网 络 安 全

——防火墙

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

- 熟悉TCP/IP协议和防火墙的基础知识和概念
- 了解和掌握防火墙的分类、特点和局限性
- 掌握防火墙的相关技术和体系结构及其接入方式
- 关注有关防火墙的发展历史和国内外的研究方向

第十章 防火墙

引言

➢被动网络安全防御技术

加密技术、VPN

防火墙

入侵检测系统

防病毒软件

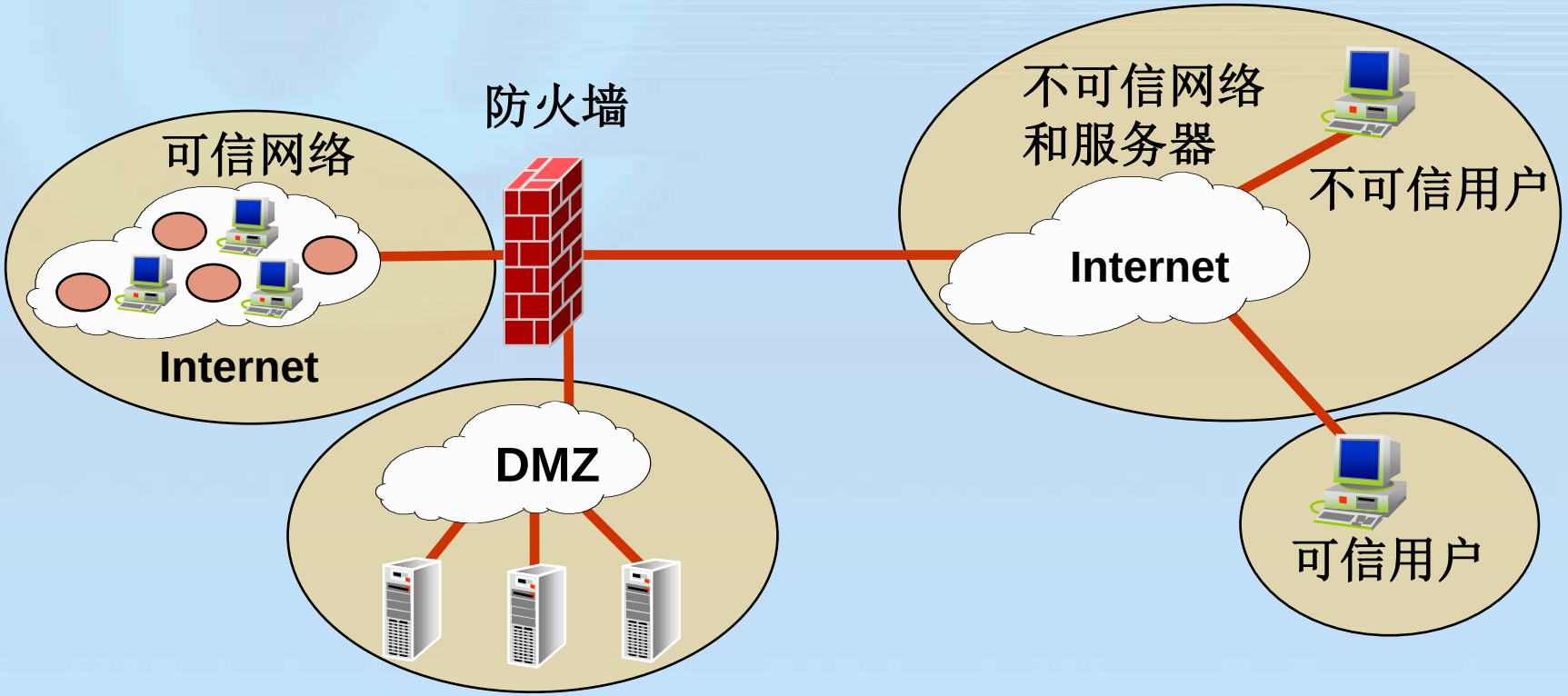
➢主动网络安全防护技术

漏洞扫描、补丁分发

入侵防御技术

蜜罐技术

防火墙



什么是防火墙

- 防火墙（Firewall）是一种用来加强网络之间访问控制的特殊网络互连设备，是一种非常有效的网络安全模型。
- **核心思想：**在不安全的网际网环境中构造一个相对安全的子网环境。
- **目的：**在被保护的内部网与不安全的非信任网络之间设立唯一的通道，以按照事先制定的策略控制信息的流入和流出，监督和控制使用者的操作。
- **本质特征:**隔离内外网络和对进出信息流实施访问控制。隔离方法可以是基于物理的，也可以是基于逻辑的；

防火墙可在链路层、网络层和应用层上实现；

从网络防御体系上看，防火墙是一种被动防御的保护装置。

保护脆弱和有缺陷的网络服务

- 一个防火墙能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。

- 防火墙同时可以保护网络免受基于路由的攻击，如IP选项中的源路由攻击和ICMP重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

加强对网络系统的访问控制

- 一个防火墙的主要功能是对整个网络的访问控制。比如防火墙可以屏蔽部分主机，使外部网络无法访问，同样可以屏蔽部分主机的特定服务，使得外部网络可以访问该主机的其它服务，但无法访问该主机的特定服务。
- 防火墙不应向外界提供网络中任何不需要服务的访问权，这实际上是安全政策的要求了。
- 控制对特殊站点的访问：如有些主机或服务能被外部网络访问，而有些则需被保护起来，防止不必要的访问。

防火墙特征

对网络存取和访问进行监控审计

- 如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。
- 另外，收集一个网络的使用和误用情况是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

防火墙的分类

个人防火墙

- 是在操作系统上运行的软件，为个人计算机提供简单的防火墙功能；
- 安装在个人PC上，而不是放置在网络边界，因此，个人防火墙关心的不是一个网络到另外一个网络的安全，而是单个主机和与之相连接的主机或网络之间的安全。

网络防火墙

防火墙的分类

软件防火墙

- 个人防火墙也是一种纯软件防火墙，但其应用范围较小，并且安全性和并发连接处理能力较差；

硬件防火墙

- 采用专用芯片（非X86芯片）来处理防火墙核心策略的一种硬件防火墙，也称为芯片级防火墙。（专用集成电路（ASIC）芯片或者网络处理器（NP）芯片）；
- 最大的亮点：高性能，非常高的并发连接数和吞吐量；
- 采用ASIC芯片的方法在国外比较流行，技术也比较成熟，如美国NetScreen公司的高端防火墙产品；国内芯片级防火墙大多还处于开发发展的阶段，采用的是NP技术。

防火墙的局限性

防火墙只是整个网络安全防护体系的一部分，且并非万无一失：

- 不能防止受病毒感染的文件的传输；
- 不能解决来自内部网络的攻击和安全问题；
- 不能防止策略配置不当或错误配置引起的安全威胁；
- 不能防止自然或人为的故意破坏；不能防止本身安全漏洞的威胁；只能防范经过其本身的非法访问和攻击，对绕过防火墙的访问和攻击无能为力。

防火墙的实现技术

- 数据包过滤(Packet Filtering)
- 状态检测(Stateful Inspection)
- 代理服务(Proxy Service)
- 网络地址转换(Network Address Translation)

数据包过滤（1）


应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
数据链路层
物理层

路由器

数据包过滤（2）

- 数据包过滤技术是一种简单、高效的安全控制技术，是防火墙发展初期普遍采用的技术。

工作原理：

- 系统在网络层检查数据包，与应用层无关。
- 依据在系统内设置的过滤规则（通常称为访问控制表——Access Control List）对数据流中每个数据包包头中的参数或它们的组合进行检查，以确定是否允许该数据包进出内部网络。

数据包过滤（3）

包过滤一般要检查（网络层的IP头和传输层的头）：

- IP源地址
- IP目的地址
- 协议类型（TCP包/UDP包/ICMP包）
- TCP或UDP的源端口
- TCP或UDP的目的端口
- ICMP消息类型
- TCP报头中的ACK位

某条过滤规则为：禁止地址1的任意端口到地址2的80端口的TCP包。**含义是什么？**

表示禁止地址1的计算机连接地址2的计算机的WWW服务

数据包过滤（4）

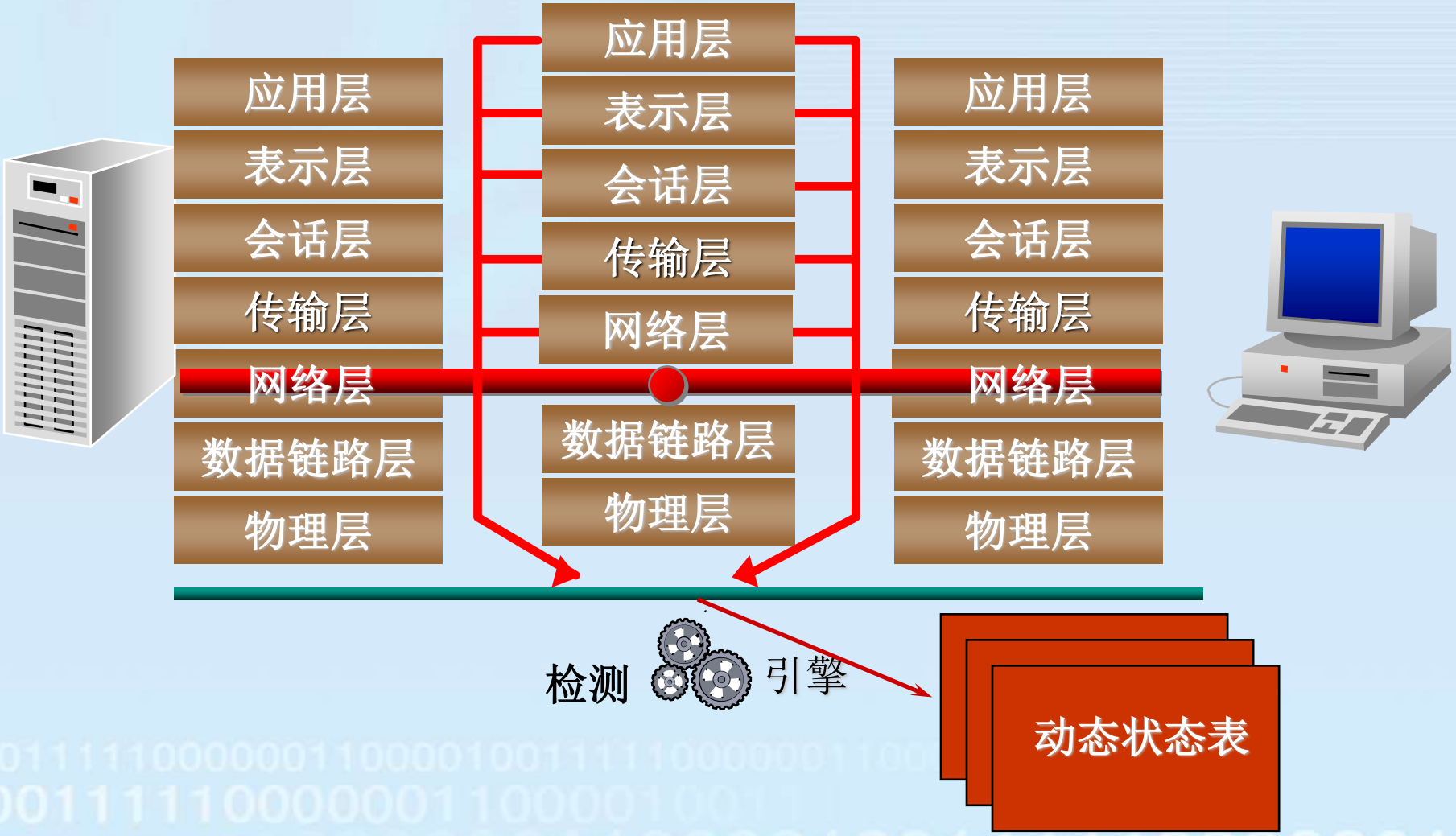
优点：

逻辑简单，价格便宜，易于安装和使用，网络性能和透明性好。

主要缺点：

- 安全控制的力度只限于源地址、目的地址和端口号等，不能保存与传输或与应用相关的状态信息，因而只能进行较为初步的安全控制，安全性较低；
- 数据包的源地址、目的地址以及端口号等都在数据包的头部，很有可能被窃听或假冒。

状态检测（1/4）


应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
检测
引擎
动态状态表

状态检测（2/4）

- 状态检测防火墙是在动态包过滤的基础上，增加了状态检测机制而形成的；
- 动态包过滤与普通包过滤相比，需要多做一项工作：对外出数据包的“身份”做一个标记，允许相同连接的进入数据包通过。
- 利用状态表跟踪每一个网络会话的状态，对每一个数据包的检查不仅根据规则表，更考虑了数据包是否符合会话所处的状态；
- 状态检测防火墙采用了一个在网关上执行网络安全策略的软件引擎，称之为检测模块。检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各层实施监测，并动态地保存起来作为以后制定安全决策的参考。

状态检测（3/4）

状态检测既能够提供代理服务的控制灵活性，又能够提供包过滤的高效性，是二者的结合；

工作过程：

对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接；请求数据包通过，并记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表，就可以通过。

状态检测（4/4）

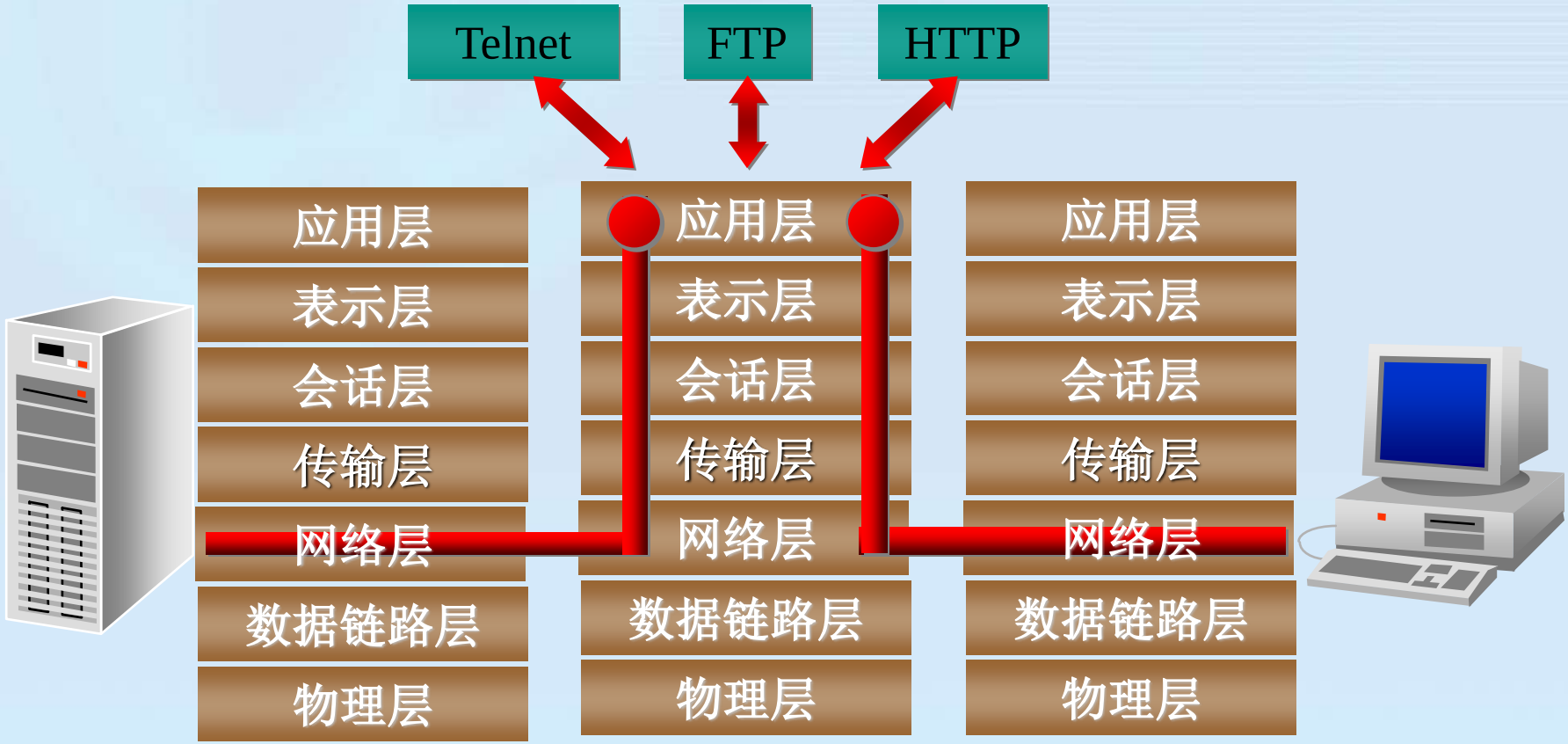
主要优点：

- 高安全性（工作在数据链路层和网络层之间；“状态感知”能力）
- 高效性（对连接的后续数据包直接进行状态检查）
- 应用范围广（支持基于无连接协议的应用）

主要缺点：

状态检测防火墙在阻止DDoS攻击、病毒传播问题以及高级应用入侵问题（如实现应用层内容过滤）等方面显得力不从心。

代理服务（1/3）


Telnet
FTP
HTTP
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层

代理服务（2/3）

代理服务是运行于连接内部网络与外部网络的主机（堡垒主机）上的一种应用，是一种比较高级的防火墙技术。

工作过程：

当用户需要访问代理服务器另一侧的主机时，对符合安全规则的连接，代理服务器会代替主机响应，并重新向主机发出一个相同的请求。当此连接请求得到回应并建立起连接之后，内部主机同外部主机之间的通信将通过代理程序把相应连接进行映射来实现。对于用户而言，似乎是直接与外部网络相连。

代理服务（3/3）

主要优点：

- 重要信息不易外泄，从而减少了黑客攻击时所必需的必要信息；
- 可以实施用户认证、详细日志、审计跟踪和数据加密等功能和对具体协议及应用的过滤，有被攻击迹象时会提示网络管理员，并保留攻击痕迹，安全性较高。

主要缺点：

- 针对不同的应用层协议必须有单独的应用代理，也不能自动支持新的网络应用；
- 有些代理还需要相应的支持代理的客户和服务器软件；用户可能还需要专门学习程序的使用方法才能通过代理访问Internet；
- 性能下降。

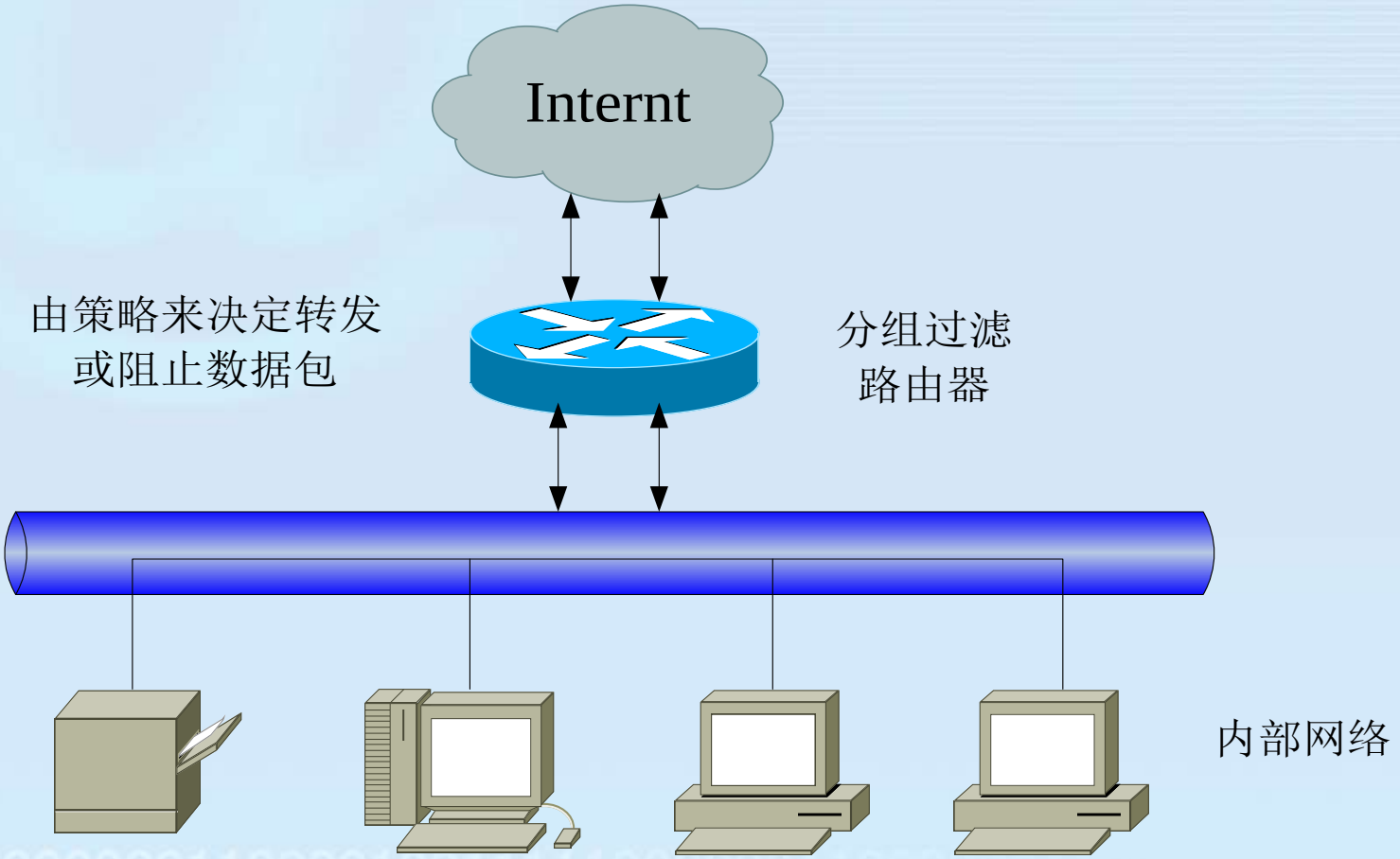
防火墙的体系结构

- **防火墙的体系结构：**防火墙系统实现所采用的架构及其实现所采用的方法，它决定着防火墙的功能、性能以及使用范围。

- 防火墙可以被设置成许多不同的结构，并提供不同级别的安全，而维护运行的费用也各不相同。

  - 分组过滤路由器
  - 双宿主机
  - 屏蔽主机
  - 屏蔽子网

分组过滤路由器



分组过滤路由器

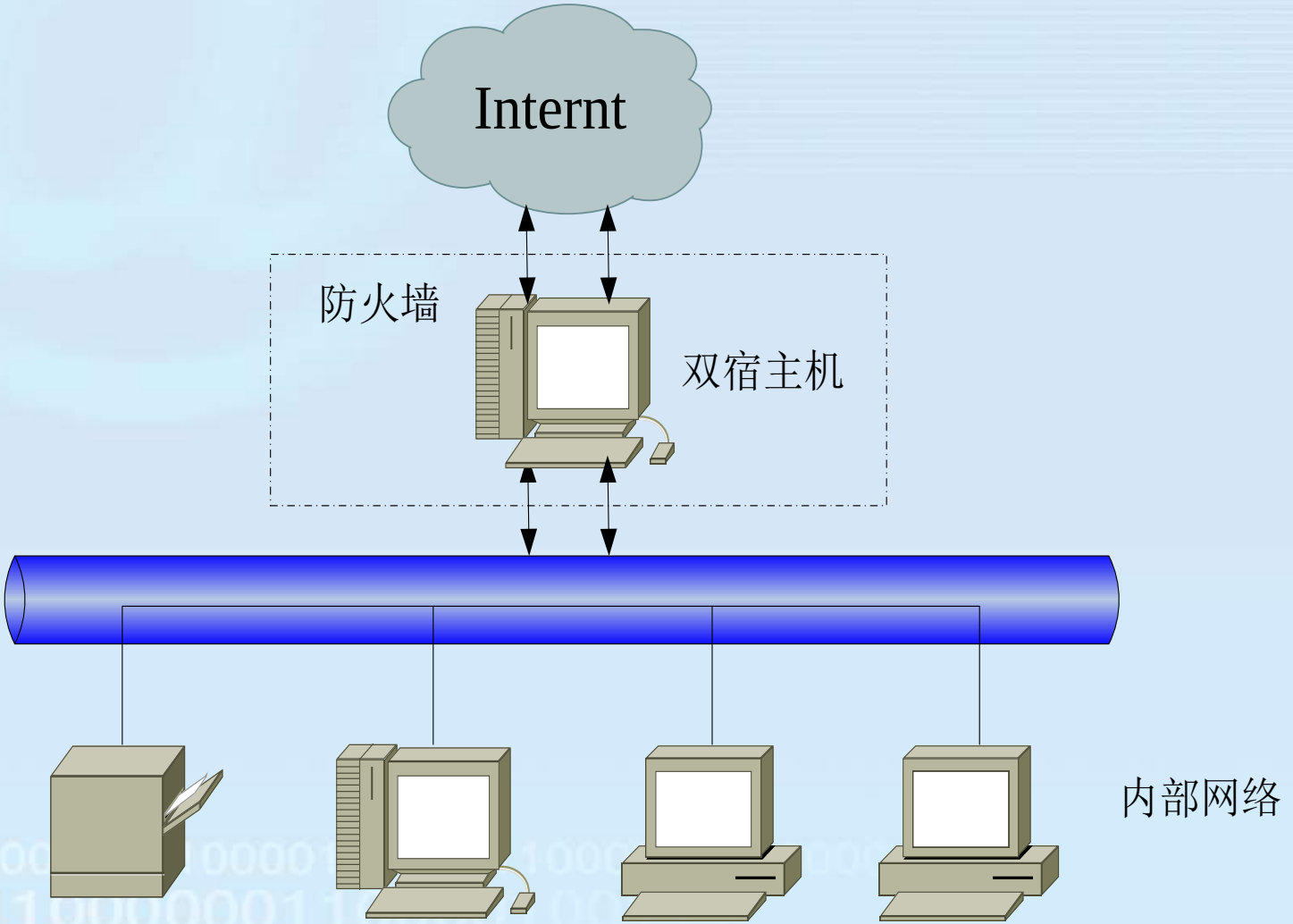
- 作为内外网连接的唯一通道，要求所有的报文都必须在此通过检查。

- 通过在分组过滤路由器上安装基于IP层的报文过滤软件，就可利用过滤规则实现报文过滤功能。

缺点：

- 在单机上实现，是网络中的“单失效点”。
- 不支持有效的用户认证、不提供有用的日志，安全性低。

双宿主机



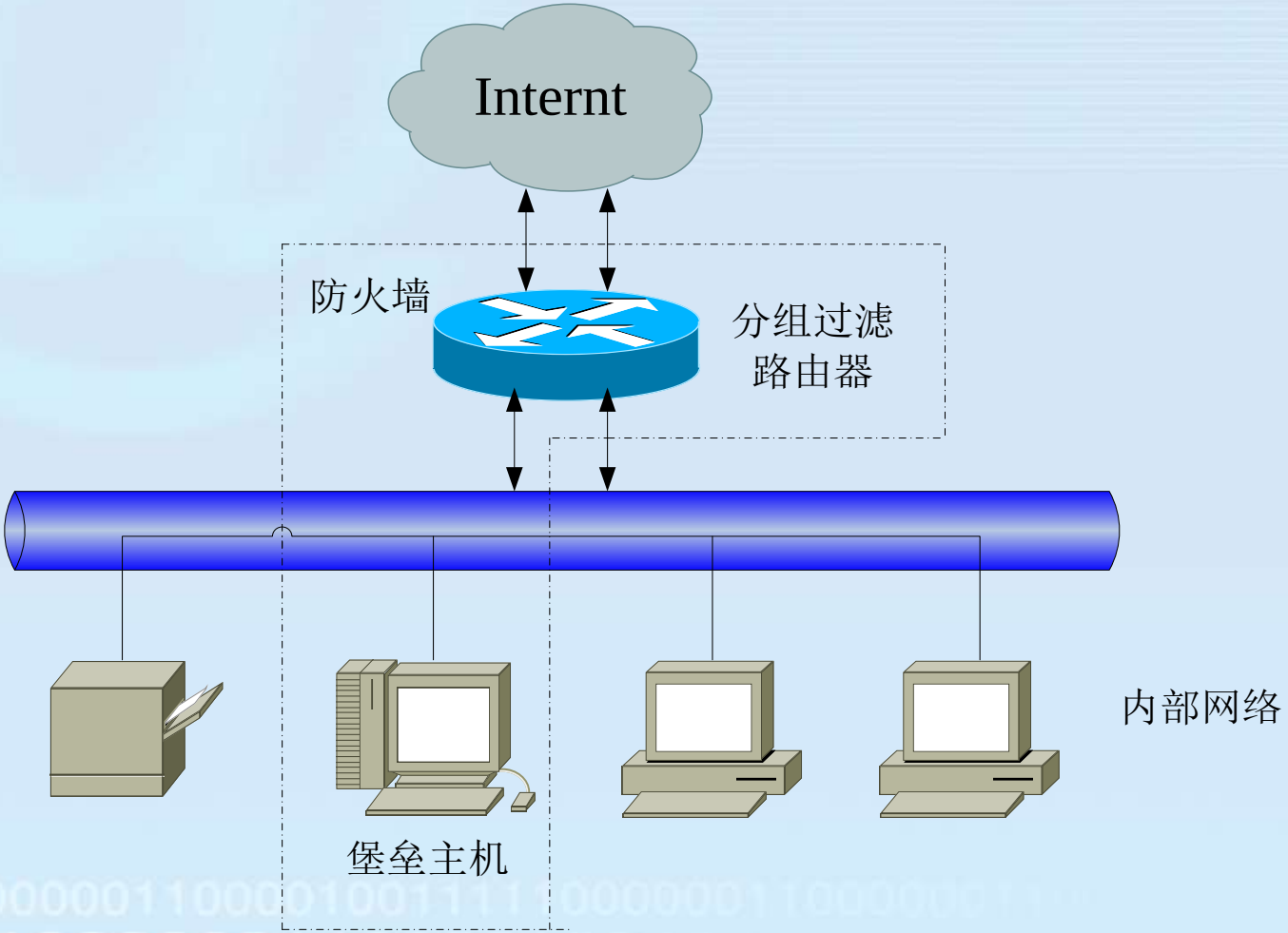
双宿主机

- 在被保护网络和Internet之间设置一个具有双网卡的堡垒主机，IP层的通信完全被阻止，两个网络之间的通信可以通过应用层数据共享或应用层代理服务来完成
- 通常采用代理服务的方法
- 堡垒主机上运行着防火墙软件，可以转发应用程序和提供服务等

优缺点：

- 堡垒主机的系统软件可用于身份认证和维护系统日志，有利于进行安全审计
- 该方式的防火墙仍是网络的“单失效点”。
- 隔离了一切内部网与Internet的直接连接，不适合于一些高灵活性要求的场合

屏蔽主机



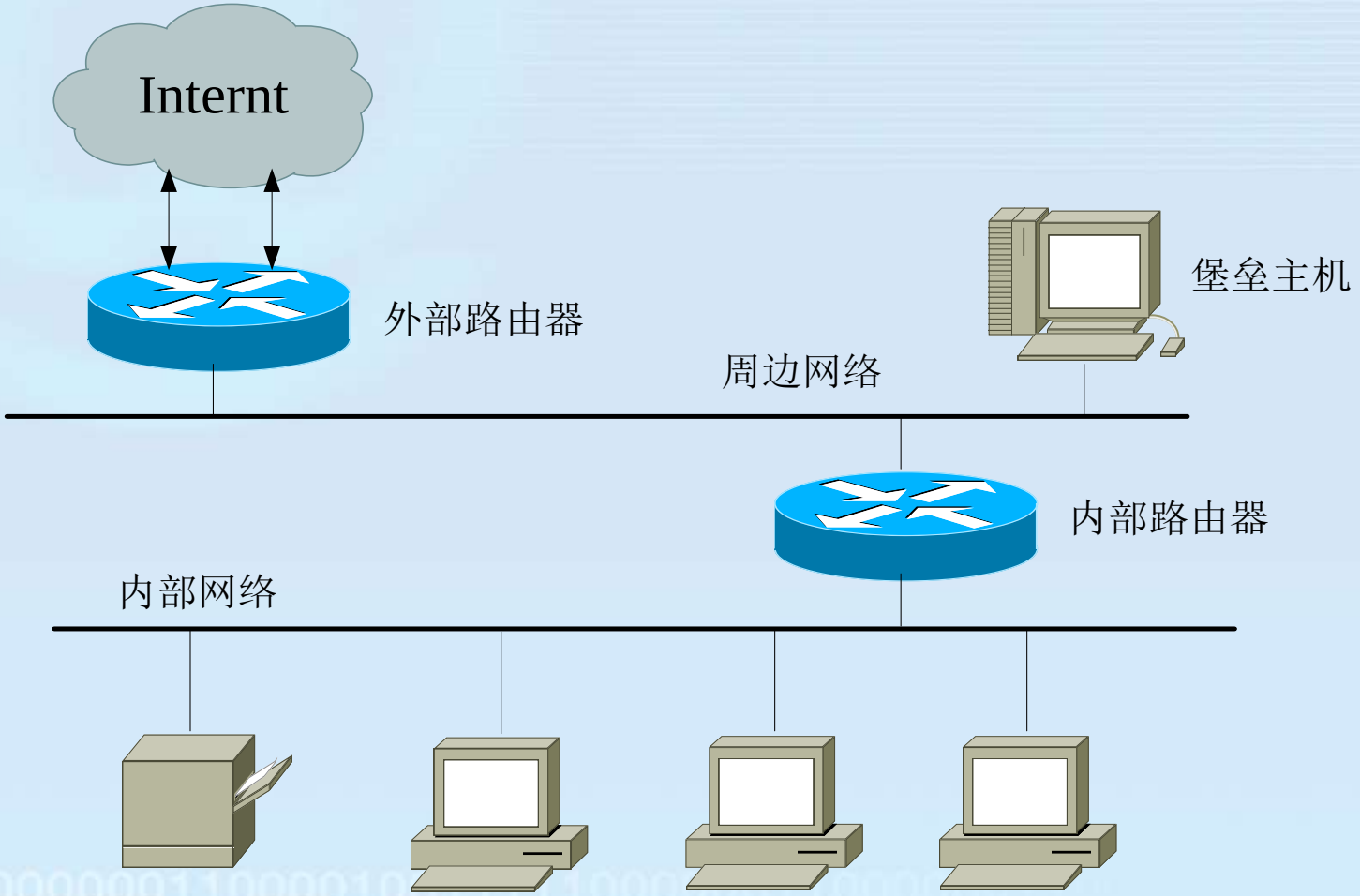
屏蔽主机

- 一个分组过滤路由器连接外部网络，同时一个运行网关软件的堡垒主机安装在内部网络。通常在路由器上设立过滤规则，使这个堡垒主机成为从外部唯一可直接到达的主机。

- 提供的安全等级较高，因为它实现了网络层安全（包过滤）和应用层安全（代理服务）。

- 过滤路由器是否正确配置是这种防火墙安全与否的关键。过滤路由器的路由表应当受到严格的保护，如果路由表遭到破坏，则堡垒主机就有被越过的危险。

屏蔽子网



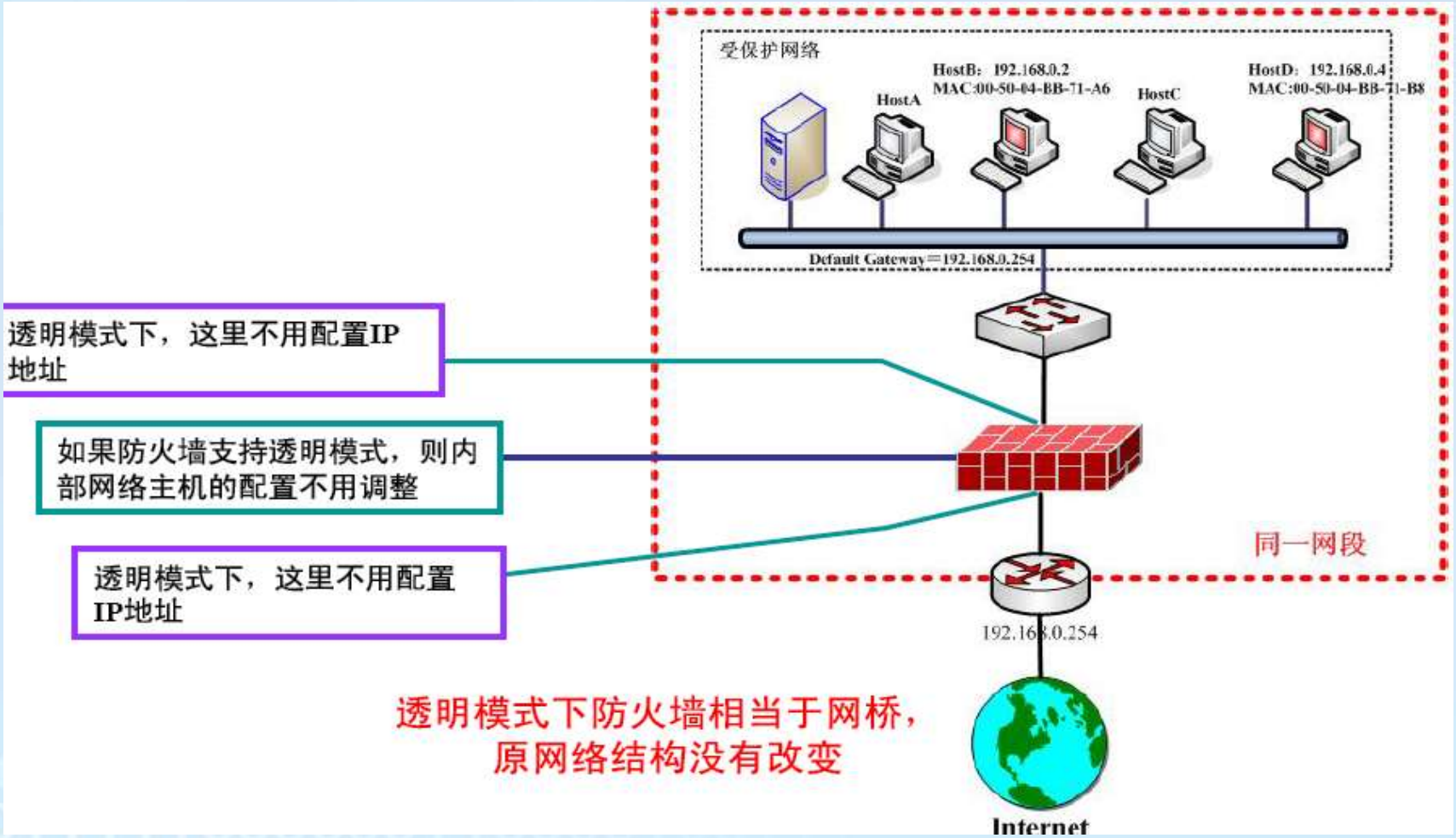
屏蔽子网

- 是最安全的防火墙系统，它在内部网络和外部网络之间建立一个被隔离的子网（非军事区，DMZ（Demilitarized Zone））
- 在很多实现中，两个分组过滤路由器放在子网的两端，内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信
- 通常将堡垒主机、各种信息服务器等公用服务器放于DMZ中
- 堡垒主机通常是黑客集中攻击的目标，如果没有DMZ，入侵者控制堡垒主机后就可以监听整个内部网络的会话

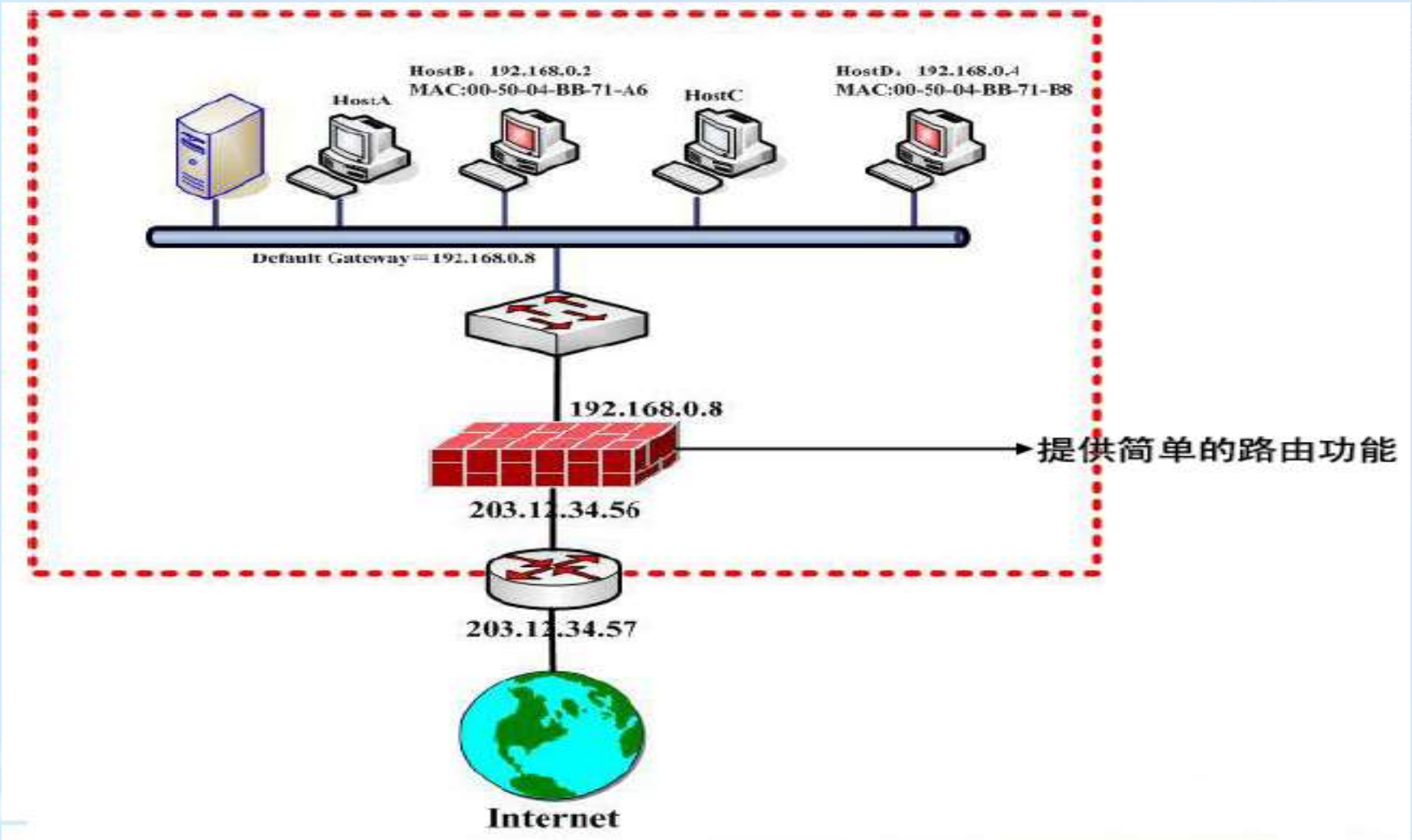
防火墙接入方式

- 透明接入
- 路由接入
- 混合接入

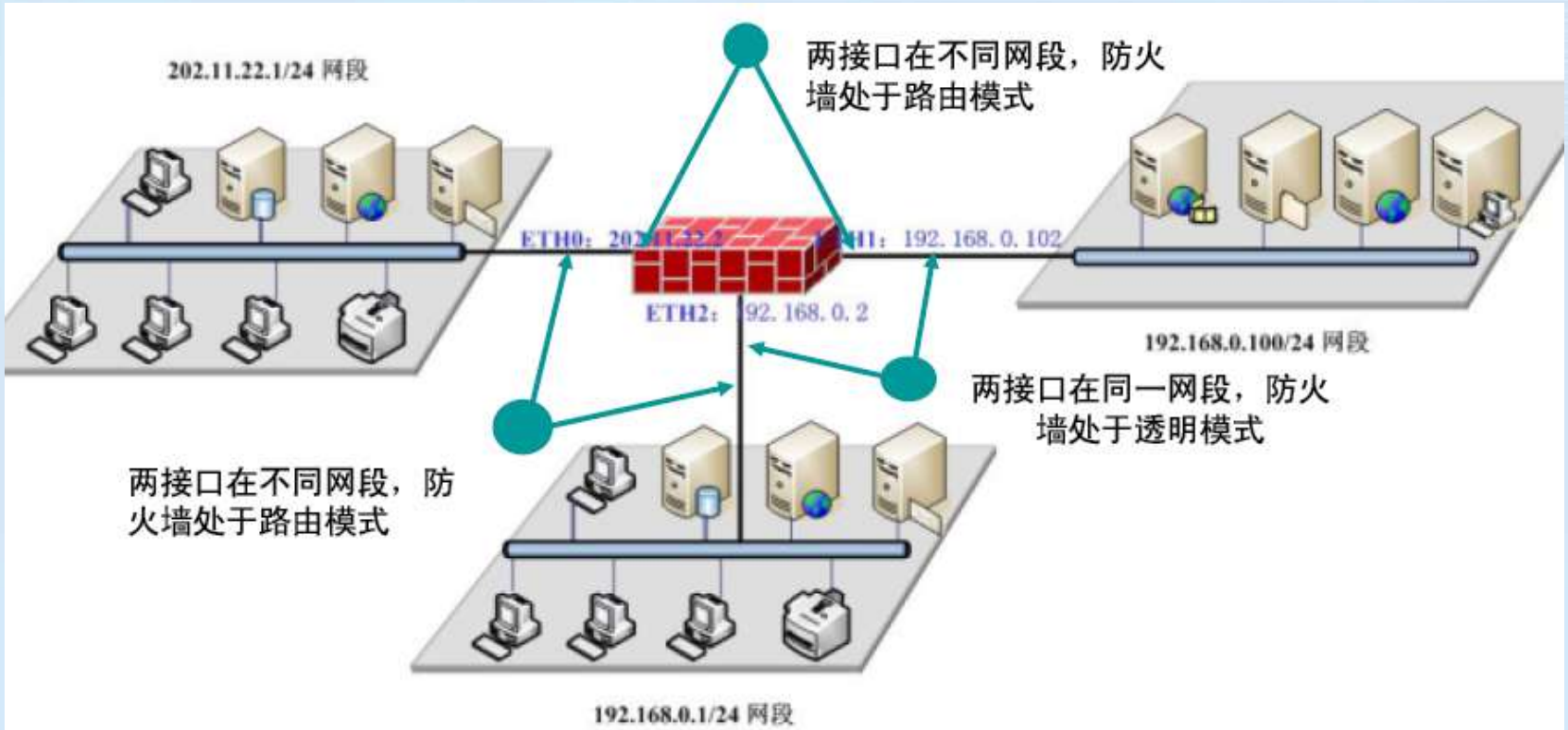
透明接入


受保护网络
HostA
HostB：192.168.0.2
MAC:00-50-04-BB-71-A6
HostC
HostD：192.168.0.4
MAC:00-50-04-BB-71-B8
Default Gateway=192.168.0.254
透明模式下，这里不用配置IP地址
如果防火墙支持透明模式，则内部网络主机的配置不用调整
透明模式下，这里不用配置IP地址
同一网段
192.168.0.254
透明模式下防火墙相当于网桥，
原网络结构没有改变
Internet

路由接入


HostB：192.168.0.2
MAC:00-50-04-BB-71-A6
HostA
HostC
HostD：192.168.0.4
MAC:00-50-04-BB-71-B8
Default Gateway=192.168.0.8
192.168.0.8
提供简单的路由功能
203.12.34.56
203.12.34.57
Internet

混合接入



此时整个防火墙工作于透明+路由模式，我们称之为综合模式或者混合模式

防火墙发展历程和展望

- 基于路由器的防火墙
- 用户化的防火墙工具套件
- 建立在通用操作系统上的防火墙
- 具有安全操作系统的防火墙
- 智能防火墙
- 分布式防火墙
- 网络安全产品的系统化
- 主流防火墙产品简介

第一代：基于路由器的防火墙

称为包过滤防火墙，其特征：

- 以访问控制表方式实现分组过滤
- 过滤的依据是IP地址、端口号和其它网络特征
- 只有分组过滤功能，且防火墙与路由器一体

缺点：

- 路由协议本身具有安全漏洞
- 路由器上的分组过滤规则的设置和配置复杂
- 攻击者可假冒地址
- 本质缺陷：一对矛盾，防火墙的设置会大大降低路由器的性能

  路由器：为网络访问提供动态灵活的路由

  防火墙：对访问行为实施静态固定的控制

第二代：用户化的防火墙工具套件

特征：

- 将过滤功能从路由器中独立出来，并加上审计和告警功能；
- 针对用户需求提供模块化的软件包；
- 安全性提高，价格降低；
- 纯软件产品，实现维护复杂。

缺点：

- 配置和维护过程复杂费时；
- 对用户技术要求高；
- 全软件实现，安全性和处理速度均有局限；

第三代：建立在通用操作系统上

特征：

- 包括分组过滤或借用路由器的分组过滤功能；
- 装有专用的代理系统，监控所有协议的数据和指令；
- 保护用户编程空间和用户可配置内核参数的设置；
- 安全性和速度大为提高。

实现方式：软件、硬件、软硬结合。

第三代：建立在通用操作系统上

问题：

- 作为基础的操作系统及其内核的安全性无从保证。
- 通用操作系统厂商不会对防火墙的安全性负责；
- 从本质上看，第三代防火墙既要防止来自外部网络的攻击，还要防止来自操作系统漏洞的攻击。
- 用户必须依赖两方面的安全支持：防火墙厂商和操作系统厂商。

第四代：具有安全操作系统的防火墙

- 防火墙厂商具有操作系统的源代码，并可实现安全内核；
- 对安全内核实现加固处理：即去掉不必要的系统特性，强化安全保护；
- 对每个服务器、子系统都作了安全处理；
- 在功能上包括了分组过滤、代理服务，且具有加密与鉴别功能；
- 透明性好，易于使用。

第四代防火墙的抗攻击能力(cont.)

抗IP假冒攻击

- 由于第四代防火墙知道网络内外的IP地址，它会丢弃所有来自网络外部但却有内部地址的分组，再之防火墙已将网内的实际地址隐蔽起来，外部用户很难知道内部的IP地址，因而难以攻击。

抗特洛伊木马攻击

- 第四代防火墙是建立在安全的操作系统之上的，其安全内核中不能执行下载的程序，故而可防止特洛伊木马的发生。必须指出的是，防火墙能抗特洛伊木马攻击并不表明受其保护的某个主机也能防止这类攻击。事实上，内部用户可通过防火墙下载程序，并执行下载的程序。

抗口令字探寻攻击

- 第四代防火墙采用了一次性口令字和禁止直接登录防火墙的措施，能有效防止对口令字的攻击。

智能防火墙

- **传统防火墙：**采用数据匹配检查技术

- **智能防火墙：**采用人工智能识别技术（统计、记忆、概率和决策等）

  优势：安全，高效

  应用：在保护网络和站点免受黑客攻击、阻断病毒的恶意传播、有效监控和管理内部局域网、保护必需的应用安全、提供强大的身份认证授权和审计管理等方面具有广泛的应用价值。

分布式防火墙

➢**传统防火墙：**边界防火墙

缺陷：结构性限制；内部威胁；效率和故障

➢**分布式防火墙（广义）：**一种新的防火墙体系结构（包含网络防火墙、主机防火墙和管理中心）

优势：在网络内部增加了另一层安全，有效抵御来自内部的攻击，消除网络边界上的通信瓶颈和单一故障点，支持基于加密和认证的网络应用，与拓扑无关，支持移动计算。

网络安全产品的系统化

“以防火墙为核心的网络安全体系”

解决方法：

- 直接把相关安全产品“做”到防火墙中
- 各个产品相互分离，但是通过某种通信方式形成一个整体（防火墙联动技术）

联动：通过一种组合的方式，将不同技术与防火墙技术进行整合，在提高防火墙自身功能和性能的同时，由其他技术完成防火墙所缺乏的功能，以适应网络安全整体化、立体化的要求。

- 防火墙与防病毒产品联动
- 防火墙与IDS联动
- 防火墙与认证系统联动
- 防火墙与日志分析系统联动

主流防火墙产品简介

国内：天融信网络卫士防火墙（NGFW）

- 我国第一套自主版权的防火墙系统
- TOPSEC（Talent Open Protocol for Security）安全体系（联动协议安全标准）

国外：CheckPoint的Firewall-1防火墙

- 状态检测（Stateful Inspection）技术最早由CheckPoint提出
- OPSEC，开放安全企业互联联盟的组织和倡导者之一，允许用户通过一个开放的、可扩展的框架集成、管理所有的安全产品。（目前已有包括IBM、HP、Sun、Cisco、BAY等超过135个公司加入到OPSEC联盟。）

防火墙性能测试简介

性能测试标准：RFC 2544（2-3层）和RFC 3511（4-7层）

- 吞吐量：网络设备在不丢失任何一个帧情况下的最大转发速率。
- 延时（比特转发）：入口处输入帧第1个比特到达被测设备至出口处输出帧的第1个比特输出时所用的时间间隔
- 丢包率：在稳态负载下由于缺少资源应转发而没有转发的帧占所有应被转发的帧的比例
- 背靠背：从空闲状态开始，以达到传输介质最小合法间隔极限的传输速率，发送一定数量固定长度的帧，当出现第一个帧丢失时所发送的帧数。

防火墙应用——Iptables

Iptables是Linux下基于内核的包过滤防火墙，功能非常强大。

优点：

- 更好的与Linux内核集成，有更高的速度和可靠性；
- 可以跟踪数据包的状态;这意味着防火墙会跟踪每个通过它的链接，查看数据流的内容，来判断是否违反规则；
- 可以基于MAC地址和TCP报文头的标志位来过滤；
- 支持级别日志；
- 更好的NAT功能；
- 更好的与web代理集成，如Squid；
- 可以有限的防范Dos攻击。

Iptables简介

Iptables将数据的传输分为三中链路

- OUTPUT(从内部网络流出的数据)
- INPUT(从外网流入的数据)
- FORWARD(需要转发的数据)

Iptables处理数据分为四种状态

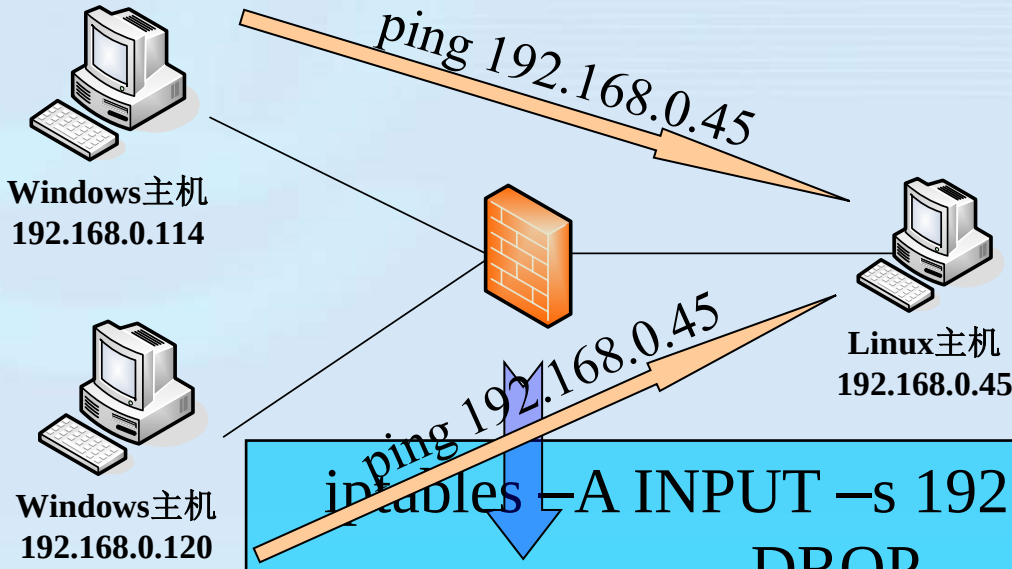
DROP(丢弃)　ACCEPT(接受)

REJECT(弹回)　LOG(日志)

Iptables基本命令

-A 添加一条规则　-D 删除一条规则　-L 显示所有规则

实验环境



iptables –A INPUT –s 192.168.0.114 –j DROP

协议	源地址	源端口	目的地址	目的端口	行为	方向
Tcp	192.168.0.114	Any	192.168.0.45	Any	DROP	IN

防火墙实验简介

实验任务一：配置Iptables包过滤规则实验

实验原理：Iptables规则存储在专用的数据包过滤表中，而这些表集成在Linux内核中。在数据包过滤表中，规则被分组放在链中。如果Linux系统连接到因特网或LAN、服务器或连接LAN和因特网的代理服务器，则Iptables有利于在Linux系统上更好地控制IP数据包过滤和防火墙配置。而当INPUT、FORWARD和OUTPUT链的配置策略为ACCEPT时，主机之间可以互相Ping通。

实验主要原理

实验任务二：配置规则控制SSH功能开关实验

实验原理：通过配置Iptables规则从而控制SSH功能开关，以实现利用SSH连通或断开主机之间的连接。

实验任务三：实现单向Ping功能实验

实验原理：使用相关命令配置Iptables防火墙，实现单向Ping功能。

Iptables命令

Iptables由四表五链组成。每个表分别实现不同的功能，每个表拥有不同的链，链代表规则实现的位置。

四表分别为：

⑩filter：过滤，防火墙；

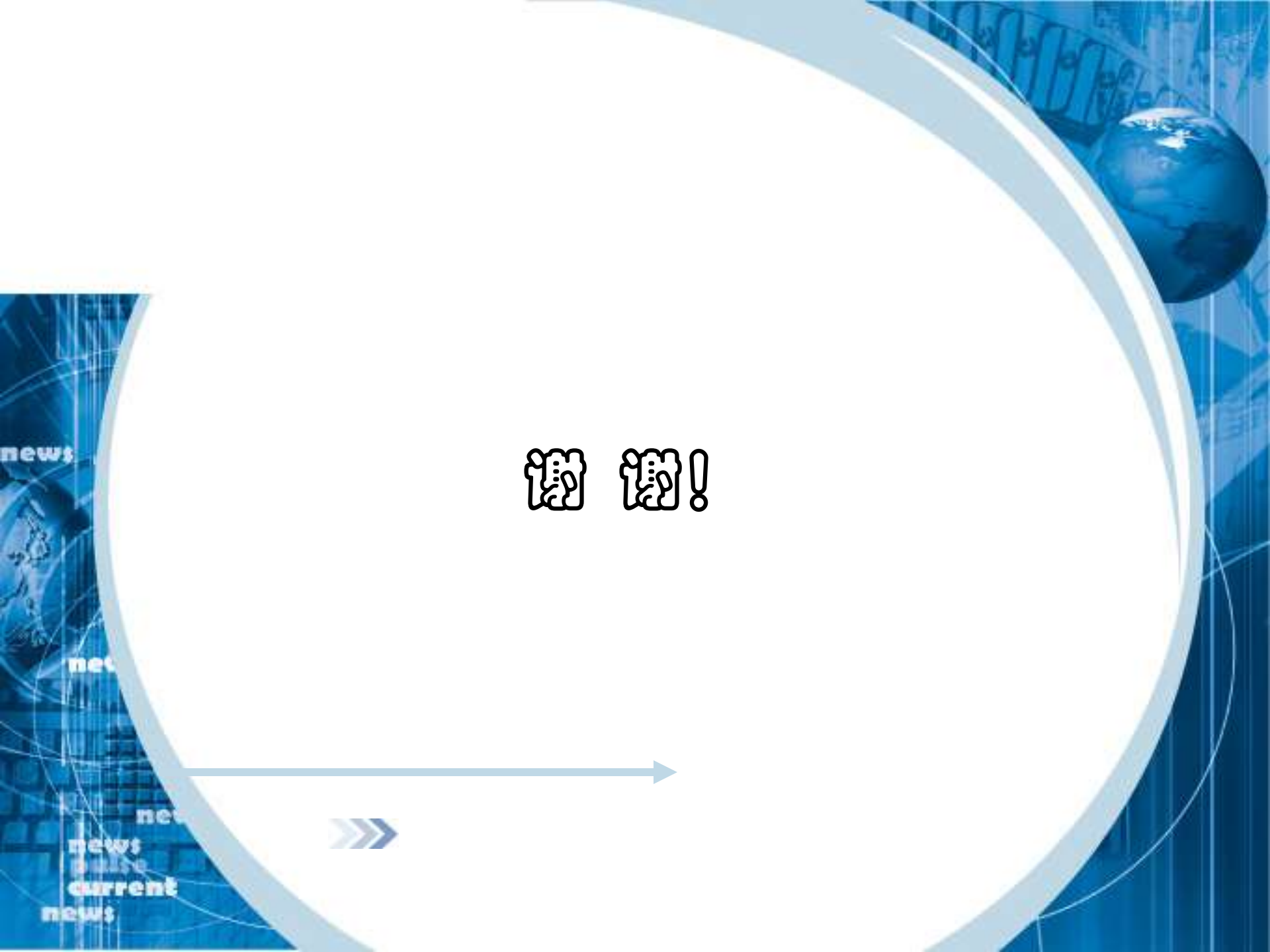
⑩nat：用于源地址转换或目标地址转换；

⑩mangle：拆解报文，做出修改，并重新封装起来；

⑩raw：关闭nat表上启用的连接追踪机制；

五链分别为：PREROUTING，INPUT，FORWARD，OUTPUT，POSTROUTING。

使用iptables命令时若不使用-t指明操作哪张表，默认操作filter表。


news
current
news