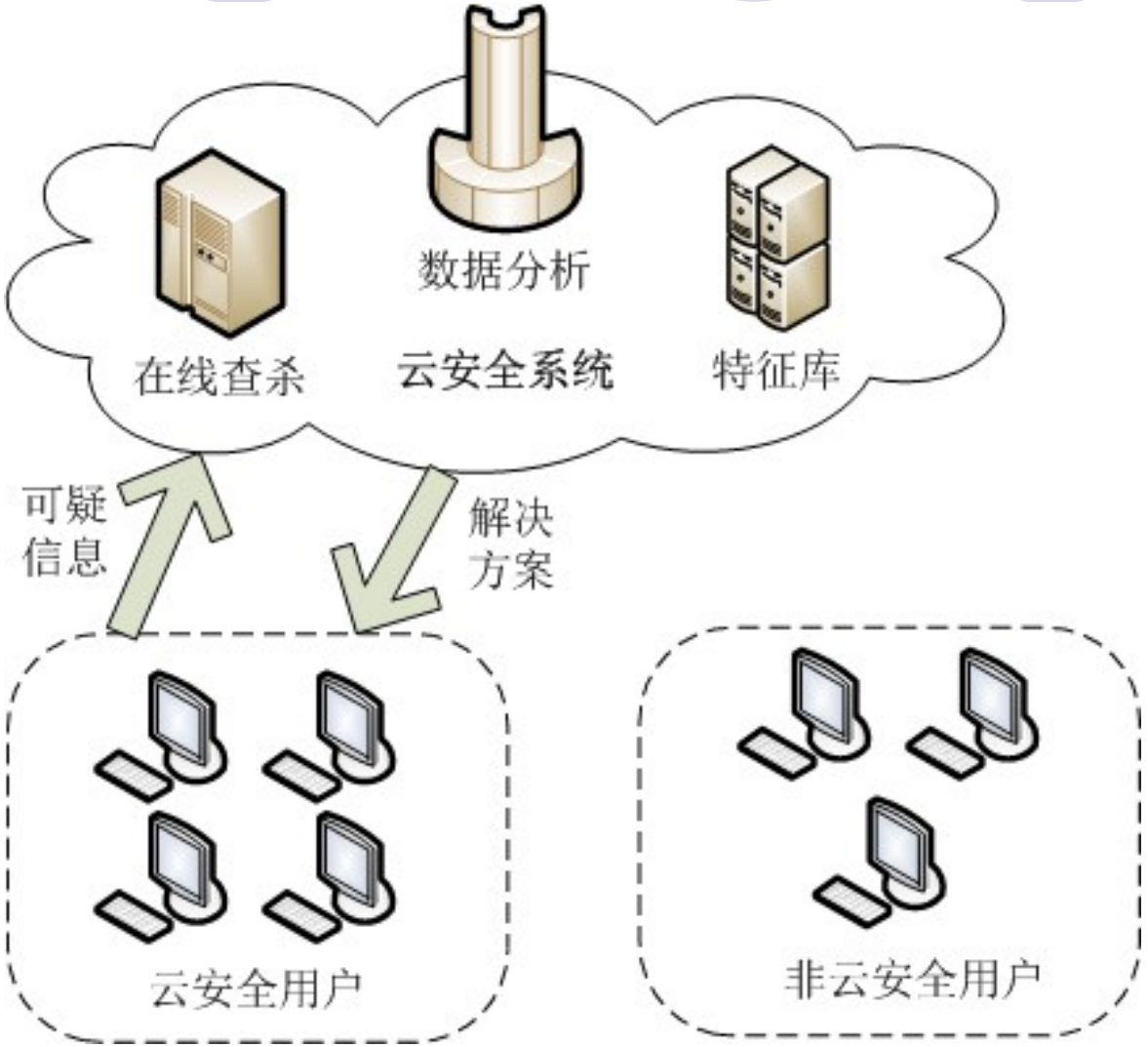
7.4.3 云安全

- “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。

7.4.3 云安全

- 云安全
  - 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”。

云安全示意图



“云安全”存在的问题

- 需要海量的客户端
- 需要专业的反病毒技术和经验
- 需要大量的资金和技术投入
- 开放的系统

Any question?