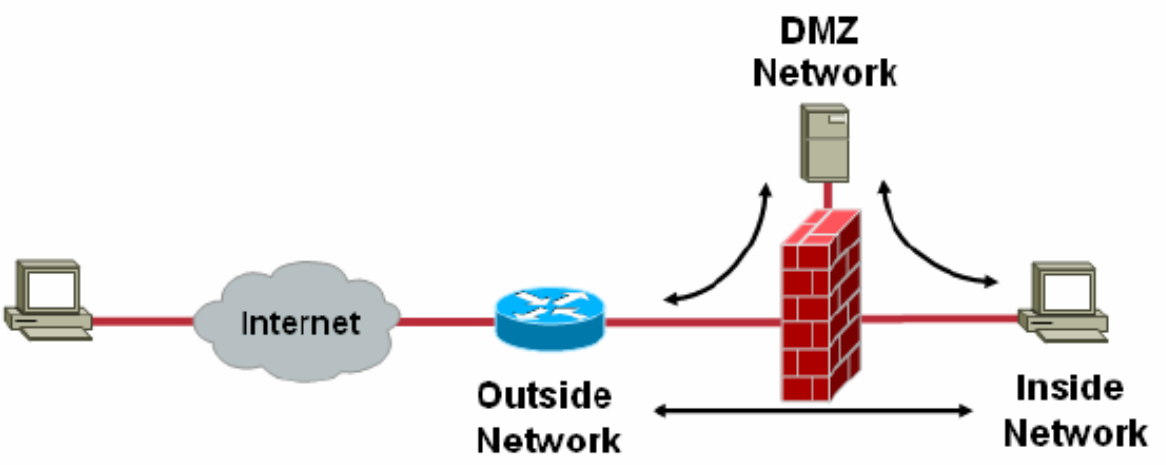
第5章 防火墙

本章内容

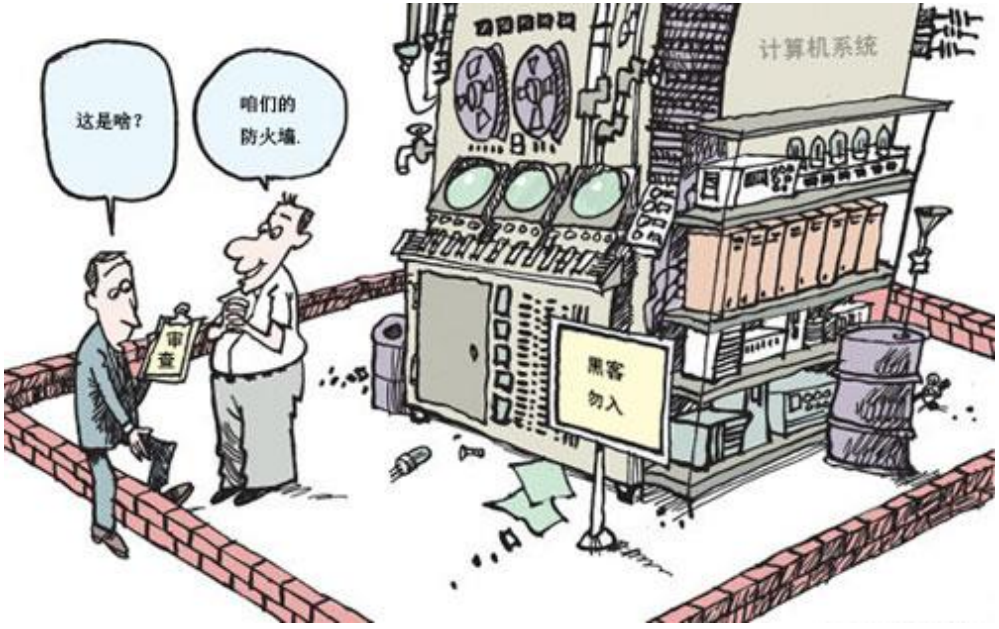
- 5.1 防火墙概述
- 5.2 防火墙分类
- 5.3 防火墙关键技术
- 5.4 防火墙体系结构
- 5.5 网络地址转换NAT

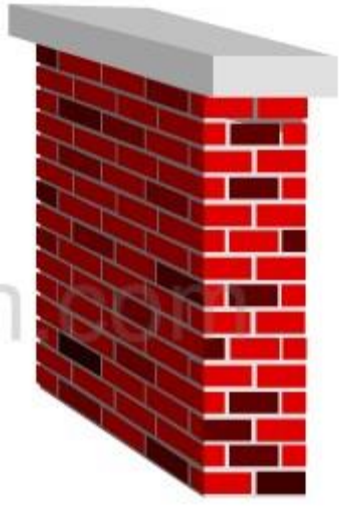
5.1 防火墙概述



什么是防火墙？

- 最初含义：当房屋还处于木制结构的时侯，人们将石块堆砌在房屋周围，以便当真正的火灾爆发时，火灾易于被控制，不会蔓延至其它房屋。这种墙被称之为防火墙。





为什么使用防火墙？

- 没有防火墙：**整个内部网络的安全性完全依赖于每个主机。**

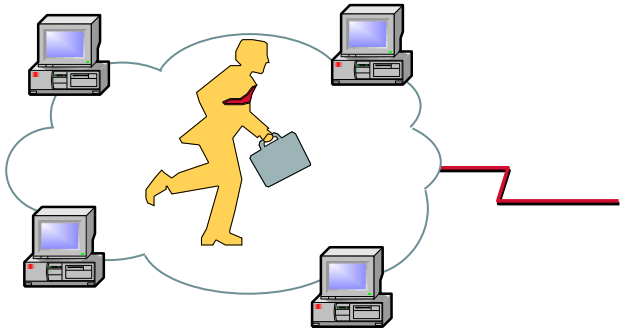
假设一个网络里有10台主机，如果你是黑客或入侵者，你会怎么做？

从安全性最差的主机入手！

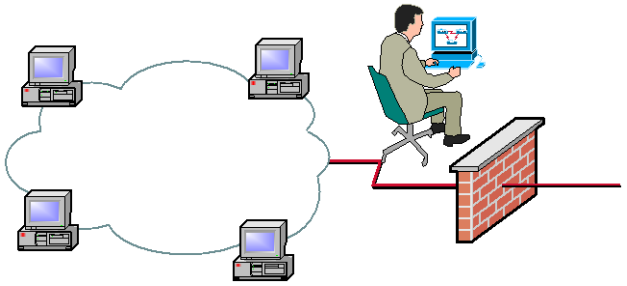
- 网络管理员要确保多台主机尽可能安全
  - 每台主机的安全由自身决定，整个系统的安全由系统中安全性最差的主机决定
  - 网络越大，维护整个网络的安全越复杂

为什么使用防火墙？

- 有防火墙：
  - 网络管理员只要集中关注防火墙
    - 注意：防火墙只是提供了一层避免错误的额外保护，并非防火墙后边的系统不再需要严格的安全措施

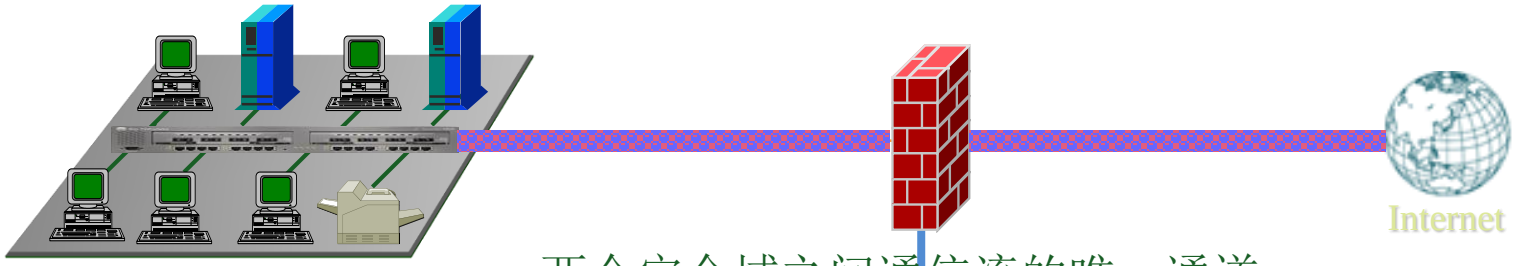


没有防火墙，分散管理，效率低下



使用防火墙，集中管理，高效率

防火墙定义



两个安全域之间通信流的唯一通道

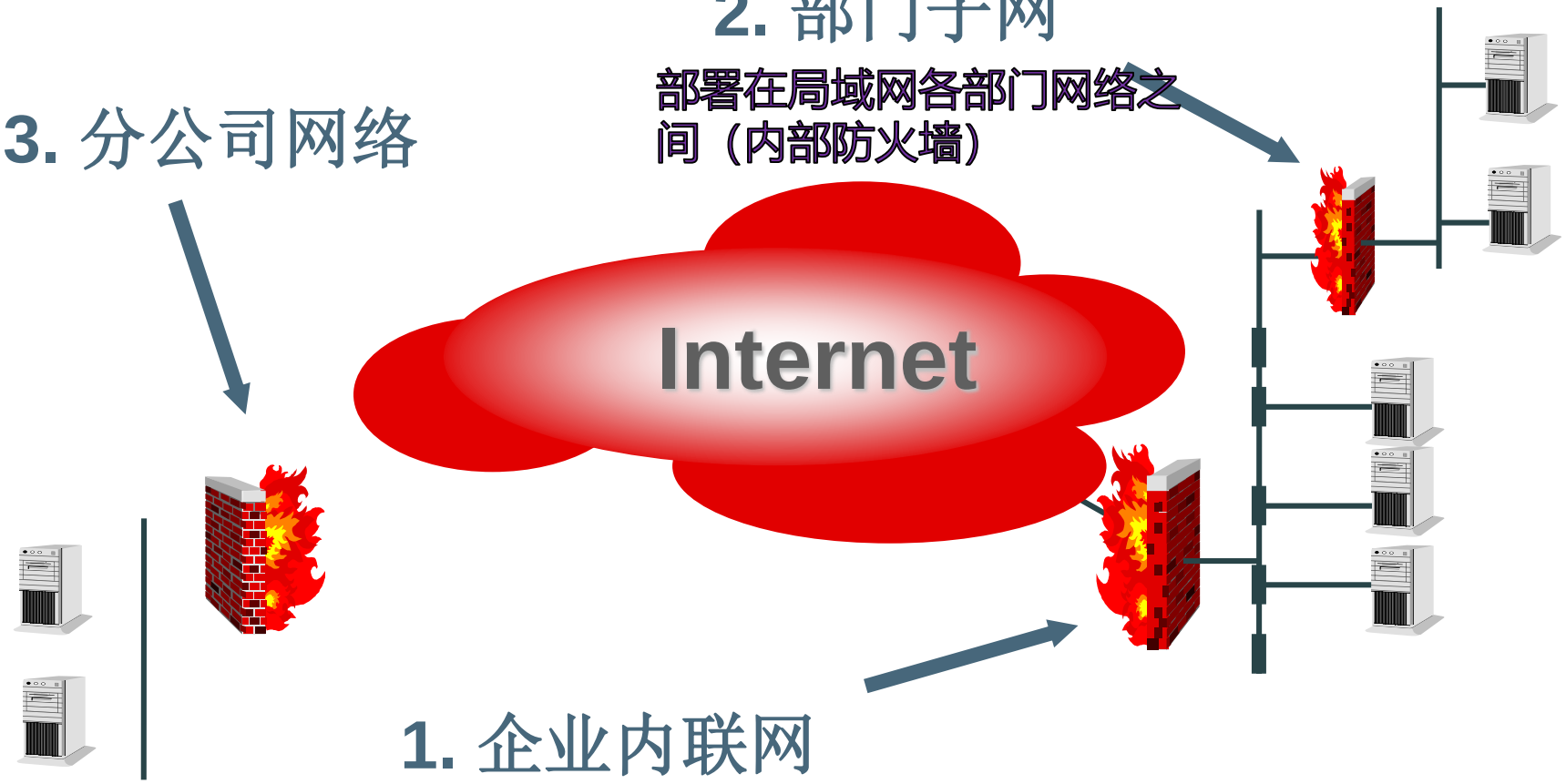
Source	Destination	Permit	Protocol
Host A	Host C	Pass	TCP
Host B	Host C	Block	UDP

根据访问控制规则决定进出网络的行为

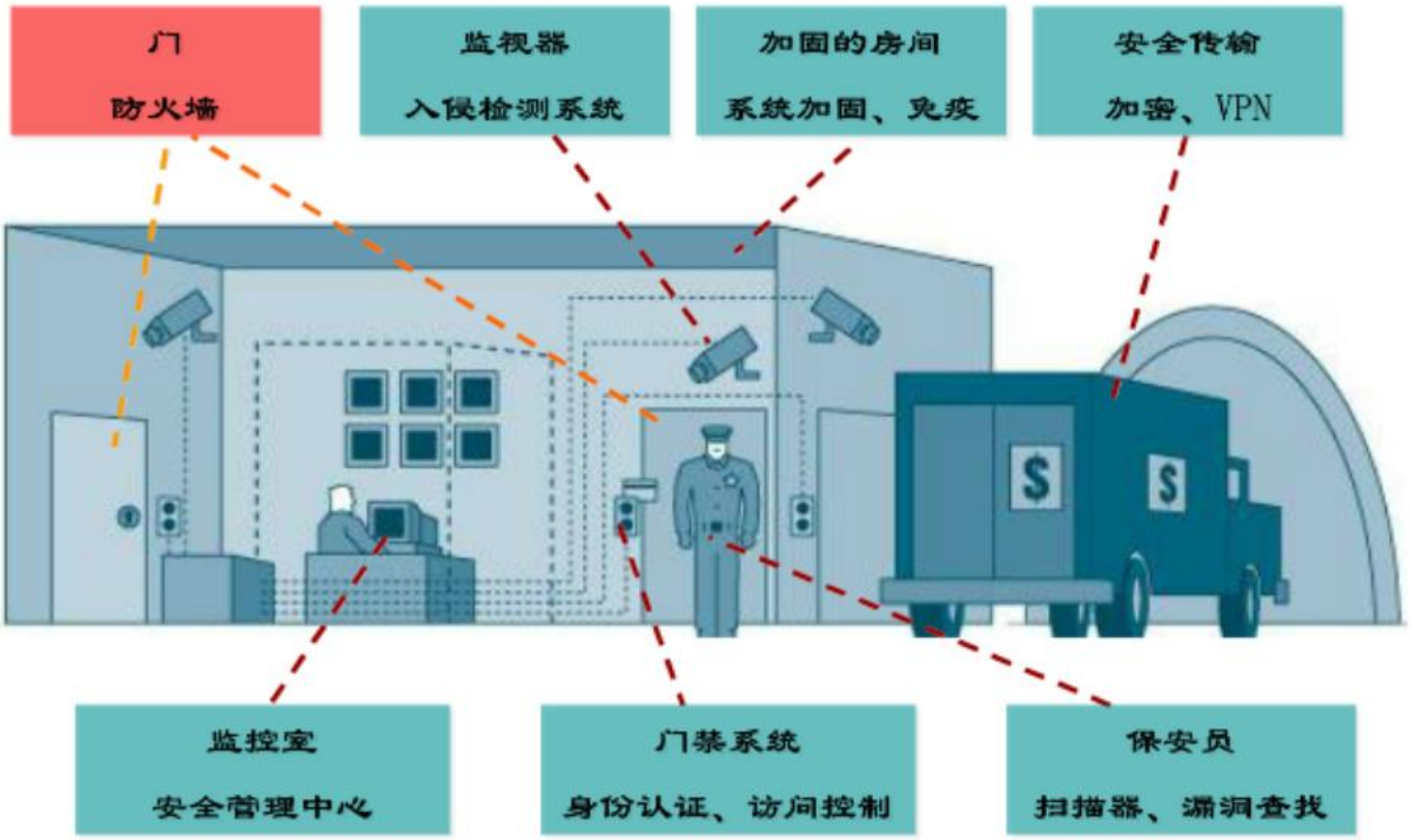
概念：一种高级访问控制设备，即由软件和硬件组成的系统，置于不同的网络安全域之间的一系列部件的组合，它是不同网络安全域间通信流的唯一通道，能根据企业有关的安全政策控制（允许、拒绝、监视、记录）进出网络的访问行为。防火墙默认阻断一切！

防火墙的部署

防火墙可以位于：
两/多个具有不同安全性要求的网络的互联之处，保护安全性要求高的网络



防火墙在安全体系中的位置



漫画之网络安全技术

漫画之网络安全技术

漫画之网络安全技术

漫画之网络安全技术

漫画之网络安全技术

漫画之网络安全技术

防火墙的功能

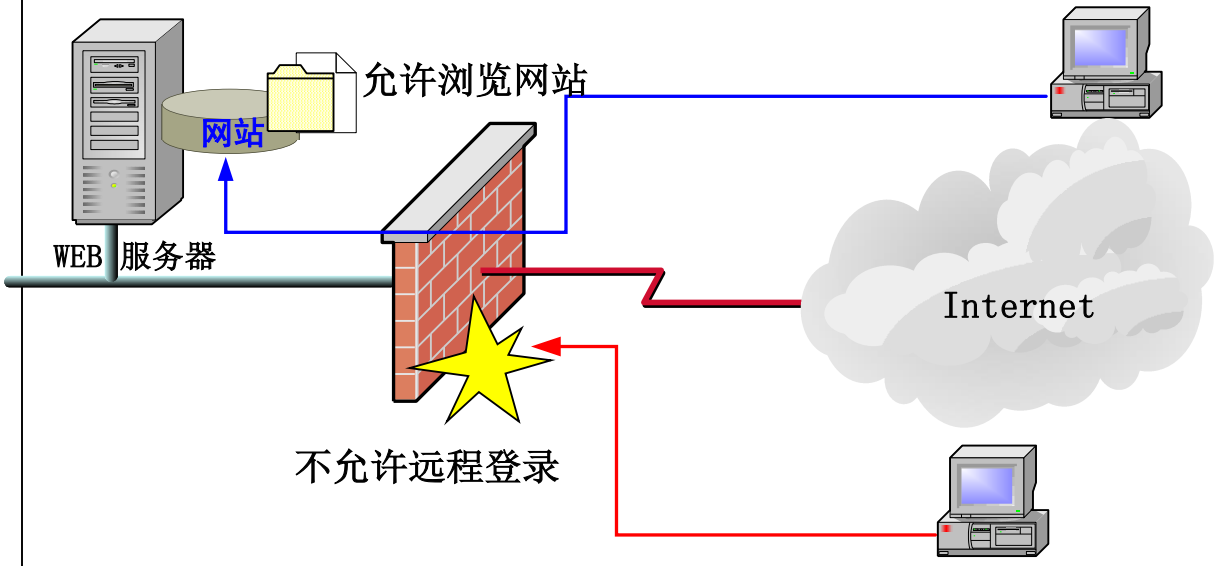
- 1. 防火墙能做什么
- 2. 防火墙不能做什么

1. 防火墙能做什么

- 防火墙并不能为网络防范一切，也不应该把它作为对所有安全问题的一个最终解决方案，所以懂得哪些工作是防火墙能做的非常重要：
  - （1）实现安全策略
  - （2）创建一个阻塞点
  - （3）记录网络活动
  - （4）限制网络暴露

（1）实现安全策略

安全策略对哪些人和哪些行为被允许做出规定。如一个常见的安全策略是允许任何人访问公司服务器上的Web站点，但是不允许telnet登陆到服务器上。



（1）实现安全策略

防火墙可以使用的两种基本的安全策略：

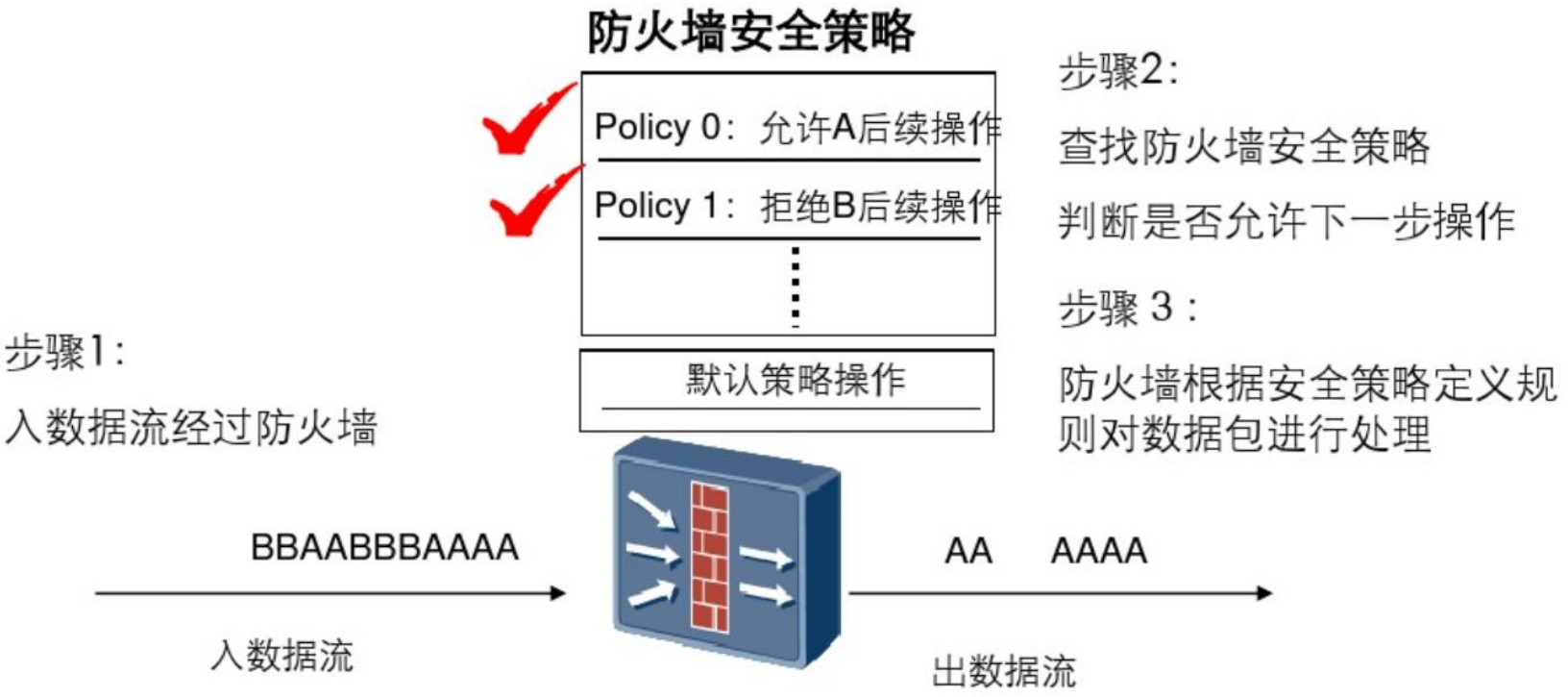
(a) 限制控制策略：一切未被允许的就是禁止的

- 防火墙应该封锁所有的信息流，然后逐项开放希望提供的服务
- 优点：安全性好，实用性强
- 缺点：用户所能使用的服务范围受到严格限制

(b) 宽松控制策略：一切未被禁止的就是允许的

- 防火墙应该转发所有的信息流，然后逐项屏蔽有害的服务
- 优点：灵活，可以为用户提供更多服务
- 缺点：安全可靠性不高

防火墙安全策略的原理

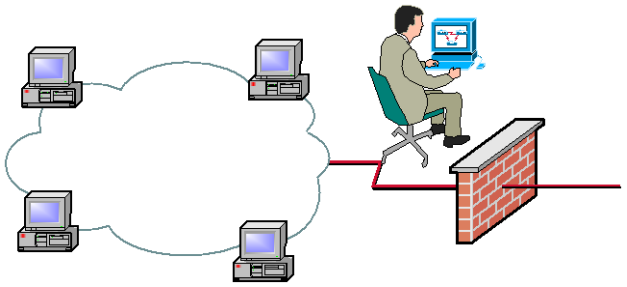


- 防火墙安全策略作用：

根据定义的规则对经过防火墙的流量进行筛选，并根据关键字确定筛选出的流量如何进行下一步操作。

（2）创建一个阻塞点

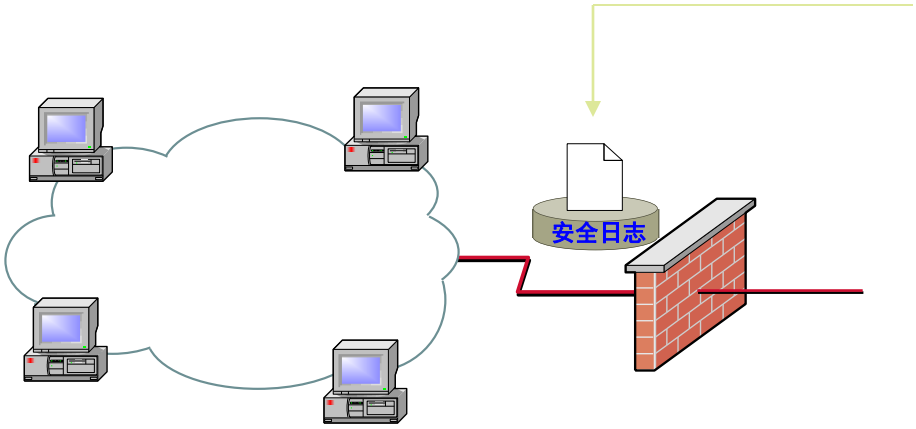
没有防火墙，分散管理，效率低下



使用防火墙，集中管理，高效率

防火墙在一个公司私有网络和分网间建立一个检查点。这种实现要求所有的流量都要通过这个检查点。在该检查点防火墙设备就可以监视，过滤和检查所有进来和出去的流量。网络安全产业称这些检查点为阻塞点。

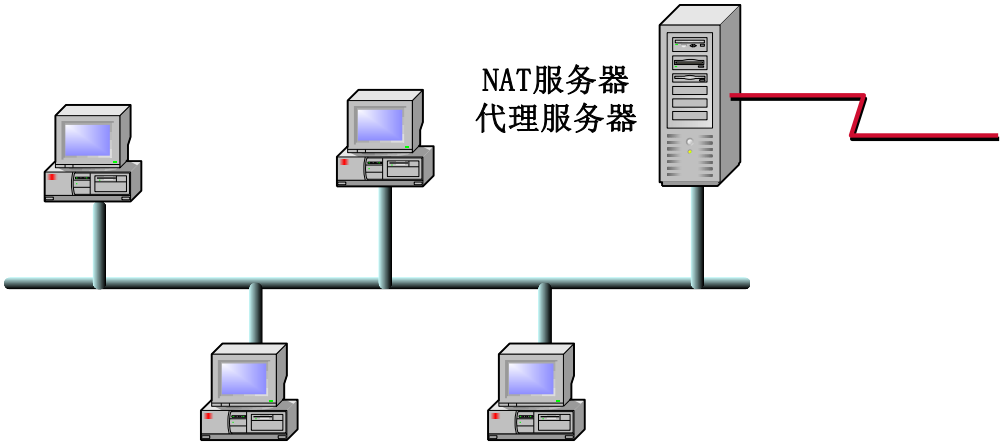
（3）记录网络活动



例如，通过查看安全日志，管理员可以找到非法入侵的相关纪录，从而可以做出相应的措施。

防火墙还能够监视并记录网络活动，并且提供警报功能。通过防火墙记录的数据，管理员可以发现网络中的各种问题。

（4）限制网络暴露



例如，防火墙的NAT功能可以隐藏内部的IP地址；代理服务器防火墙可以隐藏内部主机信息。

防火墙在你的网络周围创建了一个保护的边界。并且对于公网隐藏了你内部系统的一些信息以增加保密性。当远程节点侦测你的网络时，他们仅仅能看到防火墙。远程设备将不会知道你内部网络的布局以及都有些什么。

2. 防火墙不能做什么

- 除了懂得防火墙能保护什么非常重要外，懂得防火墙不能保护什么也是同等重要：

① 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；

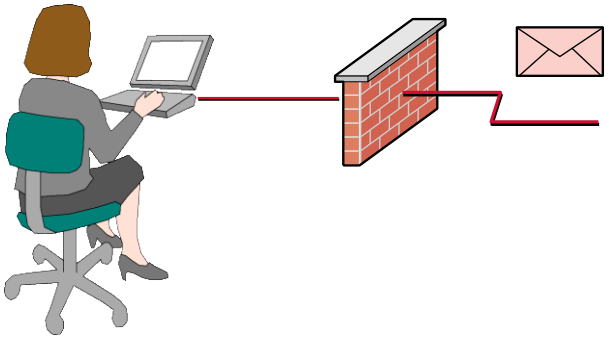
② 防火墙不能防范恶意的内部人员侵入；

③ 防火墙不能防止感染了病毒的软件或文件的传输；

④ 防火墙不能防范不断更新的攻击方式，不能防止策略配置不当或错误配置引起的安全威胁；

⑤ 防火墙不能防止数据驱动式攻击

2. 防火墙不能做什么



例如，员工接收了一封包含木马的邮件，木马是以普通程序的形式放在了附件里，防火墙不能避免该情况的发生。

总体来说，除了不能防止物理故障等错误外，防火墙本身并不能防范经过授权的东西，如内部员工的破坏等。

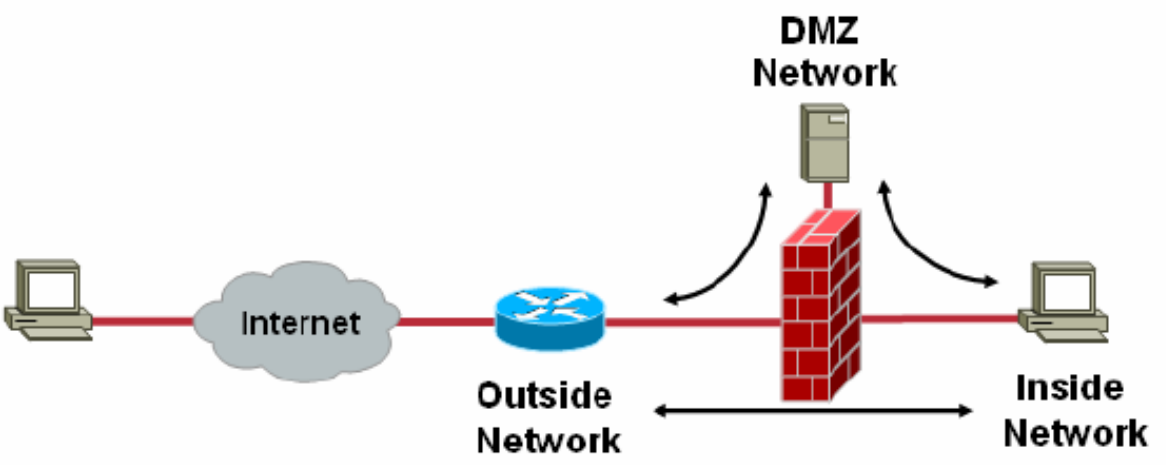
防火墙的局限性

- 网络的安全性通常是以网络服务的开放性和灵活性为代价的。
- 防火墙的使用也会削弱网络的功能：

① 由于防火墙的隔离作用，在保护内部网络的同时使它与外部网络的信息交流受到阻碍；

② 由于在防火墙上附加各种信息服务的代理软件，增大了网络管理开销，还减慢了信息传输速率，在大量使用分布式应用的情况下，使用防火墙是不切实际的。

5.2 防火墙分类



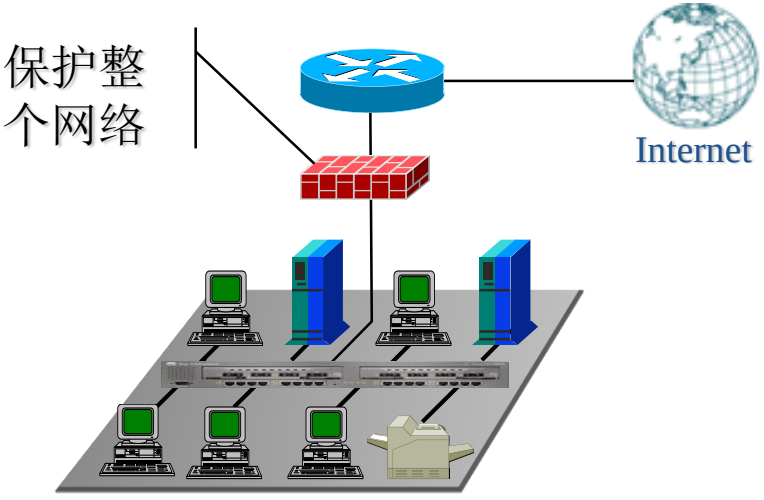
防火墙的分类

按形态分类

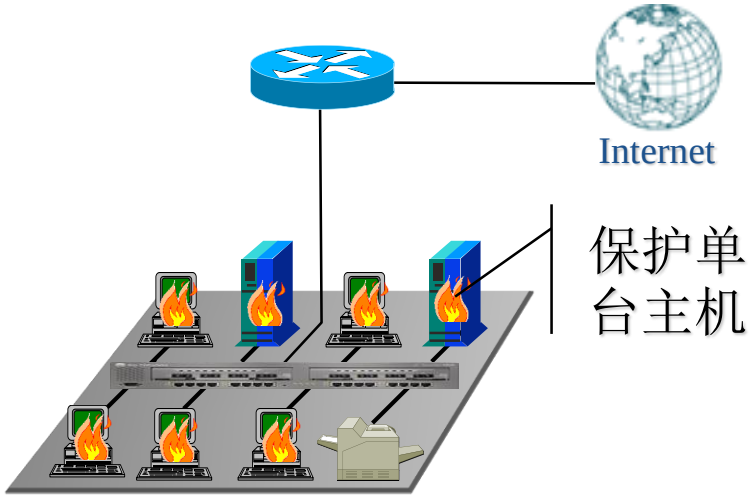
软件防火墙

硬件防火墙

按保护对象分类



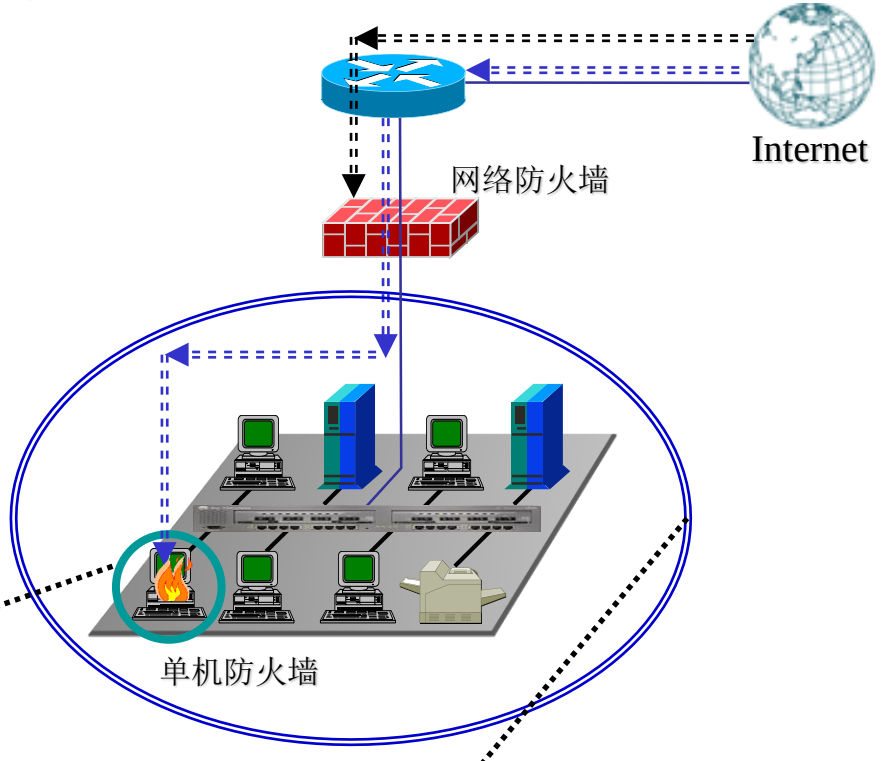
网络防火墙



单机防火墙

单机防火墙&网络防火墙

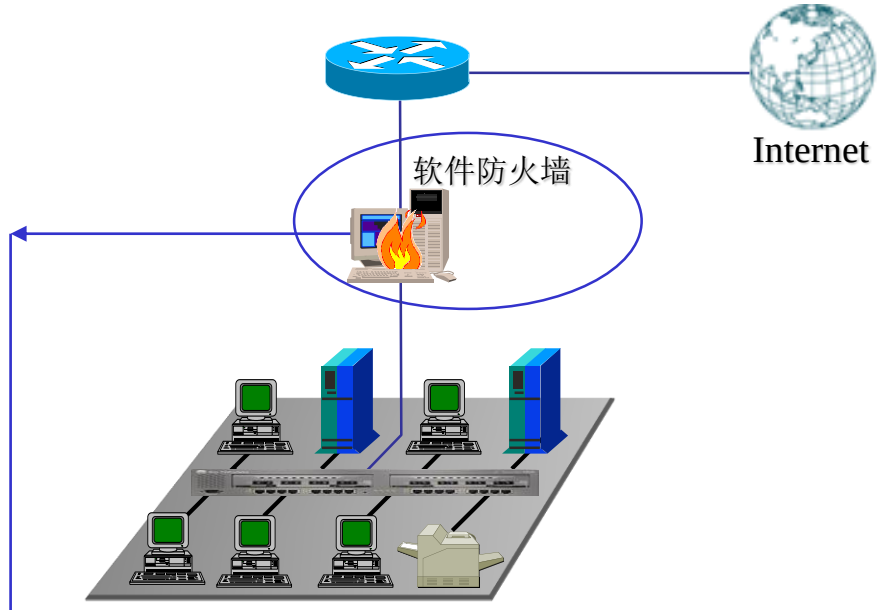
结论:单机防火墙是网络防火墙的有益补充，但不能代替网络防火墙为内部网络提供强大的保护功能。



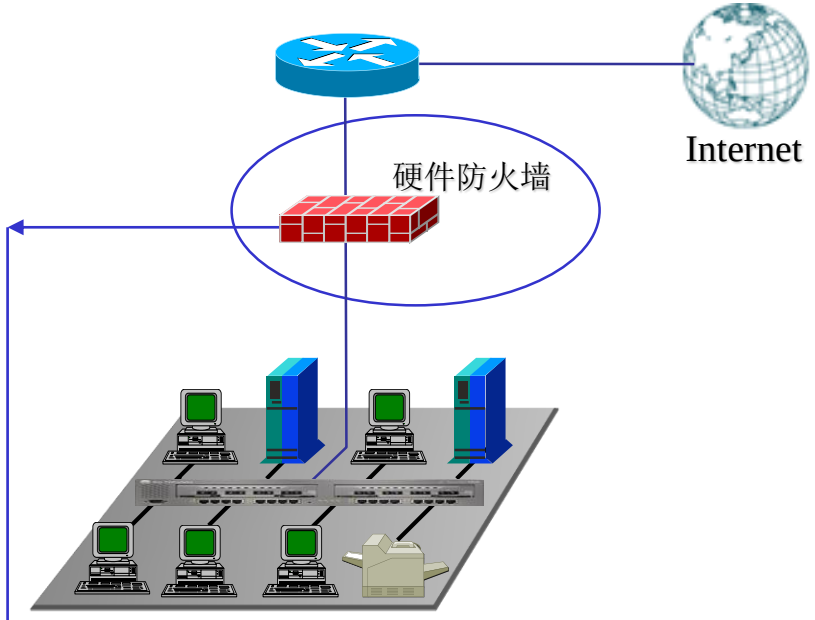
保护单台主机
安全策略分散
安全功能简单
普通用户维护
安全隐患较大
策略设置灵活

保护整个网络
安全策略集中
安全功能复杂多样
专业管理员维护
安全隐患小
策略设置复杂

硬件防火墙&软件防火墙

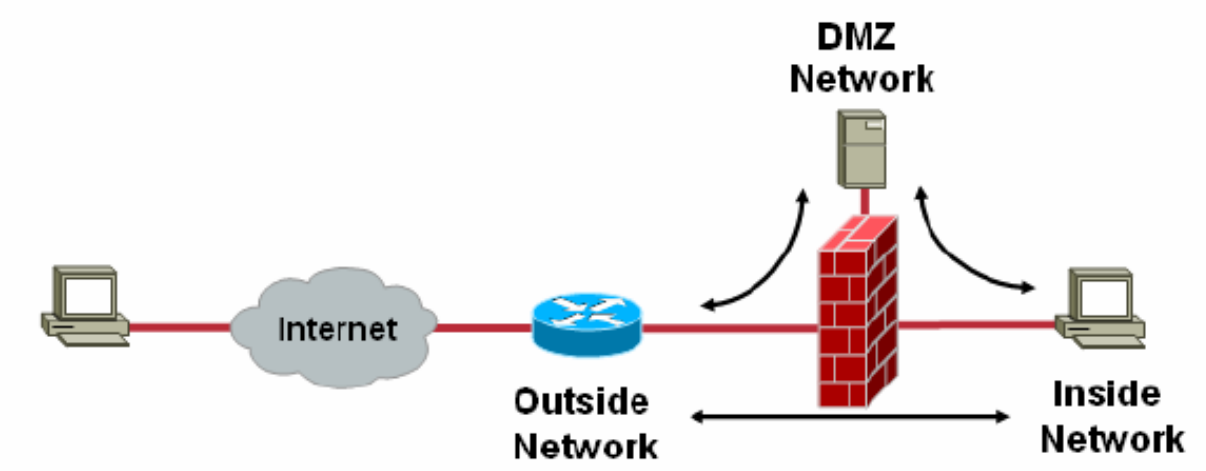


需要准备额外的OS平台
安全性依赖低层的OS
网络适应性弱（主要以路由模式工作）
稳定性高
软件分发、升级比较方便



硬件+软件，不用准备额外的OS平台
安全性完全取决于专用的OS
网络适应性强（支持多种接入模式）
稳定性较高
升级、更新不太灵活

5.3 防火墙关键技术



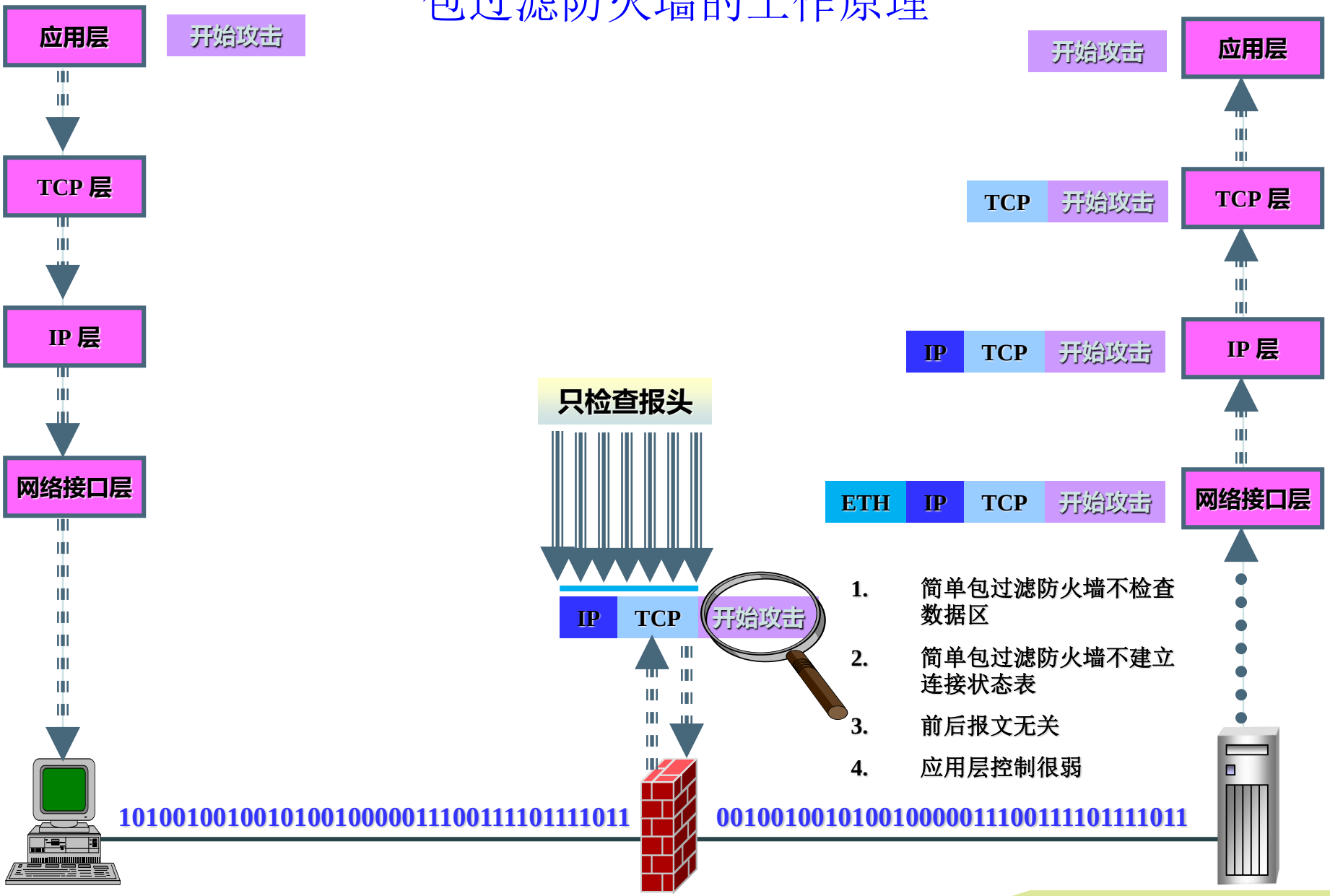
防火墙关键技术

- 包过滤技术
- 状态检测技术
- 代理服务器

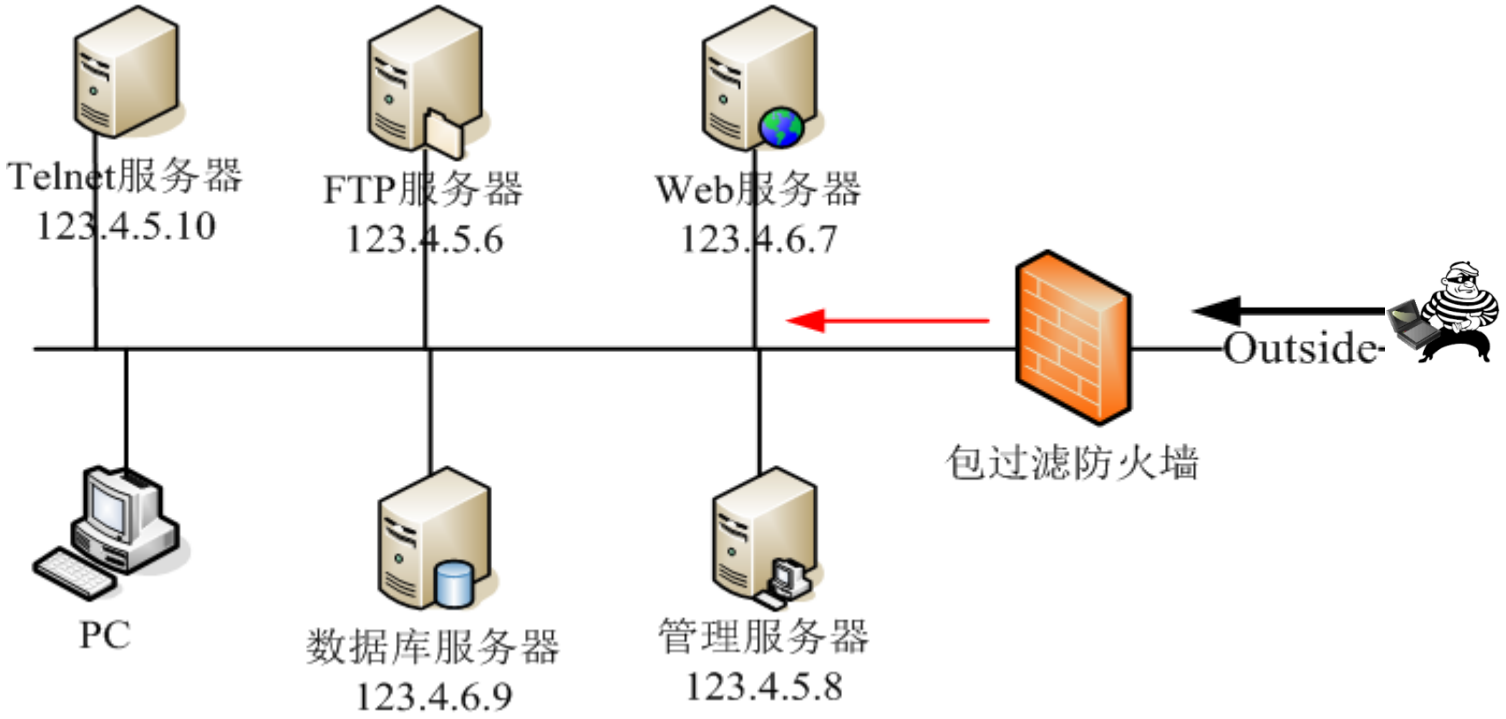
❖1. 包过滤技术

- 数据包过滤(Packet Filtering)技术在网络层和传输层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，即访问控制表(Access Control List，ACL)
- 包过滤防火墙分为静态包过滤、动态包过滤防火墙
- 包检查器并不是检查数据包的所有内容，只检查报头（IP、TCP头部），通常只检查下列几项：
  - IP源地址
  - IP目标地址
  - TCP或UDP的源端口号
  - TCP或UDP的目的端口号
  - 协议类型
  - ICMP消息类型
  - TCP报头中的ACK位
  - TCP的序列号、确认号
  - IP校验和

包过滤防火墙的工作原理



过滤规则设置



方向	类型	源地址	目的地址	源端口	目的端口	动作
inside	tcp	*	123.4.5.6	any	21	permit
inside	tcp	*	123.4.6.7	any	80	permit
inside	udp	129.6.1.2	123.4.5.8	any	161	permit
*	*	*	*	*	*	deny

优点

- 处理数据包的速度比较快(与代理服务器相比)
  - 在流量适中并定义较少过滤规则时，路由器的性能几乎不受影响
- 实现包过滤几乎不再需要费用
  - 标准的路由器软件包含数据包过滤功能
- 包过滤路由器对用户和应用来讲是透明的
  - 不必对用户进行特殊的培训
  - 不必在每台主机上安装特定的软件
  - 用户不用改变客户端程序或改变自己的行为

缺点

- 包过滤防火墙的维护比较困难
  - 定义数据包过滤器比较复杂，网络管理员需要对各种Internet服务、包头格式、以及每个域的意义有非常深入的理解；
- 随着过滤规则的增加，吞吐量会下降
  - 在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大地影响；
- 很容易受到“地址欺骗型”攻击
  - 大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证；

问题：

- 比如我们要允许内网用户访问公网的WEB服务，来看看普通包过滤防火墙是怎样处理的呢?

那首先我们应该建立一条类似下图所示的规则：

动作	源地址	源端口	目标地址	目标端口	方向(此栏为备注)
允许	*	*	*	80	出

但这就行了吗?

显然是不行的，因为这只是允许我向外请求WEB服务，但WEB服务响应我的数据包怎么进来呢?

问题：

所以还必须建立一条允许相应响应数据包进入的规则：

动作	源地址	源端口	目标地址	目标端口	方向(此栏为备注)
允许	*	*	*	80	出
允许	*	80	*	1024-655 35	进

需要注意的是，端口并不是一一对应的。比如你的电脑作为客户机访 问一台WWW服务器时，WWW服务器使用“80”端口与你的电脑通信，但你的电脑则可能使用“3457”这样的端口。

问题：

- 想一想这是多么危险的，因为入站的高端口全开放了，而很多危险的服务也是使用的高端口啊，比如微软的终端服务/远程桌面监听的端口就是3389，当然对这种固定的端口还好说，把进站的3389封了就行，但对于同样使用高端口但却是动态分配端口的RPC服务就没那么容易处理了，因为是动态的，你不便封住某个特定的RPC服务。

为了防止这种开放高端口的风险，于是就有了**状态检测技术**。

❖2. 状态检测技术

- 由动态**包过滤防火墙**演变而来，工作在**传输层**，使用各种**状态表（state tables）**来追踪活跃的TCP会话，它能够根据连接状态信息动态地建立和维持一个连接状态表，并且这个把这个连接状态表用于后续报文的处理。
- 状态检测技术一般的检查点有：
  - 检查数据包是否是一个已经建立并且正在使用的通信流的一部分。
  - 如果数据包和连接表的各项都不匹配，那么防火墙就会检测数据包是否与它所配置的规则集相匹配。
  - 在检测完毕后，防火墙会根据路由转发数据包，并且会在连接表中为此次对话**创建或者更新**一个连接项
  - 防火墙通常对TCP包中被设置的FIN位进行检测、通过**会话超时**设置决定何时从连接表中删除某连接项。

问题：

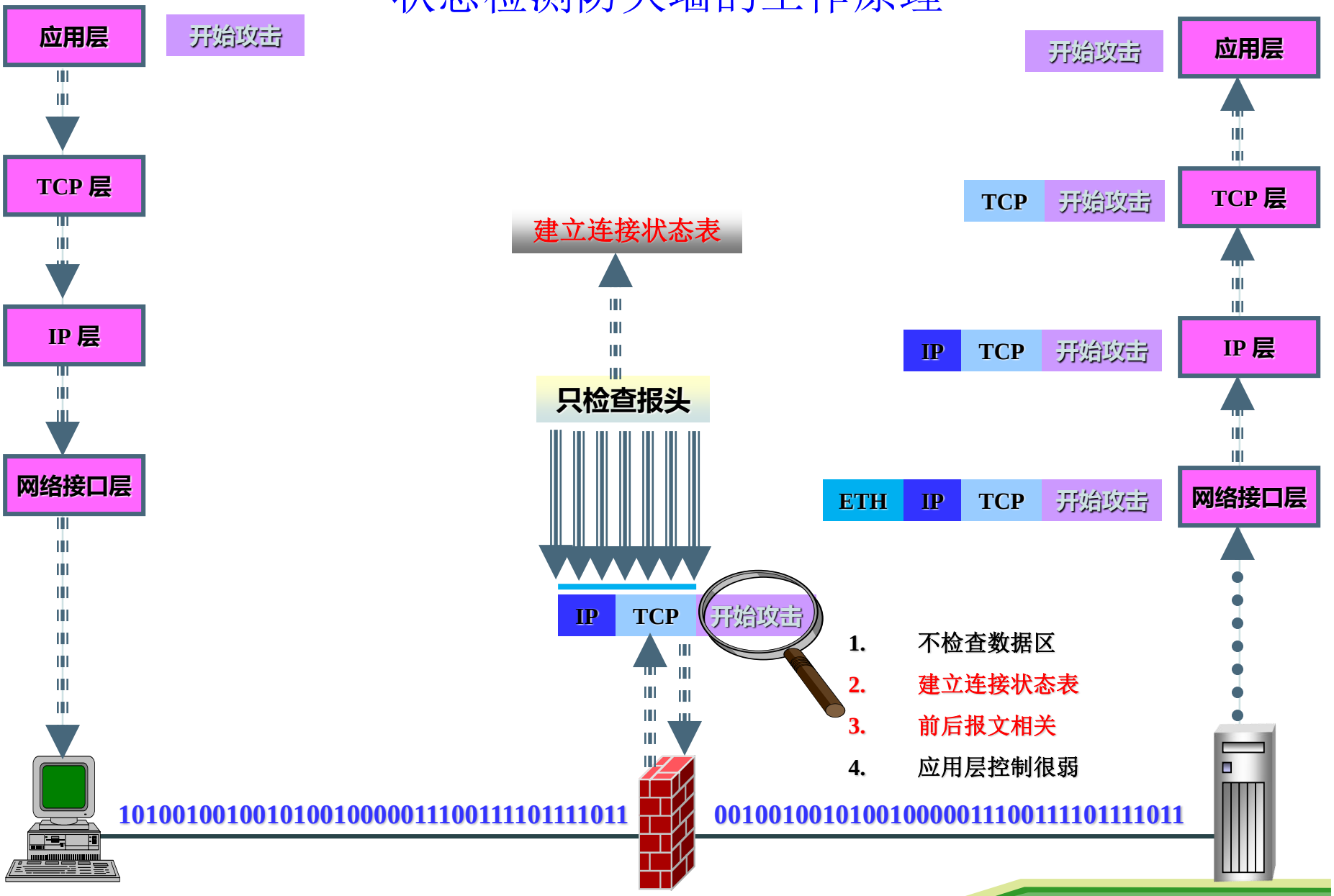
- 比如我们要允许内网用户访问公网的WEB服务，来看看状态检测过滤防火墙是怎样处理的呢？

❖ 状态检测防火墙只需要建立好一条如下规则：

动作	源地址	源端口	目标地址	目标端口	方向(此栏为备注)
允许	*	*	*	80	出

当内部网络的数据包到达防火墙时，状态检测引擎如果检测到这是一个发起连接的初始数据包(由SYN标志)，然后它就会把这个数据包中的信息与防火墙规则作比较，如果有相应规则允许，数据包外出并且在状态表中新建一条会话，通常这条会话会包括此连接的源地址、源端口、目标地址、目标端口、连接时间等信息，对于TCP连接，它还应该会包含序列号和标志位等信息。当后续数据包到达时，如果这个数据包不含SYN标志，也就是说这个数据包不是发起一个新的连接时，状态检测引擎就会直接把它的信息与状态表中的会话条目进行比较，如果信息匹配，就直接允许数据包通过，这样不再去接受规则的检查，提高了效率。如果信息不匹配，数据包就会被丢弃或连接被拒绝，并且每个会话还有一个超时值，过了这个时间，相应会话条目就会被从状态表中删除掉。

状态检测防火墙的工作原理



2. 状态检测防火墙

优点

- 更高的安全性（“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UDP ）

缺点

- 不能对应用层数据进行控制
- 不能产生高层日志
- 配置复杂

❖3、代理服务器技术

◆ 应用代理（Application Proxy）也称为应用层网关（Application Gateway）

◆ 工作在应用层，其核心是代理进程

◆ 每一种应用对应一个代理进程，实现监视和控制应用层通信流

◆ **自适应代理防火墙：**在每个连接通信的开始仍然需要在应用层接受检测，而后面的包可以经过安全规则由自适应代理程序自动的选择是使用包过滤还是代理

应用代理检查信息

❖3、代理服务器技术

优点

- 在应用层检查的一个重要作用是可以扫描数据包的内容，对数据包的检测能力比较强，这些内容是包过滤技术不能控制的。
- 代理完全控制会话，可以提供很详细的日志和安全审计功能
- 可以隐藏内部网的IP地址，保护内部主机免受外部主机的进攻

  （如何隐藏内部网的IP地址?）
- 代理服务可以提供各种用户身份认证手段，加强服务的安全性。

缺点

- 最大缺点是要求用户改变自己的行为，或者在访问代理服务的每个系统上安装特殊的软件
- 应用代理型防火墙的处理速度相对比较慢，在访问数据流量大的情况下，代理技术会增加访问的延迟。
- 每一种应用服务必须设计一个代理软件模块进行安全控制，并且应用升级时，一半代理服务程序也要升级

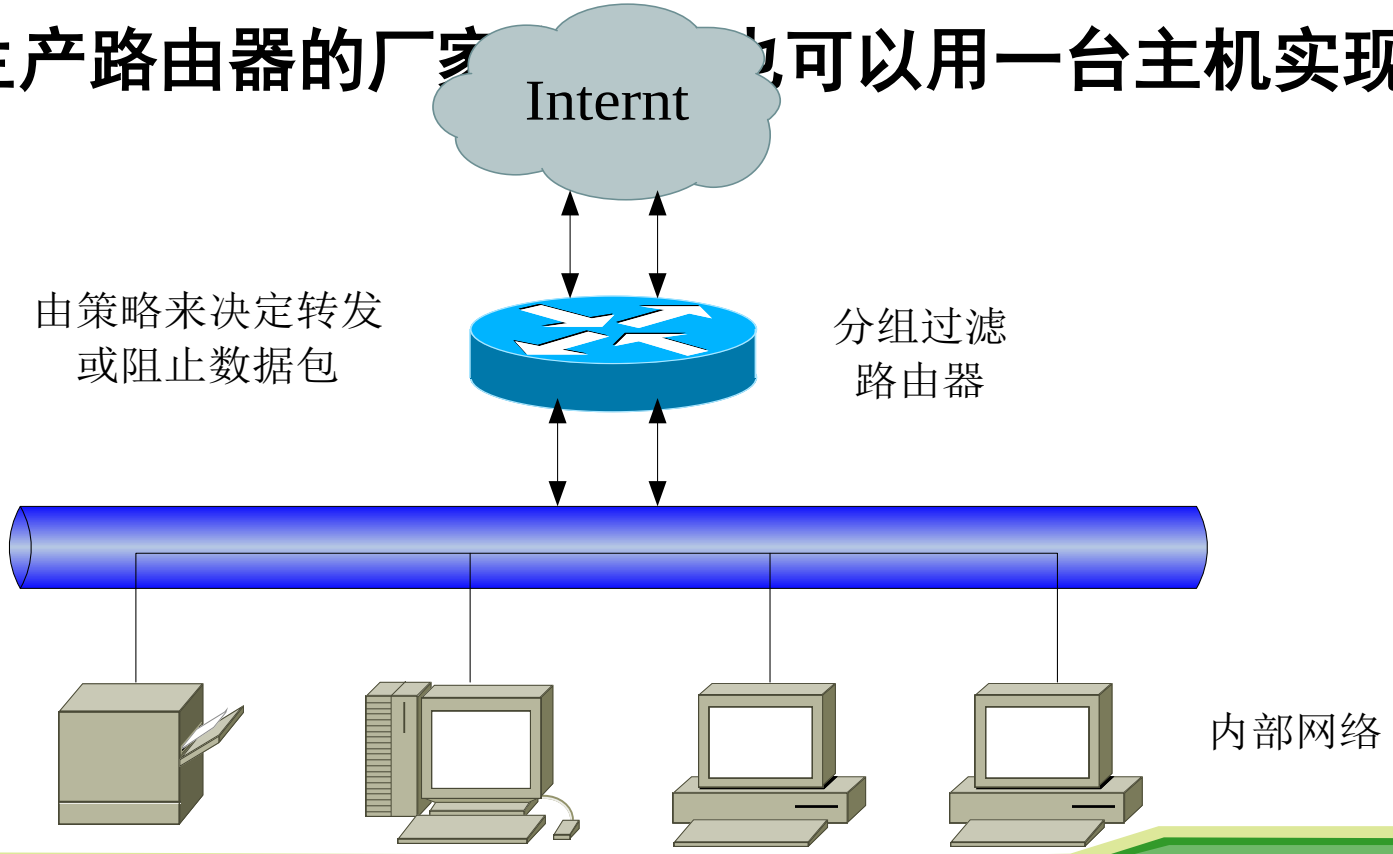
❖防火墙类型的对比

性能 / 类型	综合安全性	网络层保护	应用层保护	应用层透明	整体性能	处理对象
简单包过滤防火墙	★	★★★	★	★★★★★	★★★★	单个数据包报头
状态检测包过滤防火墙	★★	★★★★★	★★	★★★★★	★★★★★	单个数据包报头 一次会话
应用代理防火墙	★★★	★	★★★★★	★	★	单个数据包数据

5.4 防火墙体系结构

1　分组过滤防火墙

- 防火墙最简单的形式是分组过滤防火墙，一个分组过滤防火墙可以是一台有能力过滤分组数据的路由器，由生产路由器的厂家[illegible]也可以用一台主机实现。



1　分组过滤防火墙

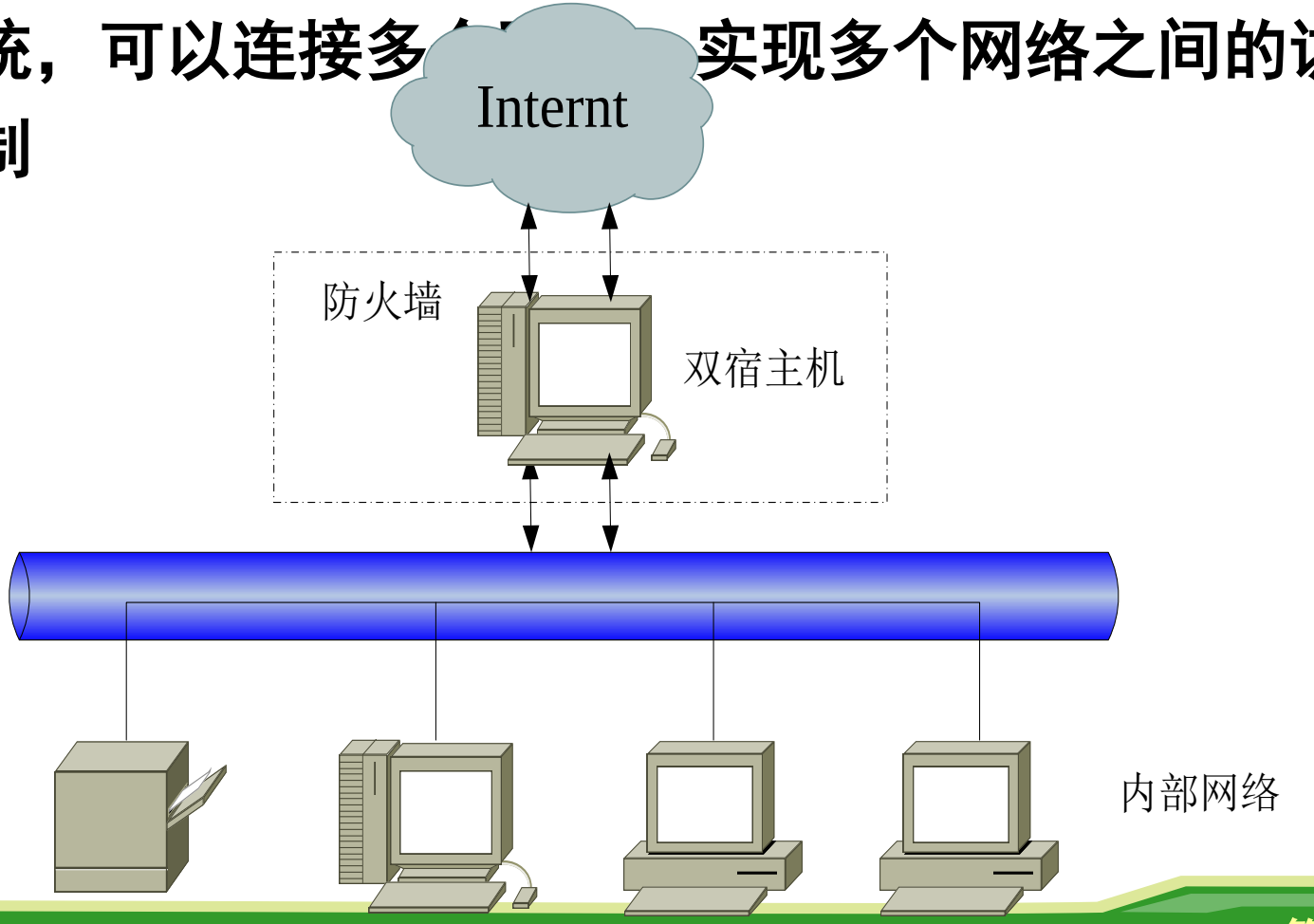
- 作为内外网连接的唯一通道，要求所有的报文都必须在此通过检查。
- 通过在分组过滤路由器上安装基于IP层的报文过滤软件，就可利用过滤规则实现报文过滤功能。

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。

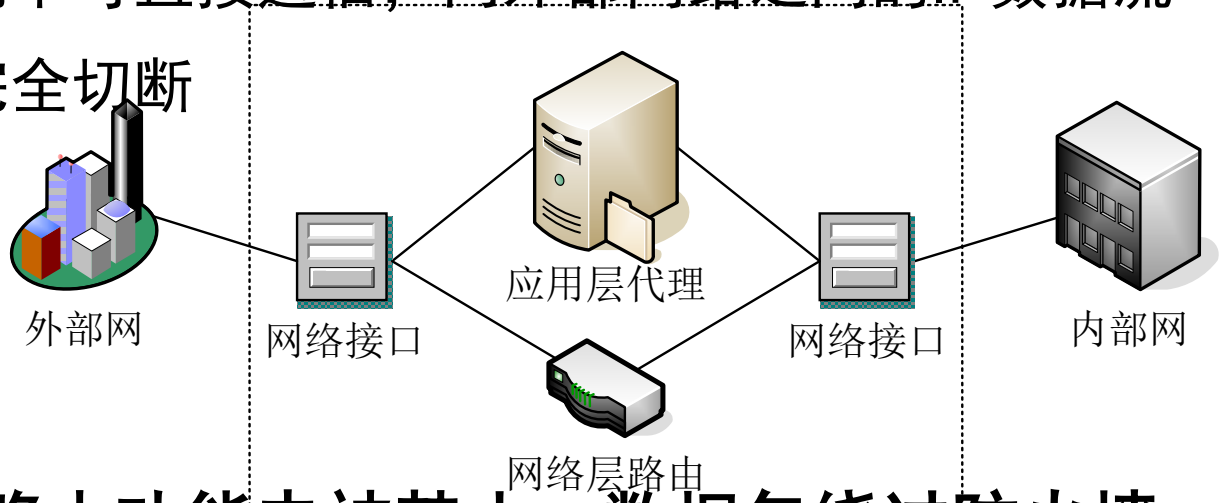
2　双宿主机防火墙

- 双宿/多宿主机：有两个或多个网络接口的计算机系统，可以连接多[illegible]实现多个网络之间的访问控制



2　双宿主机防火墙

- 特点：
  - IP层通信被阻止
  - 双宿主机内外的网络均可与双宿主机实时通信
  - 内外网络之间不可直接通信，内外部网络之间的IP数据流被双宿主机完全切断



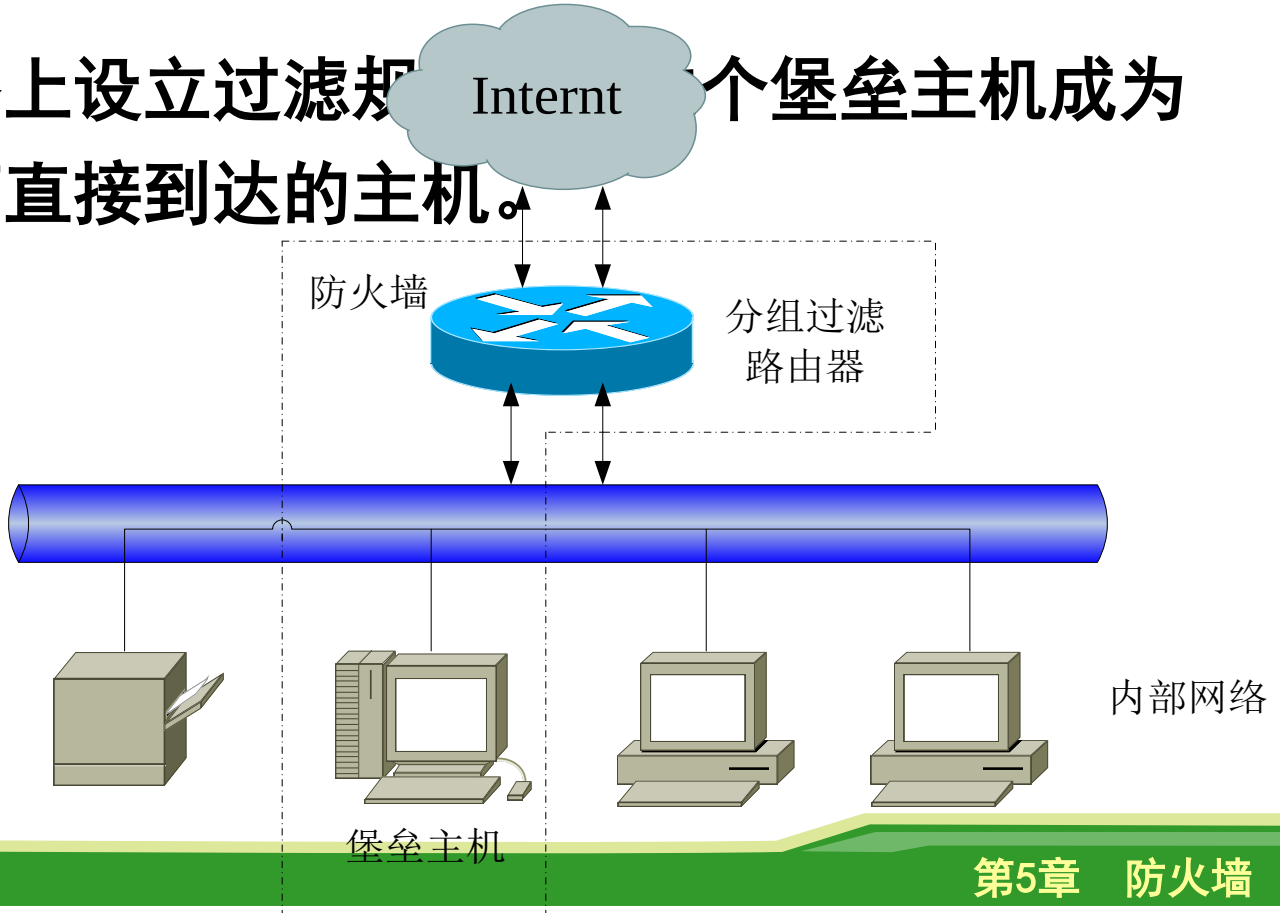
- 上图：网络层路由功能未被禁止，数据包绕过防火墙

2　双宿主机防火墙

- **优缺点：**
  - 双宿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

3　屏蔽主机防火墙

- 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[illegible]个堡垒主机成为从外部唯一可直接到达的主机。



3 屏蔽主机防火墙

❖ 过滤路由器

- 连接Internet和内部网络，它是内部网络的第一道防线
- 过滤路由器需要进行适当的配置，**使所有的外部连接被路由到堡垒主机上**
- 过滤路由器的重要性：
  - 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，否则如果路由表遭到破坏，数据包就不会被路由到堡垒主机上，使堡垒主机被绕过

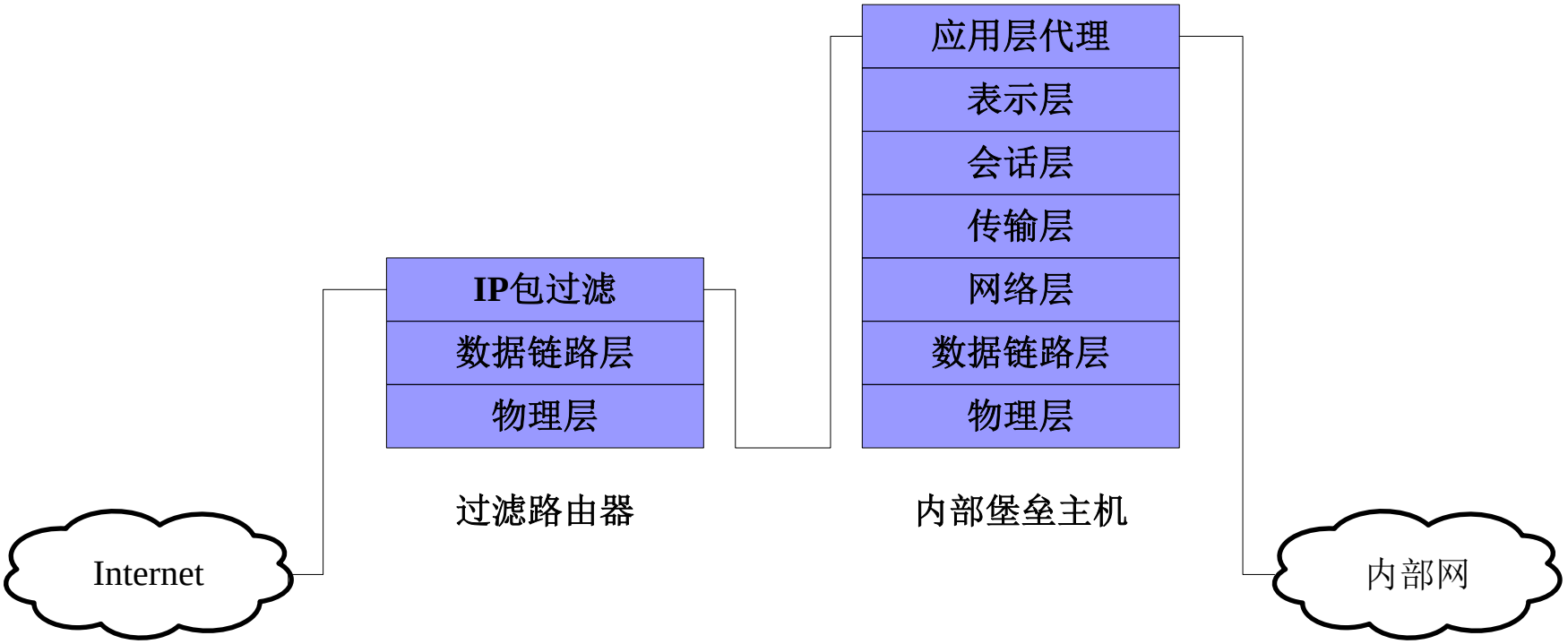
3 屏蔽主机防火墙

❖ 堡垒主机(Bastion Host)

- 位于**内部网络**，是一台安全性很高的主机，其上没有任何入侵者可以利用的工具，不能作为黑客进一步入侵的基地
- 堡垒主机上一般安装的是**代理服务器程序**，即外部网络访问内部网络的时候，首先经过外部路由器的过滤，然后通过代理服务器代理后才能进入内部网络
- 堡垒主机在应用层对客户的请求做判断，允许或禁止某种服务。如果该请求被允许，堡垒主机就把数据包发送到某一内部主机或屏蔽路由器上，否则抛弃该数据包

3　屏蔽主机防火墙

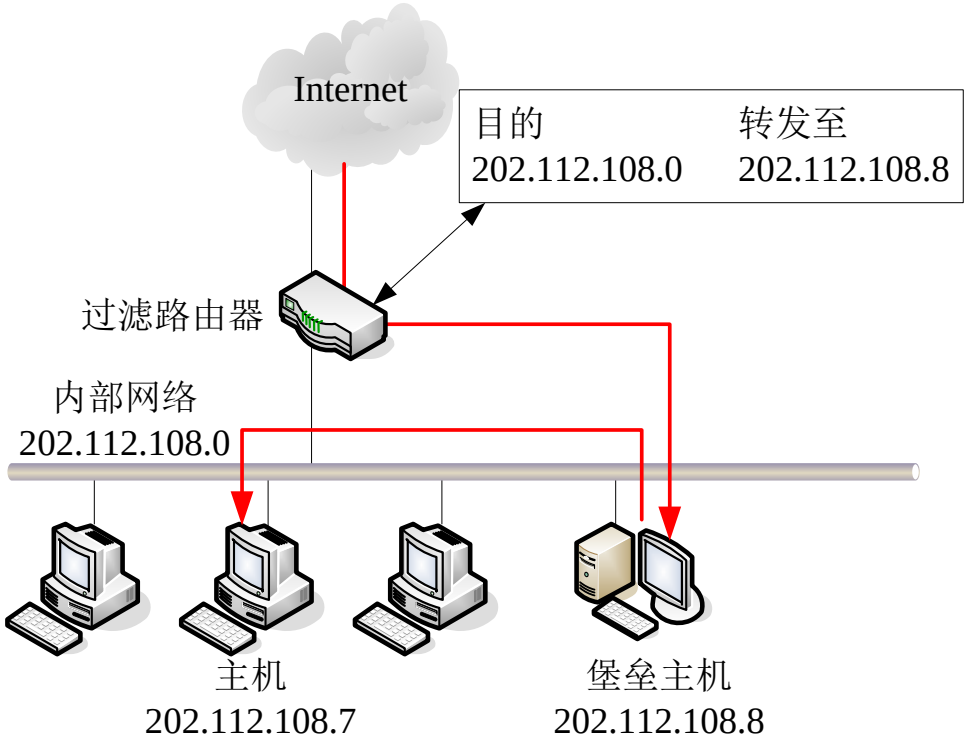
屏蔽主机防火墙转发数据包的过程



3　屏蔽主机防火墙

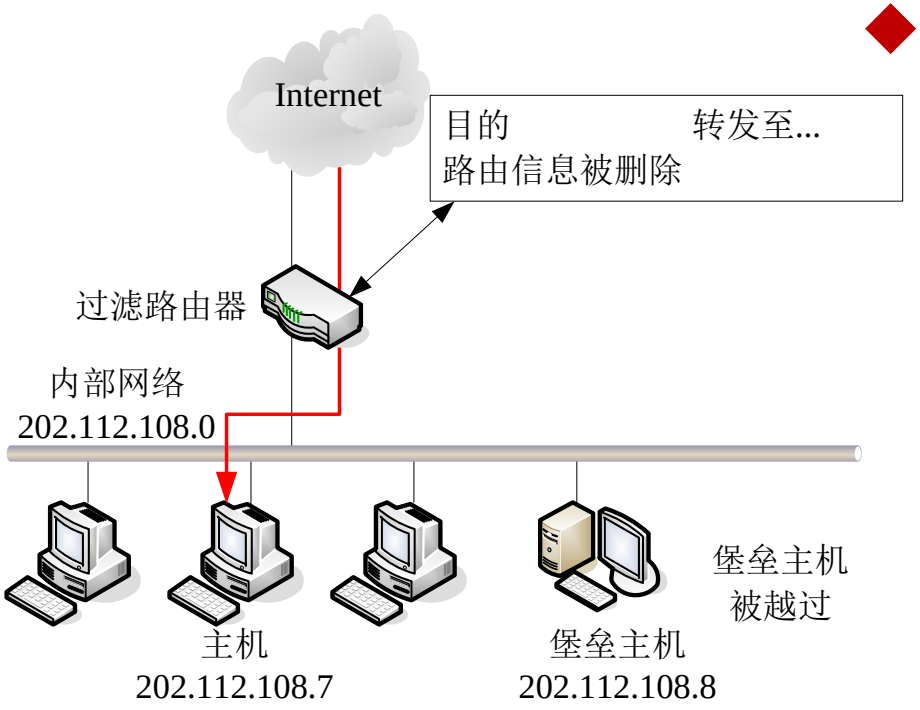
- **与包过滤型防火墙的比较：**
  - 其提供的安全等级比包过滤防火墙系统要高，实现了网络层安全(包过滤)和应用层安全(代理服务)
  - 入侵者在破坏内部网络的安全性之前，必须首先渗透两种不同的安全系统
  - 即使入侵者进入了内部网络，也必须和堡垒主机竞争，堡垒主机是一台安全性很高的主机

3　屏蔽主机防火墙



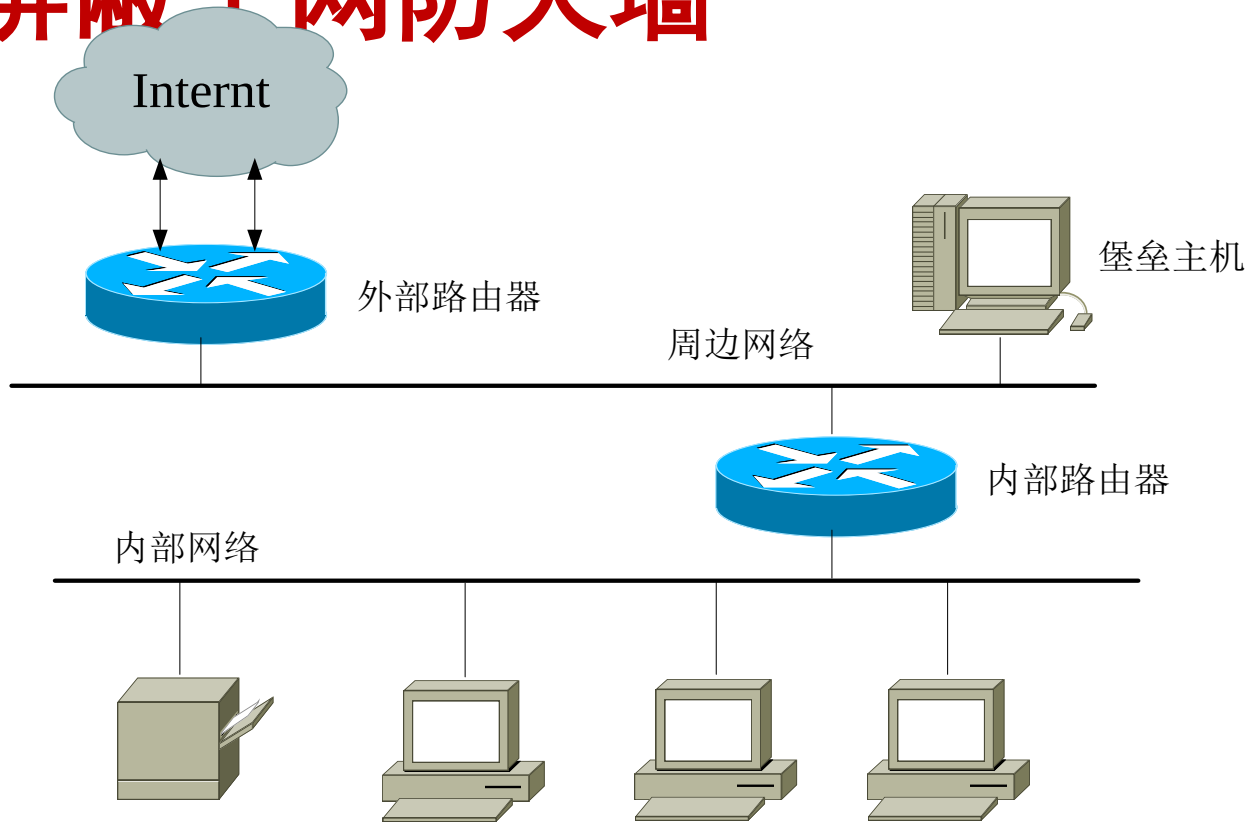
- 路由器正常路由的例子：
  - 正常路由情况：
    - 内部网络地址：202.112.108.0
    - 堡垒主机地址：202.112.108.8
    - 路由表内容
    - 所有流量发到堡垒主机上

3　屏蔽主机防火墙



- 路由表被破坏的情况：
  - 堡垒主机的路由项目被从路由表中删除
  - 进入屏蔽路由器的流量不会被转发到堡垒主机上，可能被转发到另一主机上，外部主机直接访问了内部主机，绕过了防火墙
  - 过滤路由器成为唯一一道防线，入侵者很容易突破屏蔽路由器，内部网络不再安全

4　屏蔽子网防火墙



- 本质上同屏蔽主机防火墙一样，但增加了一层保护体系——一个被隔离的子网（非军事区，DMZ）。堡垒主机位于周边网络上，周边网络和内部网络被内部屏蔽路由器分开

4 屏蔽子网防火墙

- 为什么使用非军事区DMZ？
  - 在屏蔽主机结构中，堡垒主机最容易受到攻击。而且内部网对堡垒主机是完全公开的，入侵者只要破坏了这一层的保护，那么入侵也就大功告成了
  - 屏蔽子网结构就是在屏蔽主机结构中再增加一台路由器的安全机制，这台路由器的意义就在于它能够在内部网和外部网之间构筑出一个安全子网，从而使得内部网与外部网之间有两层隔断。要想侵入用这种体系结构构筑的内部网络，侵袭者必须通过两个路由器，即使侵袭者已设法侵入堡垒主机，他将仍然必须通过内部路由器

4　屏蔽子网防火墙

- **非军事区DMZ**
  - 处于Internet和内部网络之间
  - 包含**两个包过滤路由器**和**一个/多个堡垒主机**
  - 可以放置一些信息和服务器，如WWW和FTP服务器，以便于公众访问，这些服务器可能会受到攻击，因为它们是牺牲服务器，但内部网络还被保护着
  - 通过DMZ网络直接进行信息传输是严格禁止的
  - 是最安全的防火墙系统，因为在定义了“非军事区"网络后，它支持网络层和应用层安全功能

5.5　网络地址转换NAT

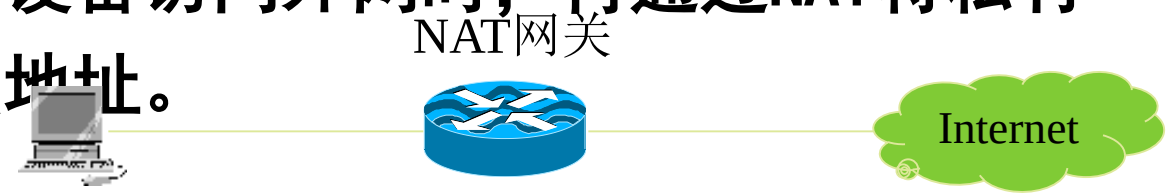
网络地址转换NAT

- NAT是将一个IP地址转换为另一个IP地址的功能。
- NAT的主要作用：

①隐藏内部网络的IP地址；

②解决地址紧缺问题。

- 通常，一个局域网由于申请不到足够多的IP地址，或者只是为了编址方便，在局域网内部采用私有IP地址为设备编址，当设备访问外网时，再通过NAT将私有地址翻译为合法地址。



局域网专用IP地址

- 局域网专用IP地址是Internet特别划分出来的，它们不会注册给任何组织。

IP地址范围	网络类型	网络个数
10.0.0.0~10.255.255.255	A	1
172.16.0.0~172.31.255.255	B	16
192.168.0.0~192.168.255.255	C	256

- 实际上，用户可以使用任意IP作为私有地址，但有可能导致某些外网的站点无法访问。
- **使用私有地址的注意事项：**私有地址不需要经过注册就可以使用，这导致这些地址是不唯一的。所以私有地址只能限制在局域网内部使用，不能把它们路由到外网中去。

NAT基本原理

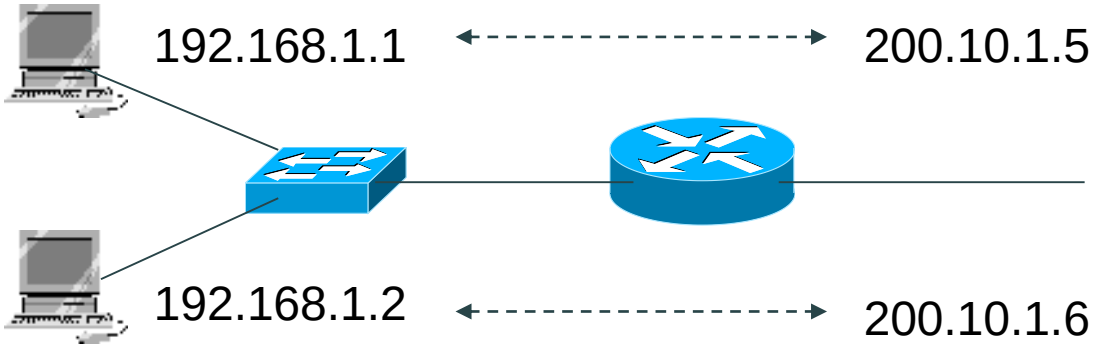
- 当一个使用私有地址的数据包到达NAT设备时，NAT设备负责把私有IP地址翻译成外部合法IP地址，然后再转发数据包，反之亦然。
- 端口多路复用技术：NAT支持把多个私有IP地址映射为一个合法IP地址的技术，这时各个主机通过端口进行区分，这就是端口多路复用技术。
- 利用端口多路复用技术可节省合法IP地址的使用量，但会加大NAT设备的负担，影响其转发速度。

NAT类型

1、静态NAT：

将内部地址和外部地址进行一对一的转换。这种方法要求申请到的合法IP地址足够多，可以与内部IP地址一一对应。

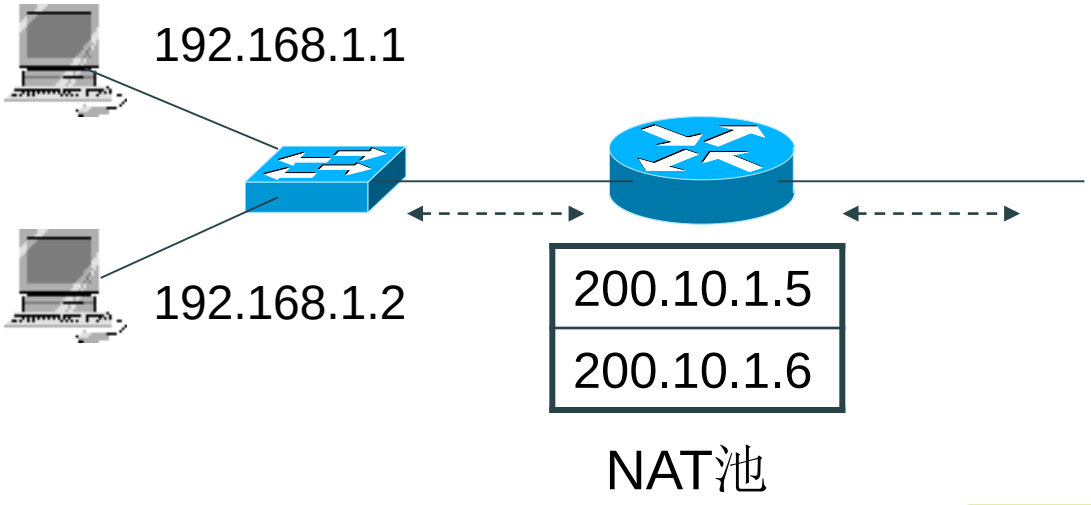
静态NAT一般用于那些需要固定的合法IP地址的主机，比如Web服务器、FTP服务器、E-mail服务器等。



2、NAT池（动态NAT）：

将多个合法IP地址统一的组织起来，构成一个IP地址池，当有主机需要访问外网时，就分配一个合法IP地址与内部地址进行转换，当主机用完后，就归还该地址。

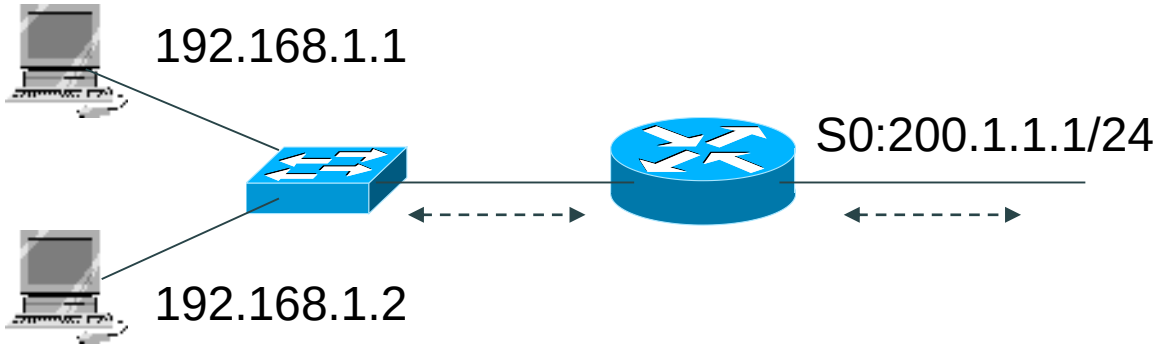
对于NAT池，如果同时联网用户太多，可能出现地址耗尽的问题。后续的NAT翻译申请将会失败。



3、PAT（端口NAT）：

使用端口多路复用技术，将多个内部地址映射为一个合法地址，用不同的端口号区分各个内部地址。这种方法只需要一个合法IP地址。

路由器支持的PAT会话数是有限制的，所以使用PAT的局域网，其网络的规模不应该太大。



4、复用NAT池（复用动态NAT）：

将多个合法IP地址构成一个NAT池，使用复用技术映射其中的地址，每个地址有可以对应多台主机，各主机用端口进行区分。

复用NAT池是NAT池和PAT技术的结合，可用于大规模的局域网。

说明：在端口复用技术中，用端口区分的不是一台主机，而是一个网络连接（会话），当一台主机同时建立了多个会话时，它的每个会话会占用一个端口映射。假如一台路由器支持4000个会话，那么它支持的主机数量会远少于4000台。

NAT技术举例

在动态方式下，有一组全局IP地址与内部IP地址对应。例如：192.168.32.10 总是翻译成213.18.123.100 to 213.18.123.150. 范围内第一个可用的IP地址

静态方式下，内部地址与外部IP地址总是一一对应的。如： 192.168.32.10 总是翻译成 213.18.123.110.

NAPT也是一种动态方式，用一个全局IP地址加上端口号实现与内部IP地址的翻译。

常用NAT设备

- 实现NAT可以使用不同的设备，它们的基本功能相同，但功能强弱有别，应根据需要进行选用。常用的设备有：

1、路由器：功能强，支持多种NAT设置；

2、防火墙：除NAT转换外，还提供多种保护功能；

3、代理服务器：提供局域网接入功能；

4、双网卡计算机：功能较弱，多用于小型网络。

河海大学

Thank You!