第三章 网络安全基础
第二节 网络安全防护技术

主讲人：李建华 张全海
网络空间安全技术研究院

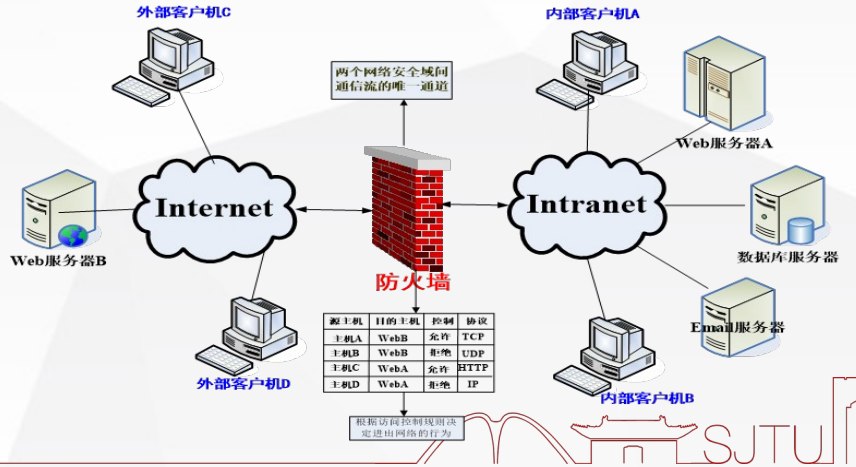
2024 年 11 月

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

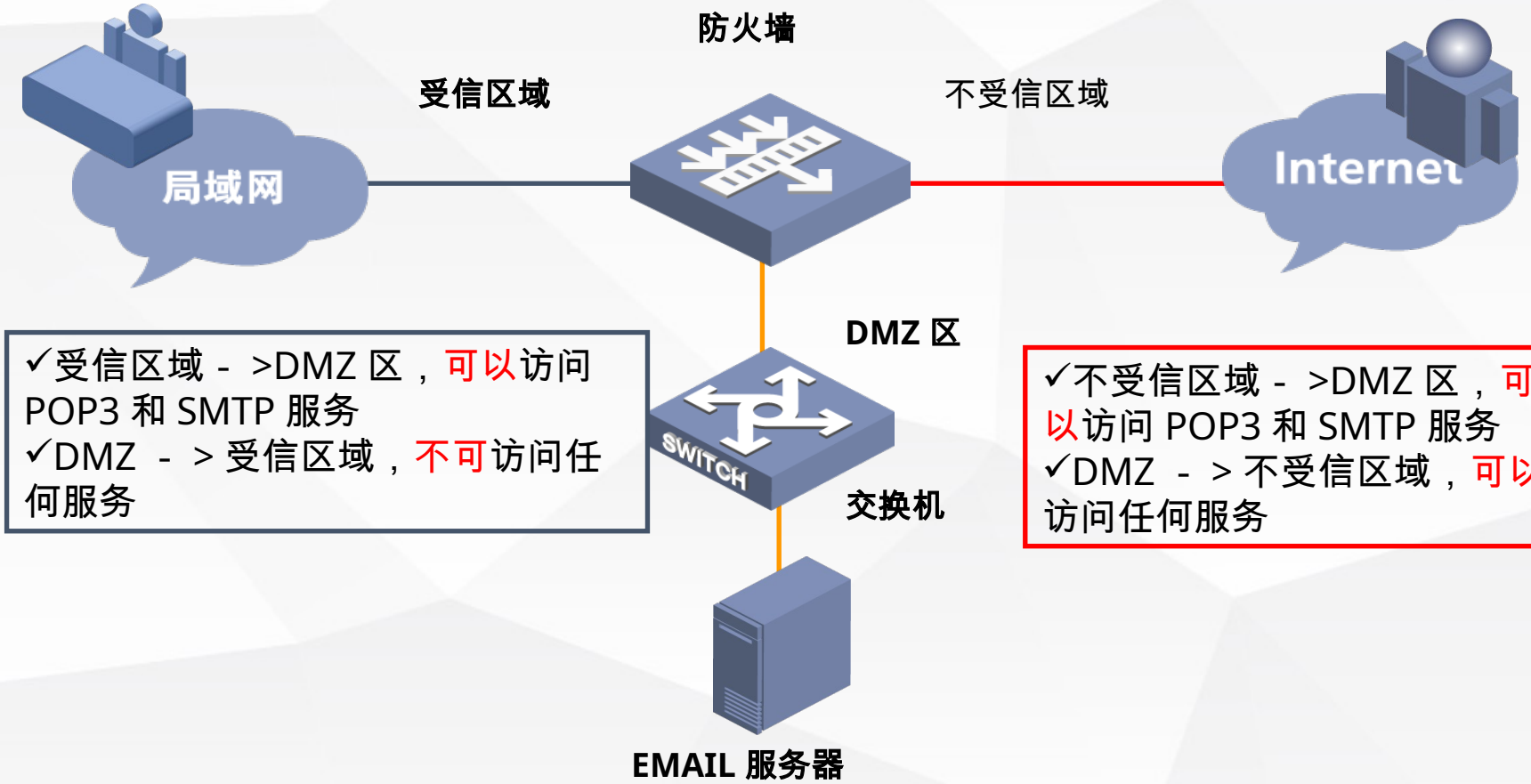
防火墙概述

- 防火墙 (Firewall) 是在两个网络之间执行访问控制策略的一个或一组安全系统。防火墙是由软件和硬件组成的系统集合，是实现网络安全策略的有效工具之一，它处于安全的网络和不安全的网络之间，属于边界防护设备。
- 防火墙通过设置访问控制规则，对进出网络边界的**数据流进行过滤。**
- 防火墙是建立在内外网络边界上的**过滤封锁机制**，是一种用于保护本地系统或者网络不受基于网络的安全威胁的有效方法。
  - 内部网络（受信网络）被认为是安全和可信赖的，而外部网络（通常是 Internet, 非受信网络）被认为是不安全和不可信赖的。
  - 非军事化区（ DMZ ）：为了配置管理方便，内网中需要向外提供服务的服务器往往放在一个单独的网段，这个网段便是非军事化区。



防火墙概述

不受信区域和受信区域之间不能互访



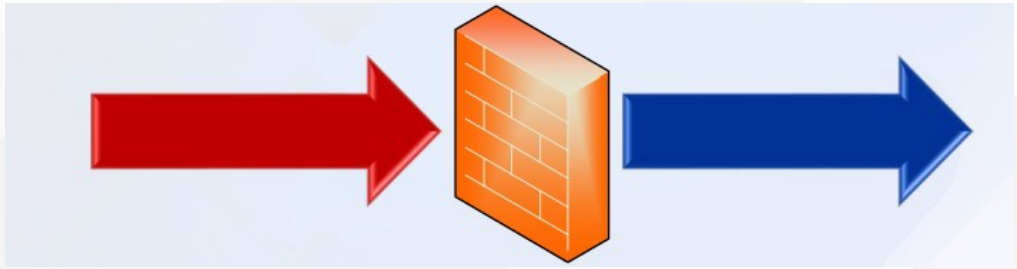
✓受信区域 - >DMZ 区，可以访问 POP3 和 SMTP 服务
✓DMZ - > 受信区域，不可访问任何服务

✓不受信区域 - >DMZ 区，可以访问 POP3 和 SMTP 服务
✓DMZ - > 不受信区域，可以访问任何服务

防火墙概述

根据安全策略，对防火墙的以下三种要求必须得到满足：

1. 所有进出网络数据流都必须经过防火墙
2. 只允许经授权的数据流通过防火墙
3. 防火墙自身对入侵免疫，即确保自身安全



防火墙提供的四种控制机制

- **服务控制**：确定了可访问的 Internet 服务类型，这种控制是双向的，如防火墙可以以 IP 地址和 TCP 端口号为基础对流量进行过滤；可以提供委托代理软件对收到的每一个服务请求进行解释之后才允许通过；

- **方向控制**：确定特定的服务请求可以发起和通过的方向，即允许通过防火墙进入或离开；

- **用户控制**：控制特定用户对某些服务的访问权限；

- **行为控制**：控制特定服务的应用方式，如控制外部用户只能访问只能访问本地 web 服务器的部分信息；

防火墙的发展

第一代防火墙

- 1985-1988 ， Cisco 的 IOS 软件公司
  - ◆包过滤（ Packet filter ）防火墙

第二代防火墙

- 1989-1990 ， AT&T 贝尔实验室
  - ◆电路级网关防火墙

第三代防火墙

- Purdue University ； AT&T 贝尔实验室
  - ◆应用级网关防火墙

第四代防火墙

- 1991-1994 ， USC 信息科学院，以色列的 CheckPoint 公司
  - ◆动态包（ Dynamic packet filter ）过滤防火墙 状态检测（ Stateful inspection ）防火墙

第五代防火墙

- 1996 年，内核代理结构
  - ◆NAI 公司，自适应代理（ Adaptive proxy ）防火墙

第六代防火墙

- 2004 年， IDC 提出统一威胁管理 UTM 概念
  - ◆将杀毒、 IDS 和防火墙安全设备划归 UTM

防火墙分类及设计结构

防火墙分类

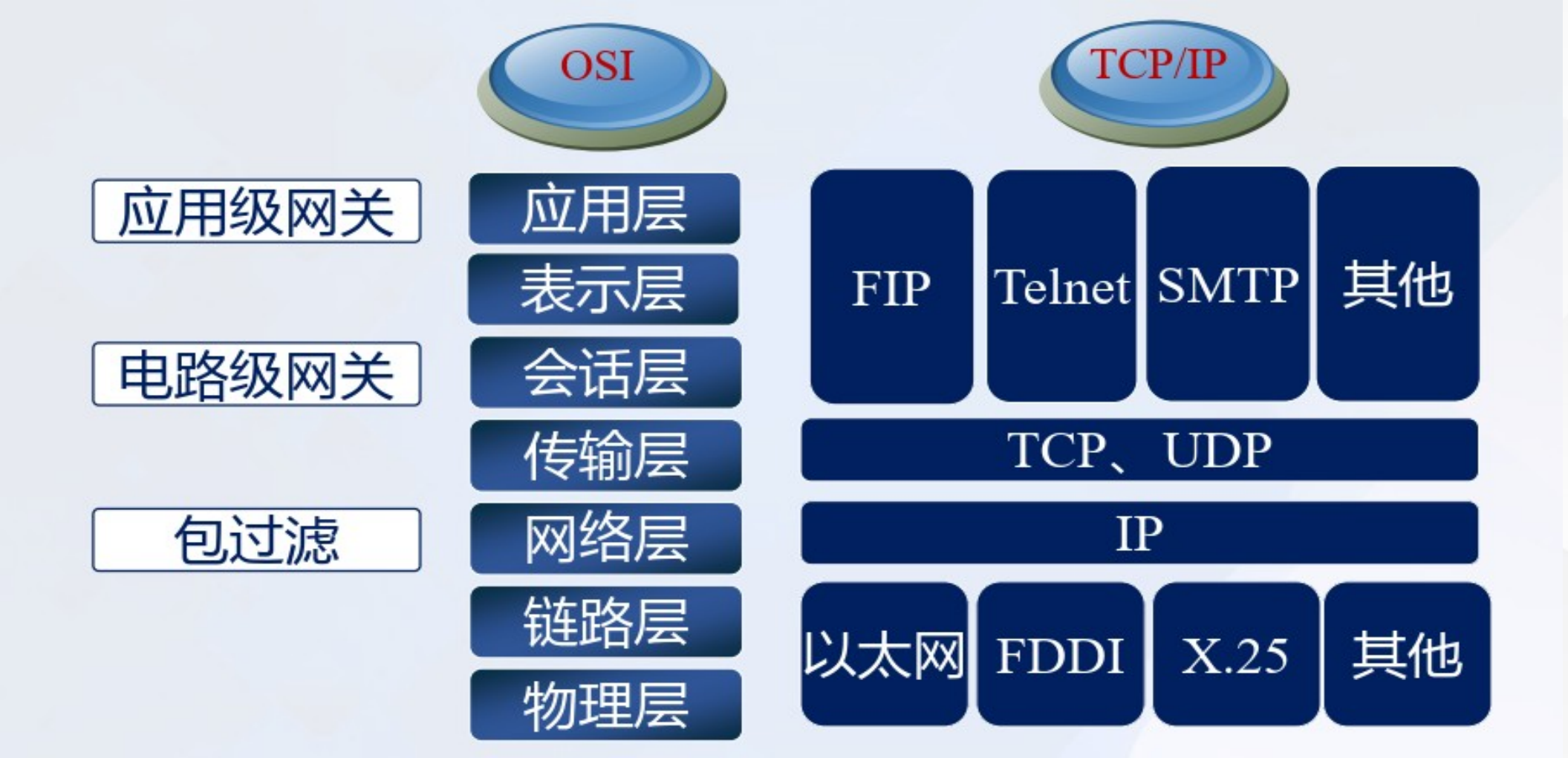
- 包过滤防火墙
- 电路级网关防火墙
- 应用级网关防火墙

防火墙设计结构

- 静态包过滤
- 动态包过滤
- 电路级网关
- 应用层网关
- 状态检查包过滤
- 切换代理
- 空气隙（物理隔离）

OSI 模型与防火墙类型的关系

防火墙工作于 OSI 模型的层次越高，能提供的安全保护等级就越高



OSI 模型与防火墙类型的关系

IP 数据包结构

IP 头部数据段

TCP 头部数据段

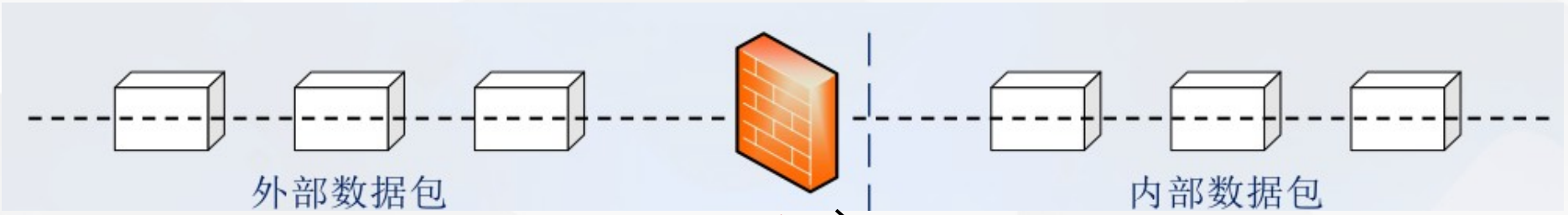
防火墙通常建立在 **TCP/IP 模型**基础上，OSI 模型与 TCP/IP 模型之间**并不存在一一对应**的关系

防火墙能和不能


网络安全的屏障
强化网络安全策略
对网络存取和访问进行监控审计
防止内部信息的外泄
安全策略检查
防火墙能做什么
防火墙不能做什么
不能防范内部人员的攻击
不能防范绕过它的连接
不能防备全新的威胁
不能防范恶意程序和病毒（数据驱动式攻击）

防火墙原理

静态包过滤防火墙



接收每个数据包，应用规则，如果规则不存在，则应用默认规则

防火墙接收到从外部网络到达防火墙的数据包，对数据包过滤。

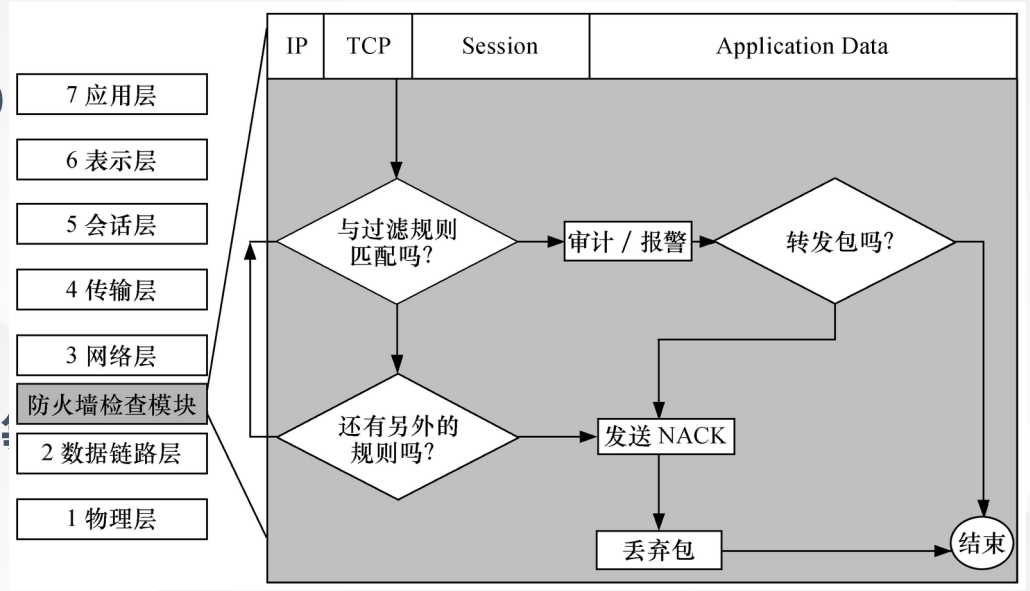
对数据包施加过滤规则，对数据包 IP 头和传输字段内容进行检查。

如果没有规则与数据包头信息匹配，则对数据包施加默认规则。

防火墙原理

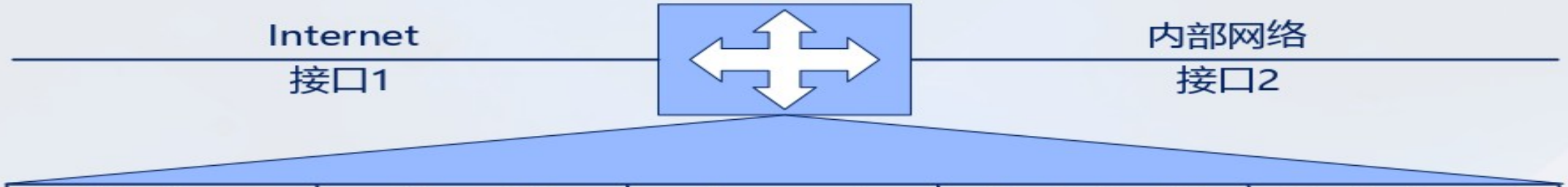
静态包过滤防火墙

- **包过滤 (Packet Filtering) 技术是防火墙利用对数据包的分析能力，在网络层中根据数据包中包头信息有选择地实施允许通过或阻断。**
- 判断依据有 (只考虑 IP 包) ：
  - 数据包**封装协议类型**： TCP 、 UDP 、 ICMP 、 IGMP 等
  - **源、目的 IP 地址**，数据包的 TCP/UDP 源、目的端口
  - **服务类型 (端口)** ： FTP （ 21 ）、 HTTP （ 80 ）、 D
    （ 53 ）等
  - IP 选项：源路由、记录路由等
  - TCP 选项： SYN 、 ACK 、 FIN 、 RST 等
  - 其它协议选项： ICMP ECHO 、 ICMP ECHO REPLY
  - **数据包流向**： in 或 out
  - **数据包流经网络接口**： eth0 、 eth1
  - 。 。 。 。 。 。



防火墙原理

静态包过滤防火墙



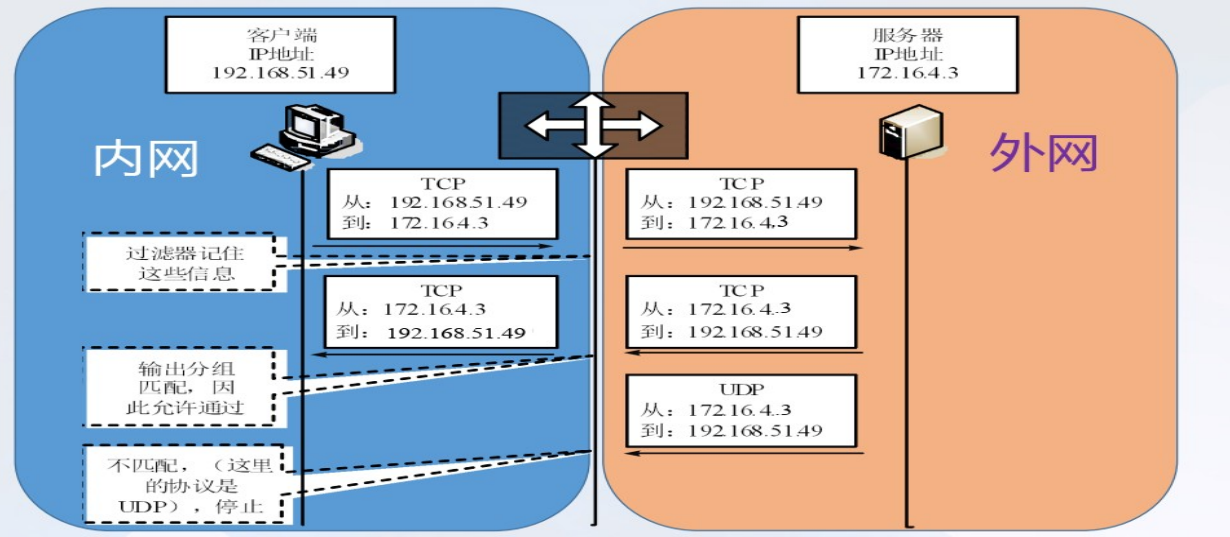
Interface	Source IP	Source port	Destination IP	Destination port
1	130.33.0.0	*	*	*
1	*	*	*	23
1	*	*	193.77.21.9	*
2	*	*	*	80

- 拒绝来自 130.33.0.0 的数据包，这是一种保守策略。
- 拒绝来自外部网络的 Telnet 服务（端口号为 23 ）的数据包。
- 拒绝试图访问内网主机 193.77.21.9 的数据包。
- 禁止 HTTP 服务（端口号为 80 ）的数据包通过防火墙。

动态包过滤防火墙

- 与普通包过滤防火墙相似，**大部分工作于网络层**。有些安全性高的动态包过滤防火墙，则**工作于传输层**。
- 动态包过滤防火墙的**不同点**：对外出数据包进行**身份记录**，便于下次让具有相同连接的数据包通过。
- 动态包过滤防火墙需要**对已建连接和规则表进行动态维护**，因此是动态的和有状态的。

实现动态包过滤器有**两种主要**的方式：
1、**实时地改变**普通包过滤器的**规则集**
2、采用类似**电路级网关**的方式**转发数据包**



电路级网关

它的作用就像一台中继计算机，用于在两个连接之间来回地复制数据；它也可以记录和缓存数据

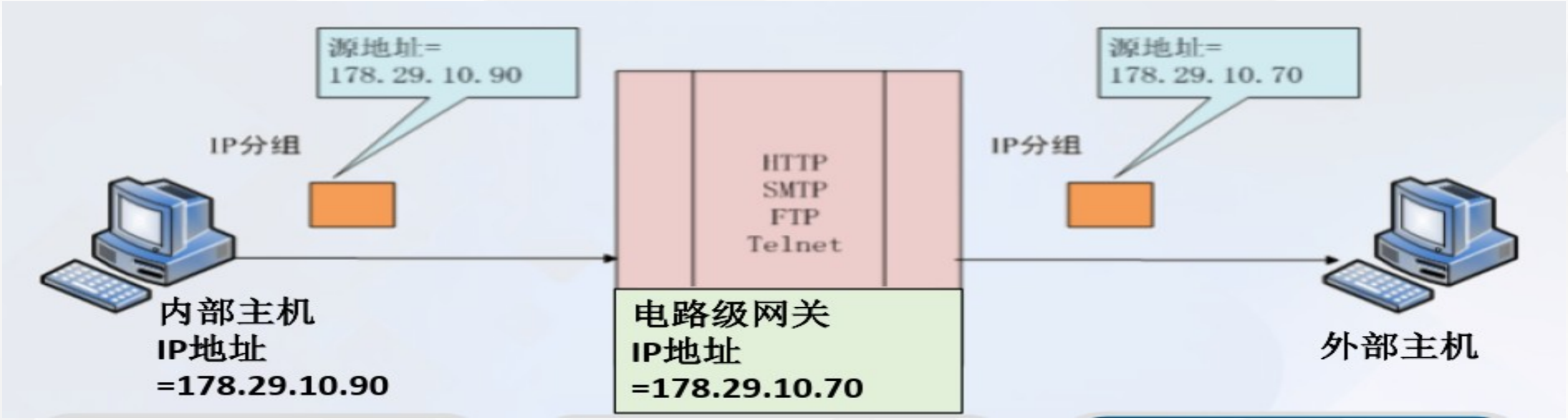
采用 C/S 结构，网关充当了服务器的角色作为代理服务器，在 Internet 和内部主机之间过滤和转发数据包

它工作于会话层，IP 数据包不会实现端到端流动；在有些实现方案中，电路连接可自动完成

- 电路级网关：被称为线路级网关，它工作在会话层，通常作为应用代理服务器的一部分，在应用代理类型的防火墙中实现，在两个主机首次建立 TCP 连接时创立一个电子屏障。
- 电路级网关不允许端到端 TCP 直接连接，相反电路级网关充当中介，接收外来请求，转发请求。
  - 它监视两主机建立连接时的握手信息，如通过在 TCP 3 次握手建立连接的过程中，SYN、ACK 等标志和序列号等是否合乎逻辑，判定该会话请求是否合法。
  - 一旦会话连接有效后网关在客户和服务器间中转数据。
- 电路级网关的防火墙的安全性比较高，但它仍不能检查应用层的数据包以消除应用层攻击的威胁。

防火墙原理

电路级网关



在转发一个数据包之前，首先将数据包的 IP 头和 TCP 头与由管理员定义的规则表相比较。

在内部连接和外部连接之间来回拷贝字节，并不进行任何附加的包处理或过滤

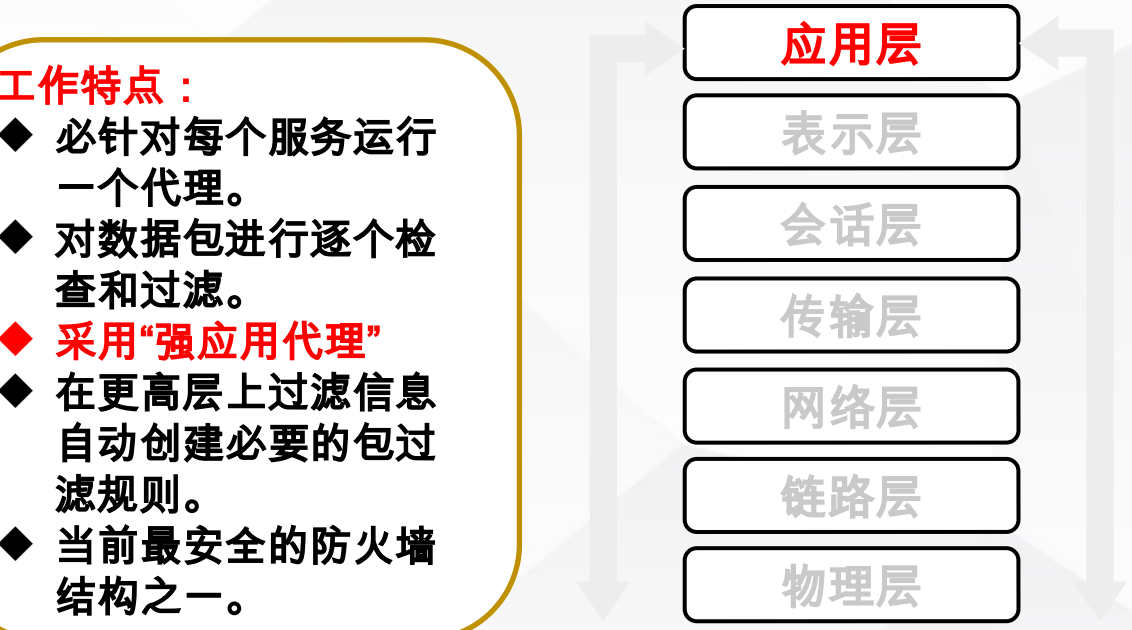
电路级网关在其自身与远程主机之间建立一个新连接，这一切对内网中用户都是完全透明的。

防火墙原理

应用层网关

工作特点：

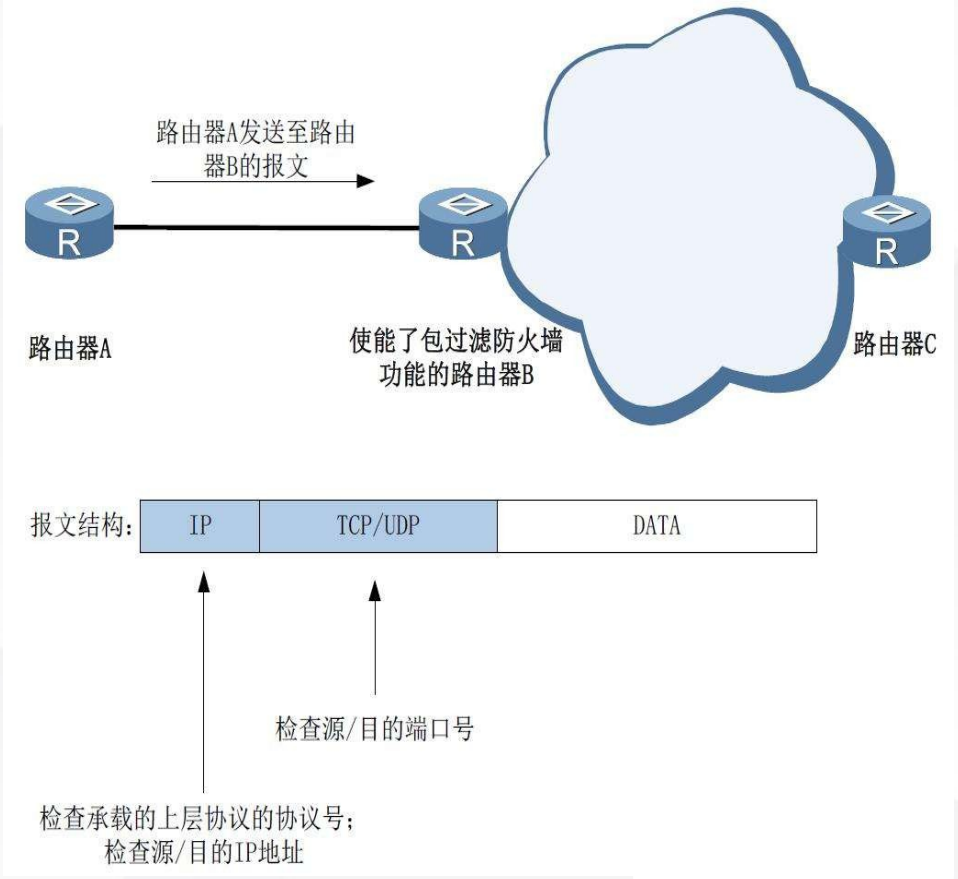
- 必针对每个服务运行一个代理。
- 对数据包进行逐个检查和过滤。
- 采用“强应用代理”
- 在更高层上过滤信息自动创建必要的包过滤规则。
- 当前最安全的防火墙结构之一。



- 代理对整个数据包进行检查，因此能在应用层上对数据包进行过滤。
- 应用代理与电路级网关有两个重要区别：
  - ✓ 代理是针对应用的。
  - ✓ 代理对整个数据包进行检查，因此能在 OSI 模型的应用层上对数据包进行过滤。

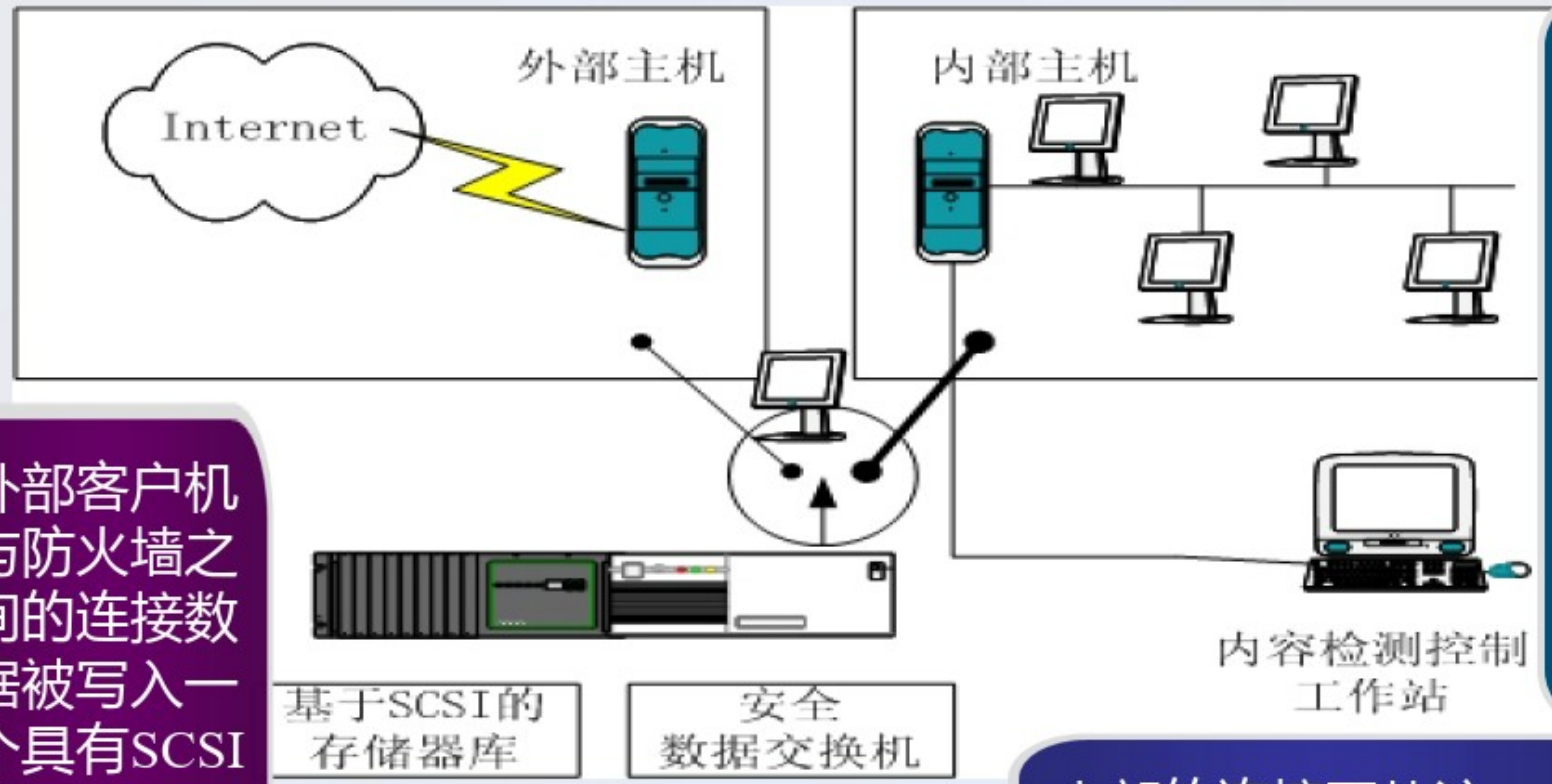
状态检测包过滤

- 状态检测是一种相当于 4.5 层的过滤技术，建立状态连接表，并将进出网络的数据当成一个个的会话，利用状态表跟踪每一个会话状态。它不限于包过滤防火墙的 3/4 层的过滤，又不需要应用层网关防火墙的 5 层过滤，既提供了比包过滤防火墙更高的安全性和更灵活的处理，也避免了应用层网关防火墙带来的速度降低的问题。
- 要实现状态检测，最重要的是实现连接的跟踪功能，实现多个包的关联分析。能够进一步分析主连接中的内容信息，识别出所协商的子连接的端口而在防火墙上将其动态打开，连接结束时自动关闭。
- 通过建立一个出站的 TCP 连接目录加强了 TCP 数据流的监测规则，对网络通信的各层实施监测分析，提取相关的通信和状态信息，并在动态连接表中进行状态及上下文信息的存储和更新



防火墙原理

空气隙防火墙



外部客户机与防火墙之间的连接数据被写入一个具有SCSI接口的高速硬盘。

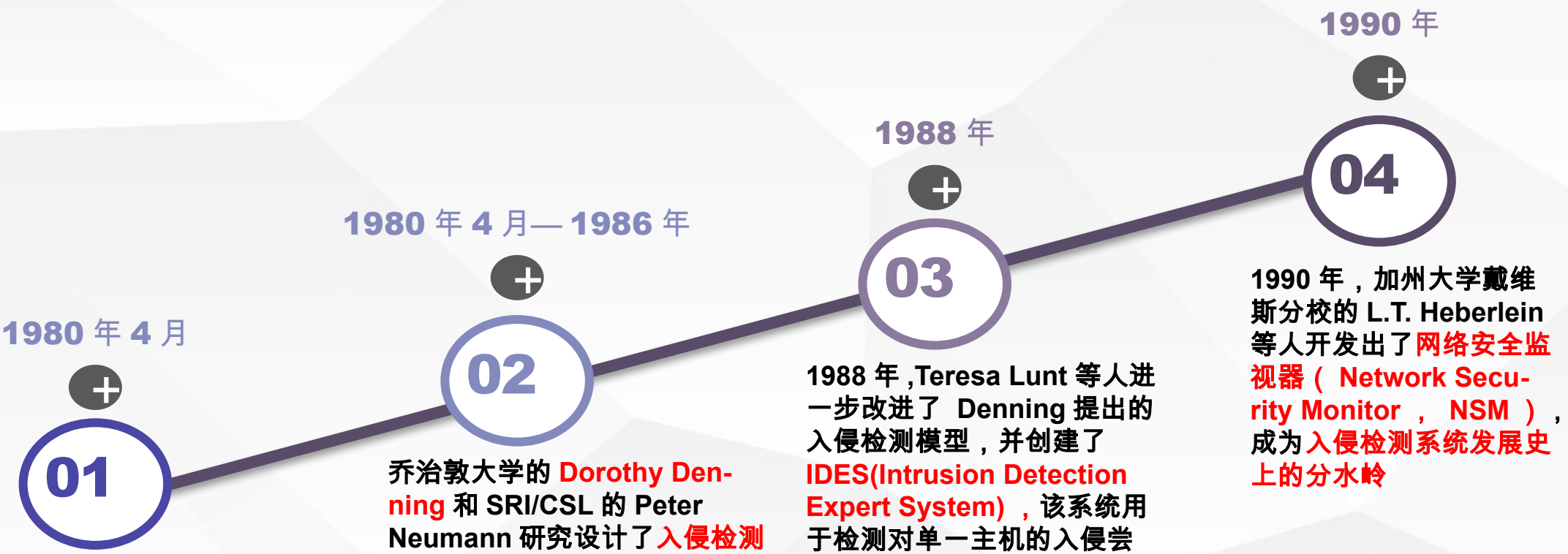
防火墙切断了客户机到服务器的直接连接，并且对硬盘数据的读/写操作都是独立进行的。

内部的连接再从该SCSI硬盘中读取数据。

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

目 录

入侵检测系统发展史


1980 年 4 月
01
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，将计算机系统威胁分类为外部渗透、内部渗透和不法行为以及提出了利用审计跟踪数据监视入侵活动的思想。
1980 年 4 月— 1986 年
02
乔治敦大学的 Dorothy Denning 和 SRI/CSL 的 Peter Neumann 研究设计了入侵检测专家系统。首次将入侵检测作为一种计算机系统安全的防御措施提出，建立了 Denning 模型
1988 年
03
1988 年 ,Teresa Lunt 等人进一步改进了 Denning 提出的入侵检测模型，并创建了 IDES(Intrusion Detection Expert System)，该系统用于检测对单一主机的入侵尝试，提出了与系统平台无关的实时检测思想
1990 年
04
1990 年，加州大学戴维斯分校的 L.T. Heberlein 等人开发出了网络安全监视器（ Network Security Monitor ， NSM ），成为入侵检测系统发展史上的分水岭

通用的入侵检测系统模型

入侵检测系统功能任务

- 系统和网络的日志文件
- 目录和文件中的异常改变
- 程序执行中的异常行为
- 物理形式的入侵信息

- 模式匹配
- 统计分析
- 完整性分析

- 主动响应
- 被动响应

信息收集

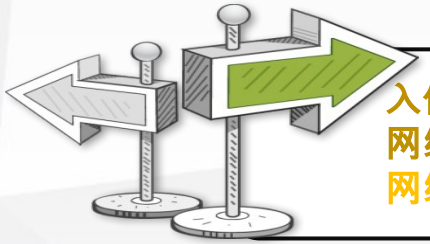
所收集的信息内容：用户在网络、系统、数据库及应用系统中活动的状态和行为。

信息分析

① 操作模型
② 方差
③ 多元模型
④ 马尔可夫过程模型
⑤ 时间序列分析

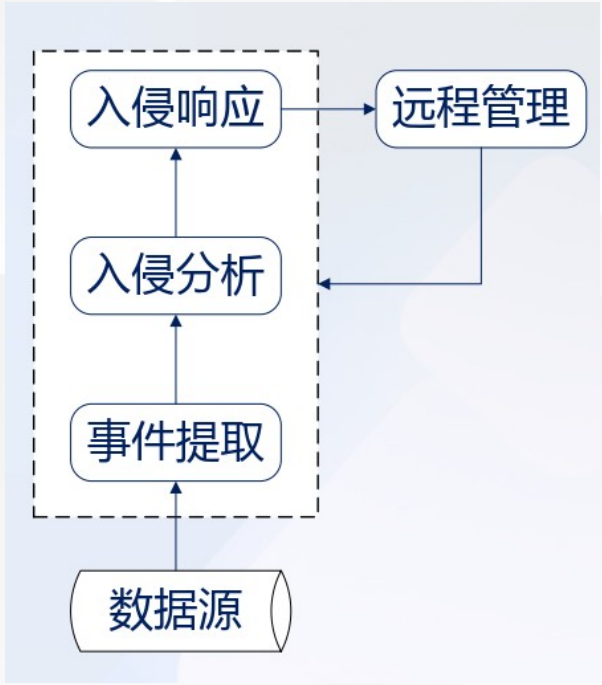
安全响应

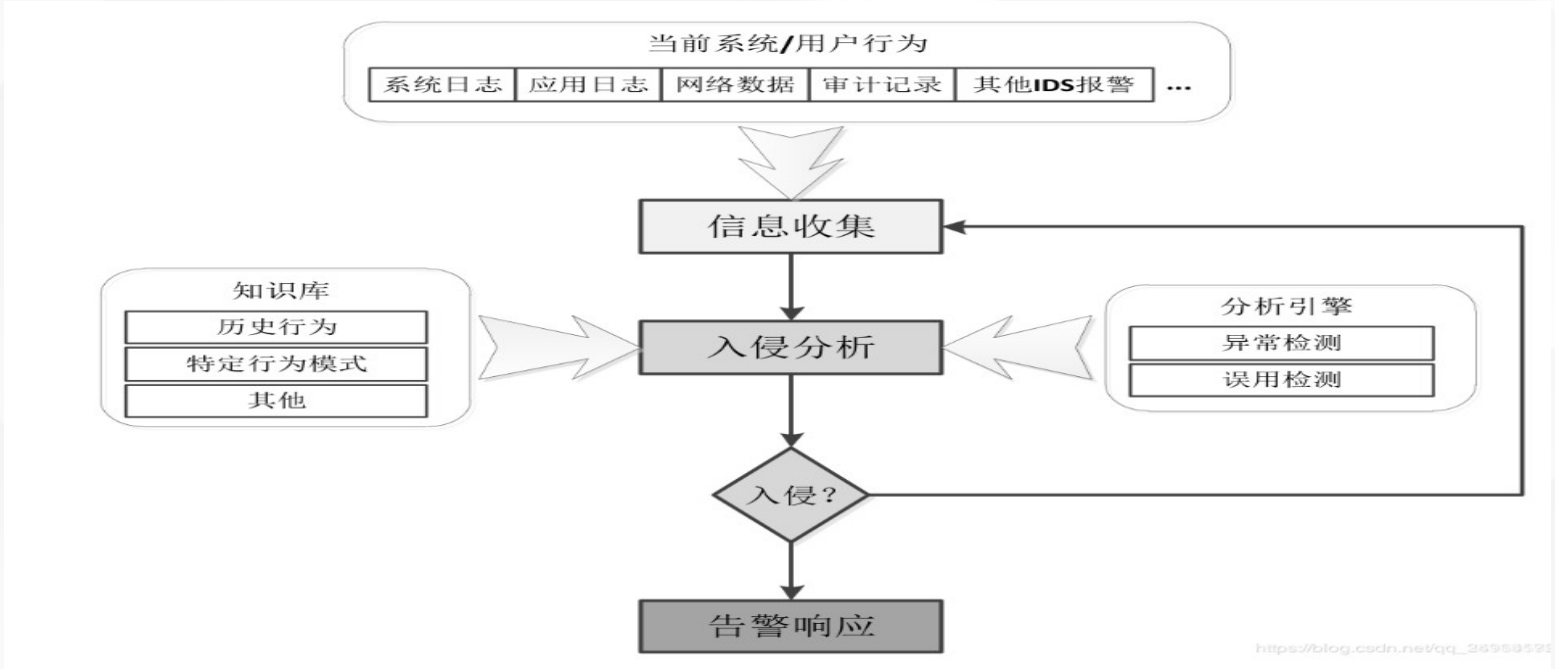
流行的响应方式：记录日志、实时显示、 E-mail 报警、 声音报警、 SNMP 报警、 实时 TCP 阻断、防火墙联动、 WinPop 显示、手机短信报警



入侵检测 (IDS：Intrusion Detection System) 是通过从计算机网络或系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击迹象的一种机制，基本上不具有访问控制的能力，单独使用不能起到保护网络的作用，也不能独立地防止任何一种攻击。

入侵检测系统结构





- **事件提取**：负责提取相关运行数据或记录，并对数据进行简单过滤。
- **入侵分析**：找出入侵痕迹，发现异常行为，分析入侵行为并定位入侵者。
- **入侵响应**：分析出入侵行为后被触发，根据入侵行为产生响应。
- **远程管理**：在一台管理站上实现统一的管理监控。

入侵检测系统分类

按照数据来源分类

- 基于网络的 IDS
- 基于主机的 IDS
- 分布式 IDS

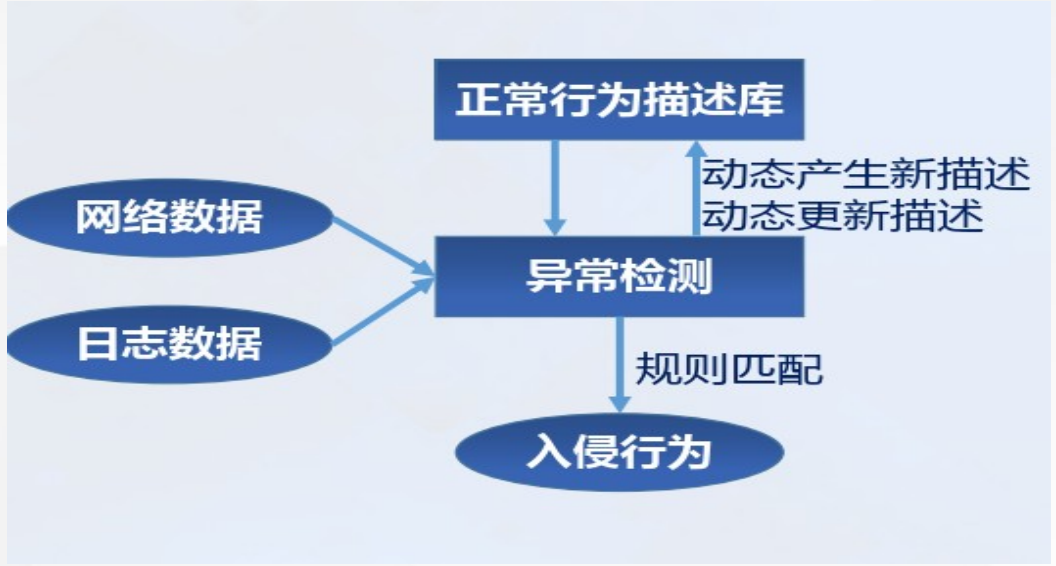
- ✓ **NIDS**：截获数据包，提取特征并与知识库中已知的攻击签名相比较
- ✓ **HIDS**：通过对日志和审计记录的监控分析来发现攻击后的误操作
- ✓ **DIDS**：同时分析来自主机系统审计日志和网络数据流

按照检测策略分类

- 误用检测
- 异常检测
- 完整性分析

- ✓ **误用检测**：将收集的信息与数据库作比较
- ✓ **异常检测**：测量属性的平均值，并用来与系统行为比较
- ✓ **完整性分析**：关注是否被更改

异常检测原理

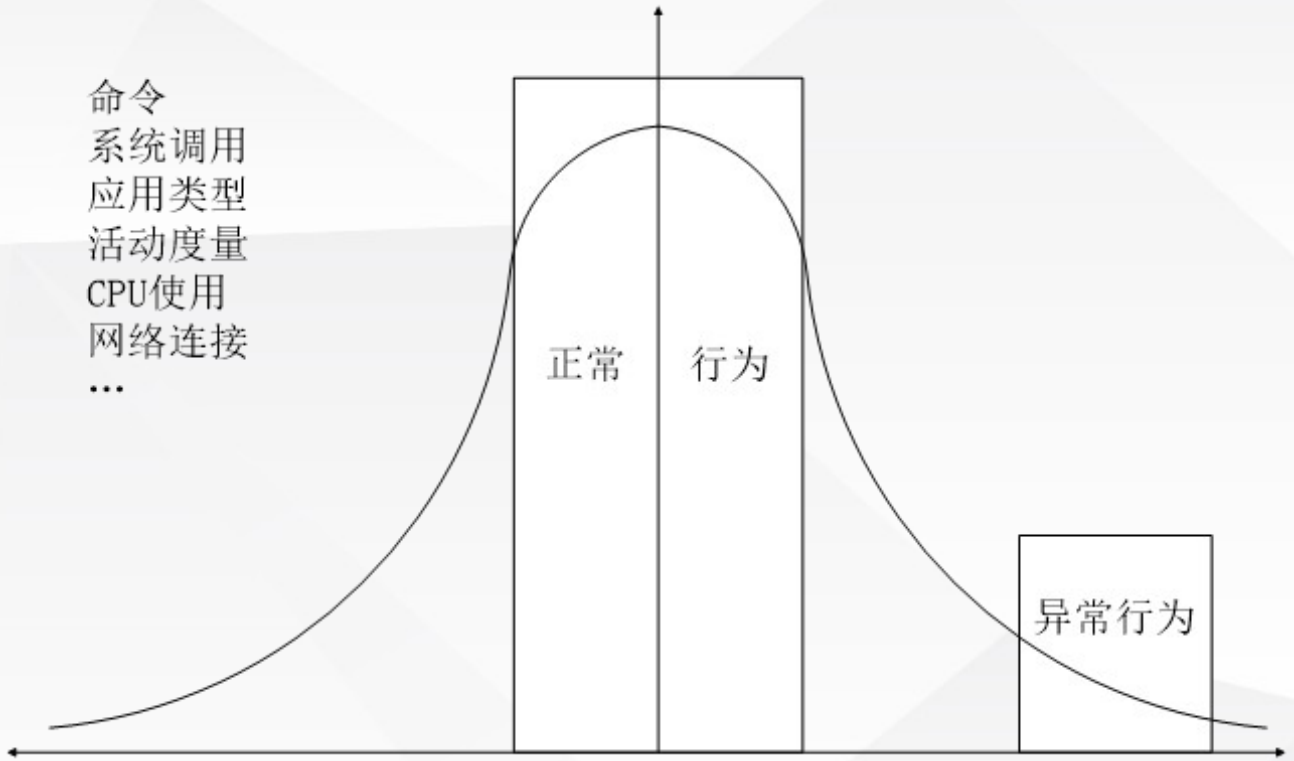


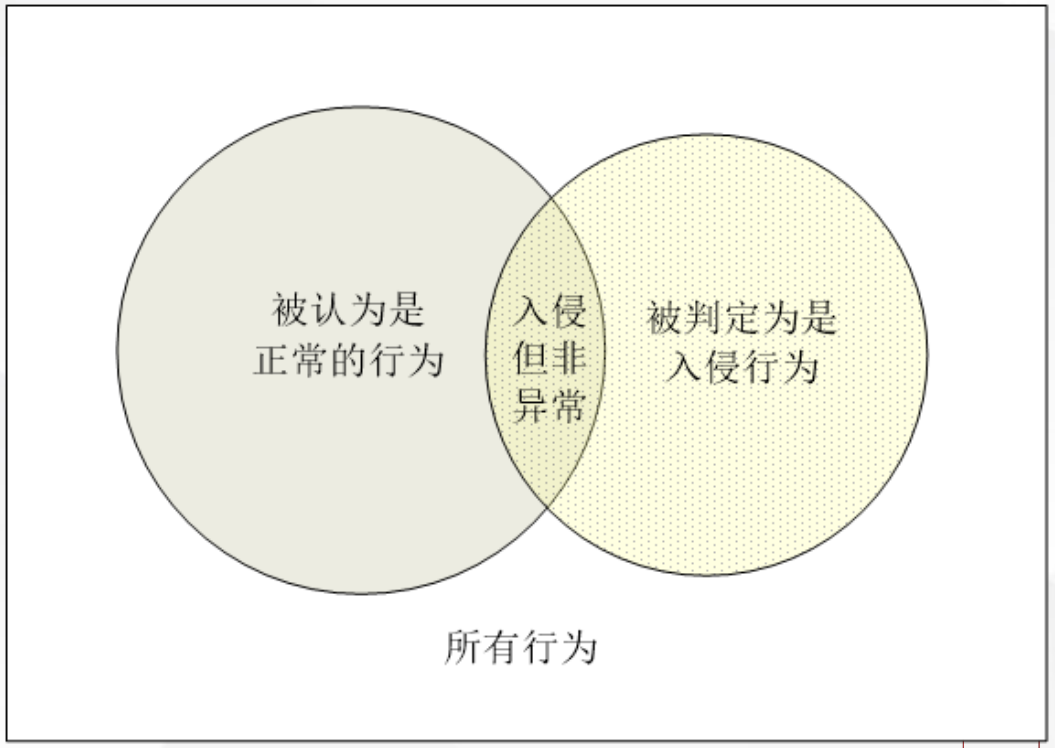
入侵检测方法：

- 统计异常检测方法
- 特征选择异常检测方法
- 基于贝叶斯推理异常检测方法
- 基于贝叶斯网络异常检测方法
- 基于模式预测异常检测方法

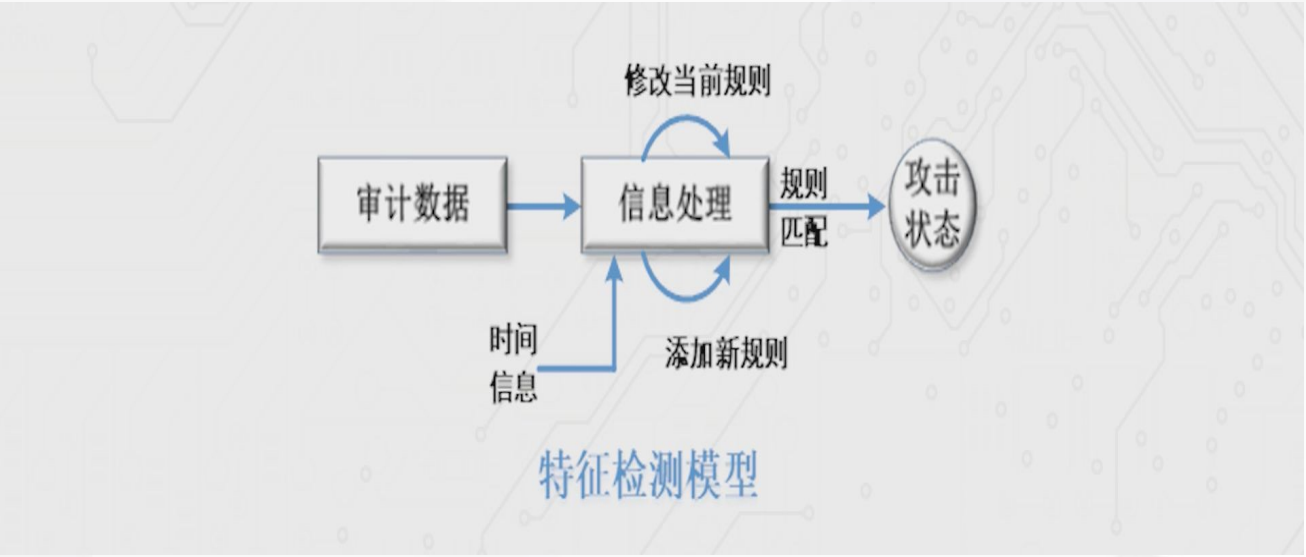
- 异常检测技术又称为**基于行为的入侵检测技术**，用来识别主机和网络中的**异常行为**。该技术假设攻击与正常合法的活动有明显的差异首先假设网络攻击行为是不常见的或是异常的，区别于所有的正常行为。
  - **阈值检测：异常检测技术先定义一组系统正常活动的阈值，**如 CPU 利用率、内存利用率、文件校验和等，然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。
  - **用户轮廓 (Profile): 通常定义为各种行为参数及其阀值的集合，用于描述正常行为范围。**
- **这种检测方式的核心在于如何分析系统运行情况。**异常检测系统的效率取决于**用户轮廓的完备性和监控的频率。**

异常检测原理


命令
系统调用
应用类型
活动度量
CPU使用
网络连接
…
正常
行为
异常行为


被认为是
正常的行为
入侵
但非
异常
被判定为是
入侵行为
所有行为

误用检测原理

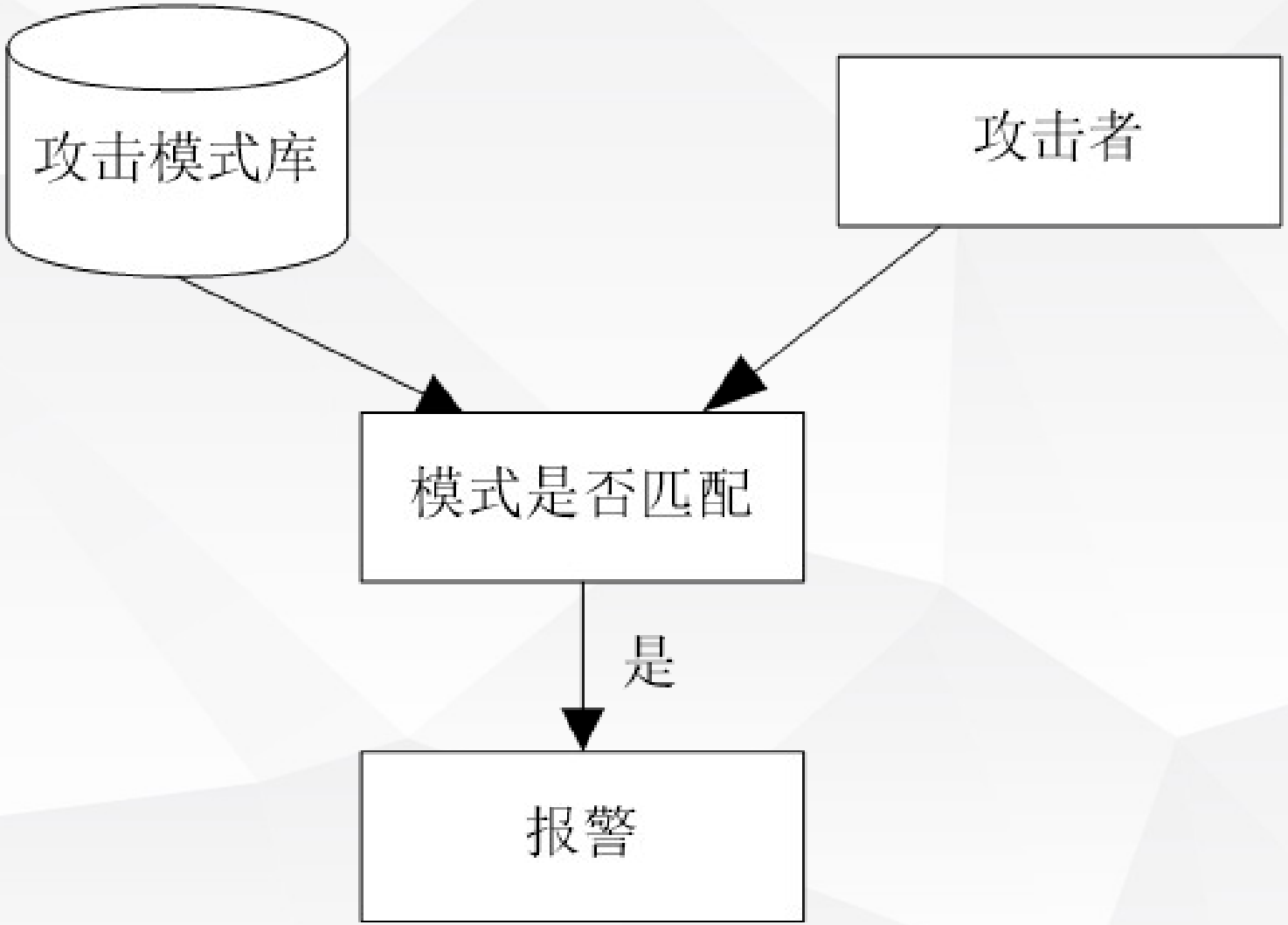


入侵检测方法：

- 基于条件概率误用检测
- 基于专家系统误用检测
- 基于状态迁移误用检测
- 基于键盘监控误用检测
- 基于 Petri 网状态转换检测

- 误用检测技术又称为**基于知识（或规则）的检测技术或者模式匹配检测技术**，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 。
  - 假设所有的网络攻击行为和方法都具有一定的模式或特征。入侵模式说明了那些导致安全突破或其它误用的事件中的特征、条件、排列和关系。

误用检测原理



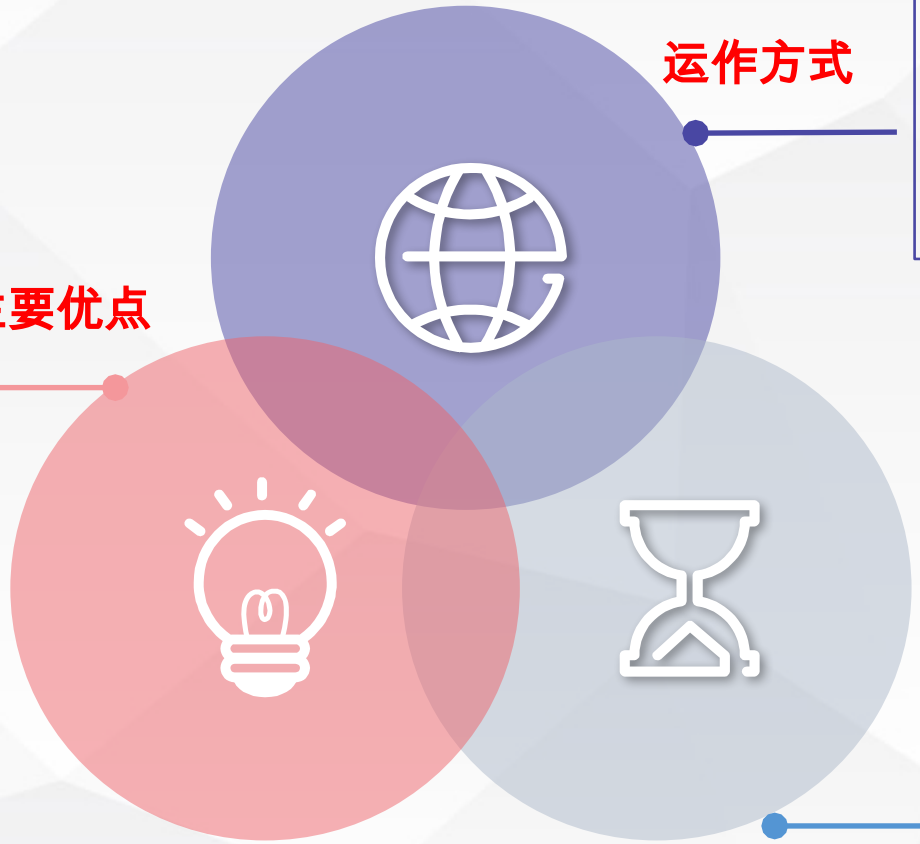
NIDS 概述

运作方式

- 根据网络流量、网络数据包和协议来分析入侵检测。
- 通常利用一个运行在随机模式下的网络适配器来监视并分析通过网络的所有通信业务。

主要优点

- 拥有成本低。
- 攻击者转移证据困难。
- 实时检测和响应。
- 能够检测未成功的攻击企图。
- 操作系统独立。



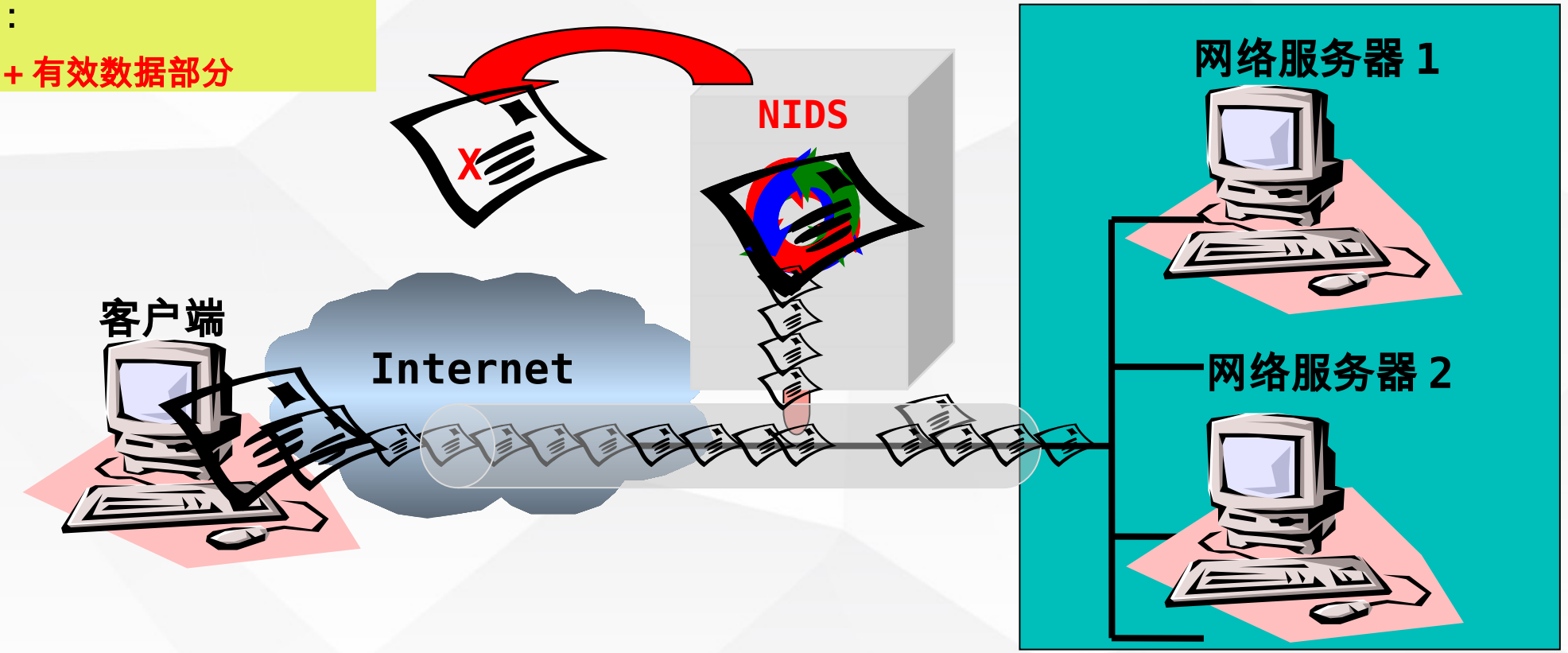
常用技术

- 攻击模式、表达式或字节匹配。
- 频率或穿越阈值。
- 低级事件的相关性。
- 统计学意义上的非常规现象检测。

NIDS 工作原理

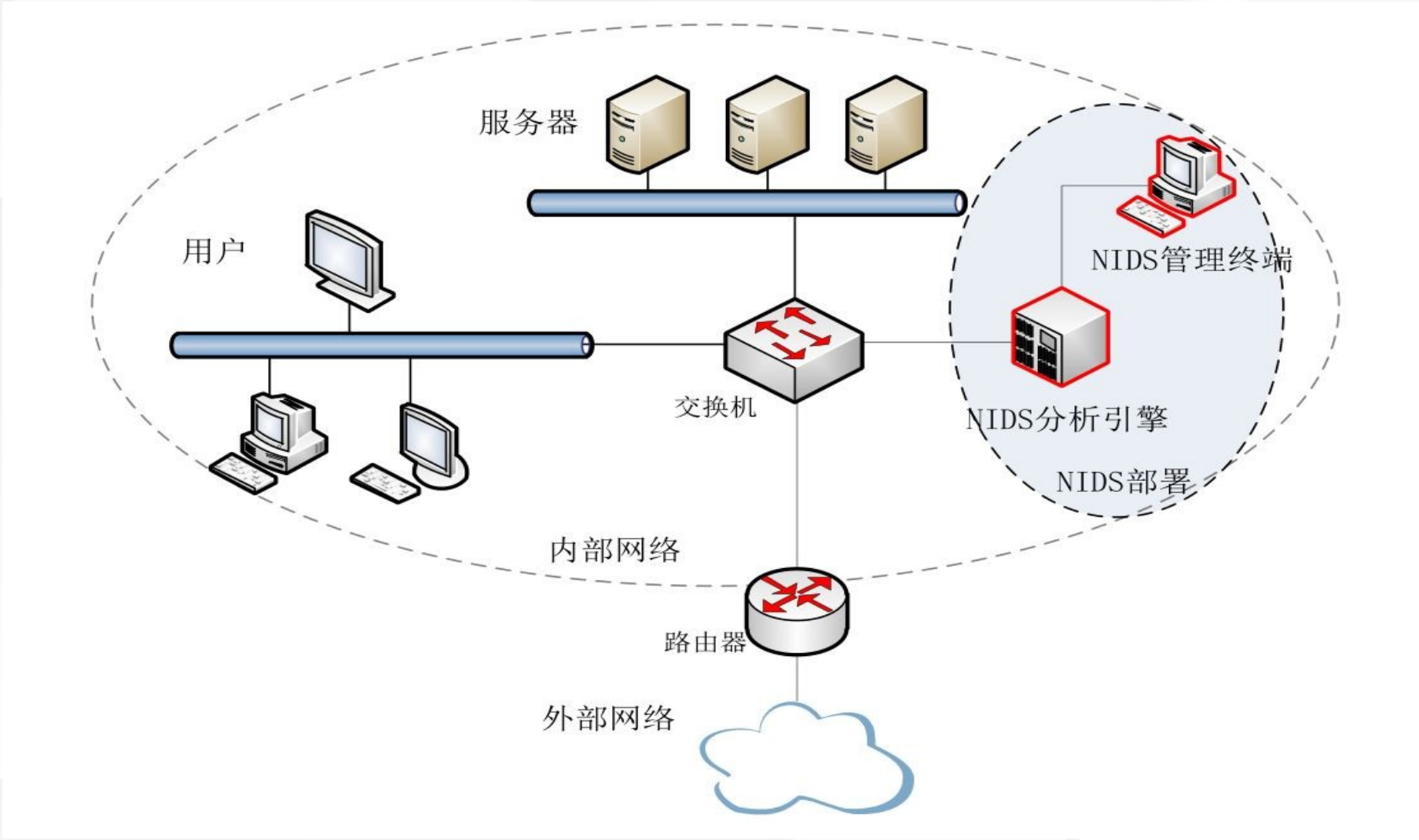
检测内容：

包头信息 + 有效数据部分



数据包 = 包头信息 + 有效数据部分

NIDS 部署

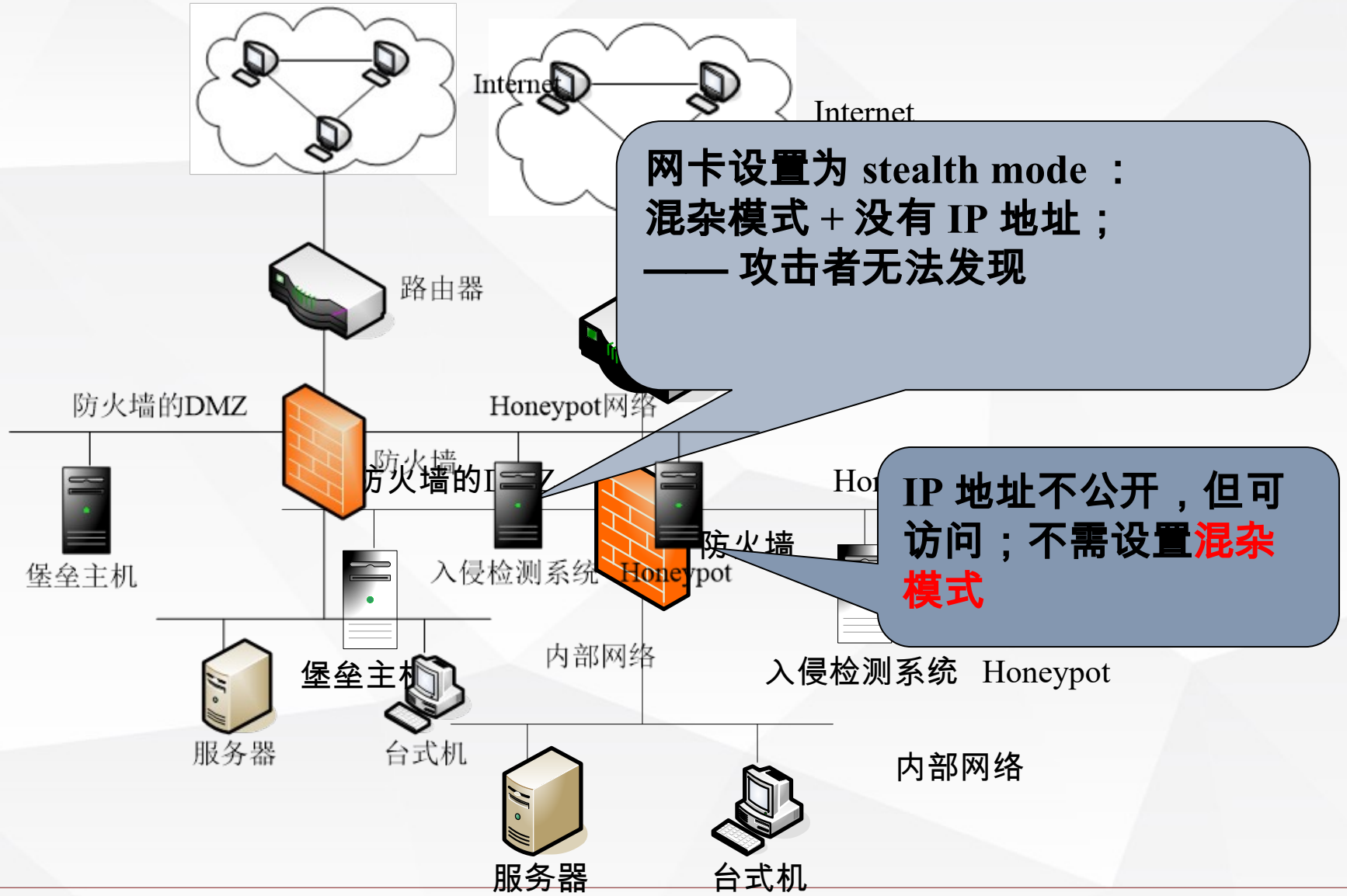


网络诱骗系统 *

- 密罐技术（ Honeypot ）就是建立一个虚假的网络，诱惑黑客攻击这个虚假的网络，从而达到保护真正网络的目的。
  - 蜜罐系统是一个包含漏洞的诱骗系统，通过模拟一个或多个易攻击的主机，给攻击者提供一个容易攻击的目标
  - 观测黑客如何探测并最终入侵系统
  - 拖延攻击者对真正目标的攻击
- 蜜罐的分类

	目的	特点	缺点	评价
低交互蜜罐产品型	检测和减轻威胁	模拟、监听不发送	获得信息有限、易被察觉	最安全、风险最小
中交互蜜罐	检测和分析	接近真实系统与真实交互	需经常检测蜜罐的状态	中等安全、用得少
高交互蜜罐研究型	研究攻击手段找到保护方法	真实系统、真实交互，不易被察觉	被攻陷后易成为黑客的跳板	危险大、使用价值大

网络诱骗系统 *



网卡设置为 stealth mode ：
混杂模式 + 没有 IP 地址；
—— 攻击者无法发现

IP 地址不公开，但可访问；不需设置混杂模式

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

谢谢！

饮水思源 爱国荣校