电子科技大学
University of Electronic Science and Technology of China

网络攻防安全技术

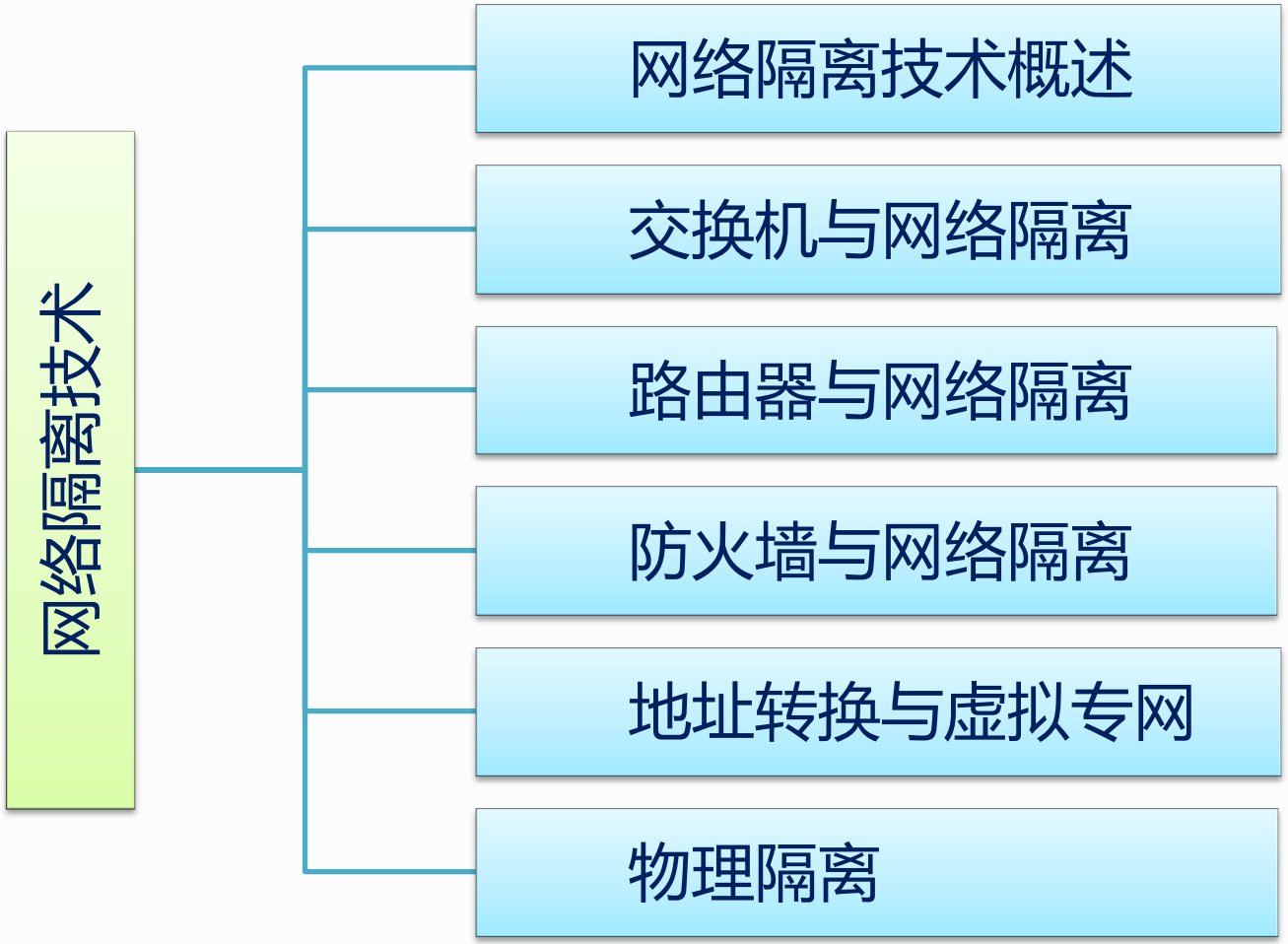
电子科技大学 信息与软件工程学院

2020/10/15

第六讲 网络隔离技术

了解网络隔离的基本概念；理解不同层次上隔离技术的原理和特点；掌握网络隔离技术在实际环境中的应用方式。

内容安排


网络隔离技术
网络隔离技术概述
交换机与网络隔离
路由器与网络隔离
防火墙与网络隔离
地址转换与虚拟专网
物理隔离

第六讲 网络隔离技术

一、网络扫描技术概述

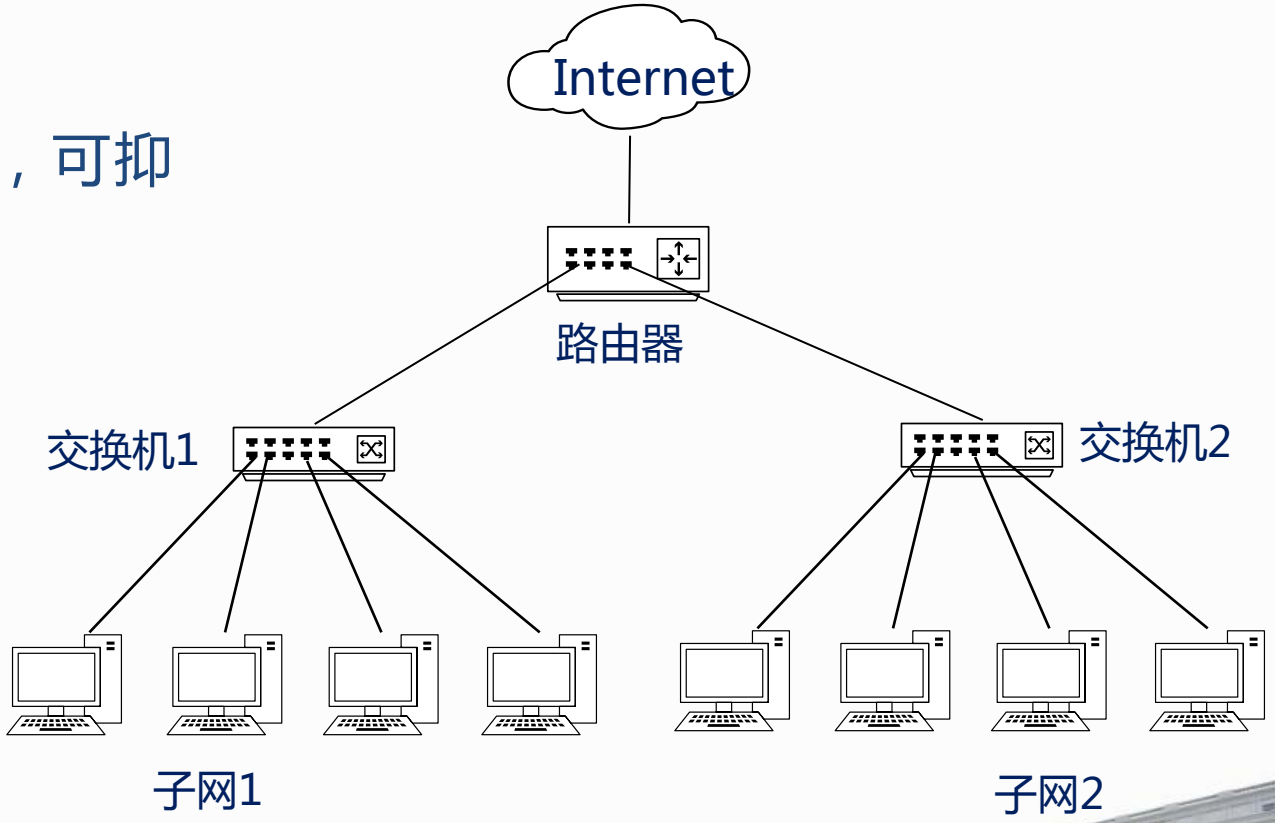
- 什么是网络隔离？
  - 隔离技术是指通过对具有不同安全需求的应用系统进行分类保护，从而有助于将风险较大的应用系统与其他需要更多安全保护的应用系统隔离，达到保护的目的。
  - 隔离的本质需求
    - 既要信息交换或共享资源，又要通过隔离提高安全性保障。
  - 隔离的类型
    - 逻辑隔离、物理隔离

二、交换机与网络隔离

- 交换机的功能
  - 物理编址：（相对应的是网络编址）定义了设备在数据链路层的编址方式；
  - 网络拓扑结构：包括数据链路层的说明，定义了设备的物理连接方式，如星型拓扑结构或总线拓扑结构等；
  - 错误校验：向发生传输错误的上层协议告警；
  - 帧序列化：数据帧序列重新整理并传输除序列以外的帧；
  - 流量控制：可以延缓数据的传输能力，以使接收设备不会因为在某一时刻接收到了超过其处理能力的信息流而崩溃。

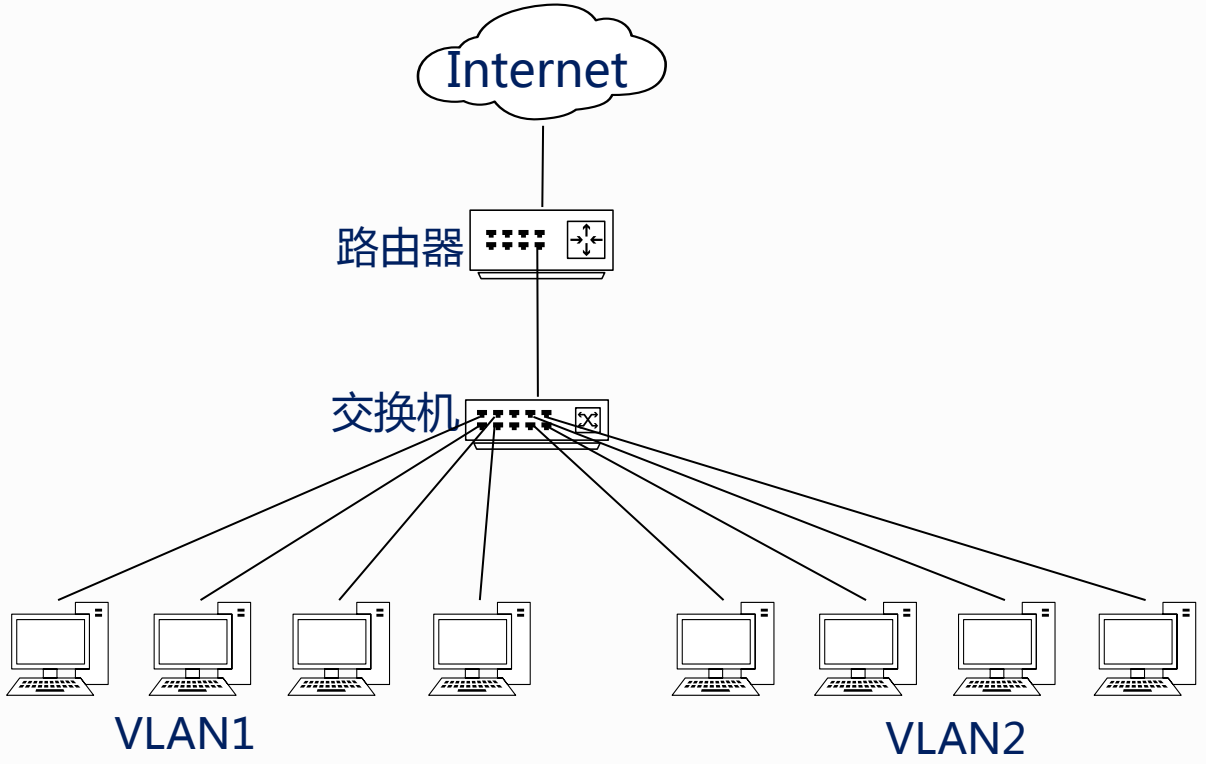
二、交换机与网络隔离

- 交换机直接隔离
  - 子网1和子网2分属不同的网段，可抑制广播数据的传播和监听



二、交换机与网络隔离

- 虚拟子网（Vlan）的隔离
  - 通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的新兴技术。连接在同一交换机上的主机可以通过VLAN划分到不同的虚拟子网，也就是不同的广播域。通过VLAN的构建能够更有效的对局域网的数据进行隔离。
  - VLAN1和VLAN2采用逻辑方式划分，分属不同的广播域。



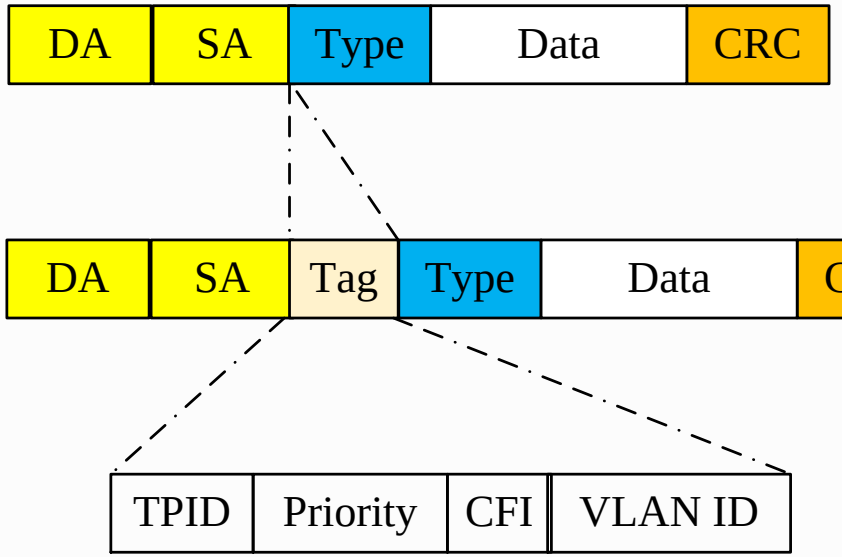
二、交换机与网络隔离

Vlan的划分方式

	基于端口划分	基于MAC地址划分	基于IP层划分	基于IP组播划分
优点	简单，一次定义	支持用户动态迁移	支持用户动态迁移，可按协议类型划分	可通过路由器扩展，支持广域网
缺点	灵活性差	配置工作量大，执行效率低	效率低，需要交换机支持	效率低，不适合局域网

二、交换机与网络隔离

- 虚拟子网的实例——802. 1Q协议标准



标准的以太网帧

带有802.1Q标记的以太网帧

TPID（Tag Protocol Identifier）：表明这是一个加了802.1Q标签的帧。TPID包含了一个固定的值0x8100。

Priority：3 位指明帧的优先级。

CFI （Canonical Format Indicator ）：值为0说明是规范格式，1为非规范格式。

VLAN Identified(VLAN ID)：这是一个12位的域，指明VLAN的ID。

第六讲 网络隔离技术

- 测试点6-1
  - 集线器能作为网络隔离设备吗？请说明理由？
  - 简述Vlan划分的不同方式及特点。

三、路由器与网络隔离

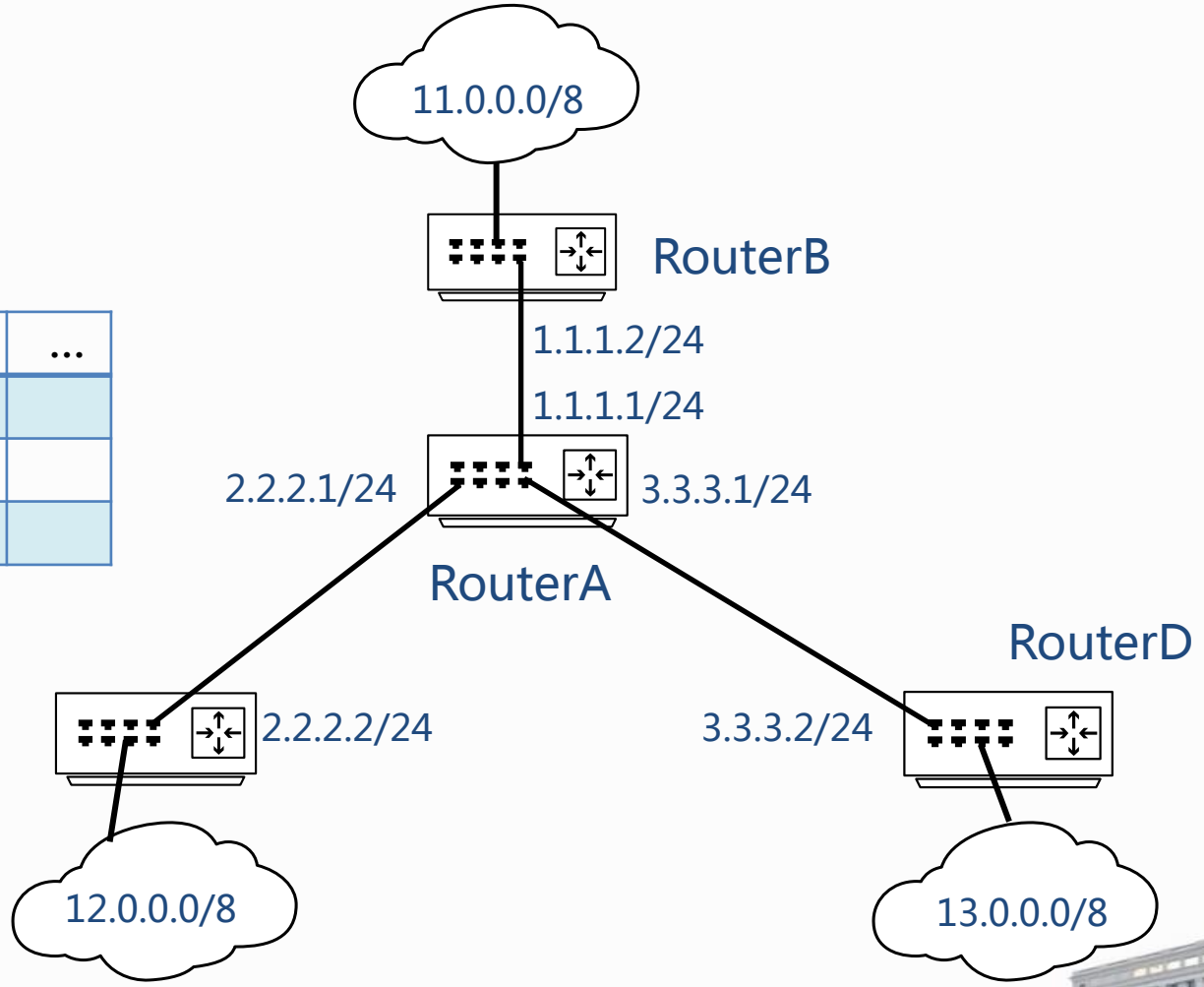
路由器的功能

- 网络互连，路由器支持各种局域网和广域网接口，主要用于互连局域网和广域网，实现不同网络互相通信；
- 数据处理，提供包括分组过滤、分组转发、优先级、复用、加密、压缩和防火墙等功能；
- 网络管理，路由器提供包括配置管理、性能管理、容错管理和流量控制等功能。

三、路由器与网络隔离

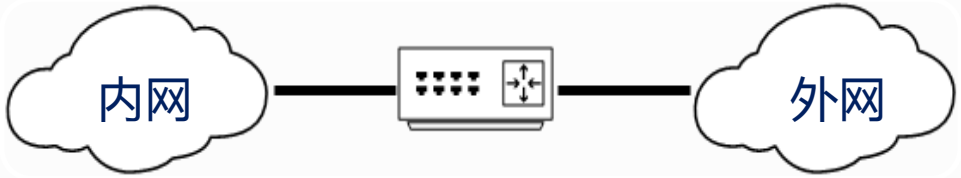
路由器工作实例

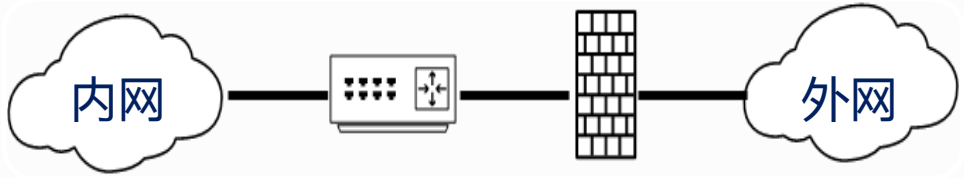
Destination	Nexthop	Interface	…
11.0.0.0/8	1.1.1.2	P1	
12.0.0.0/8	2.2.2.2	P2	
13.0.0.0/8	3.3.3.2	P3	



三、路由器与网络隔离

◘ 路由器隔离部署方式





路由器作为唯一安全组件

- 相对交换机，能提供更高层次的安全功能
- 包过滤，NAT等

路由器作为安全组件的一部分

- 在一个全面安全体系结构中，常用作屏蔽设备，执行包过滤功能，而防火墙对能够通过路由器的数据包进行检查

四、防火墙与网络隔离

防火墙基本概念

- 定义
  - 防火墙是用一个或一组网络设施，在两个或多个网络间加强访问控制，以保护一个网络不受到另一个网络攻击的安全技术
- 功能
  - 逻辑上防火墙是一个分离器，一个限制器，也是一个分析器
- 主要技术
  - 分组（包）过滤、应用代理（网关）、状态检测、链路层代理（网关）

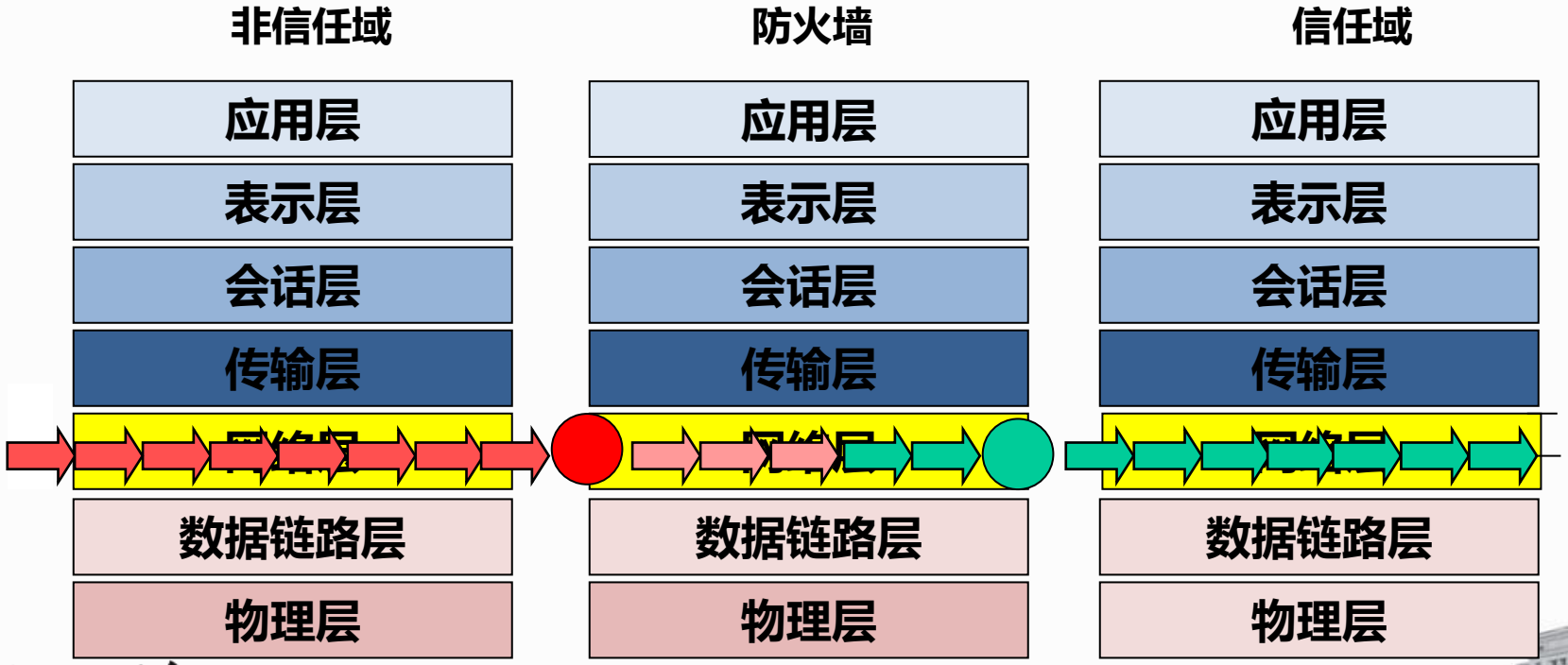
四、防火墙与网络隔离

◘ 防火墙部署示意

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

四、防火墙与网络隔离

- 分组过滤防火墙
  - 基于源地址和目的地址、应用、协议类型以及每个IP包的端口来作出通过与否的判断。



四、防火墙与网络隔离

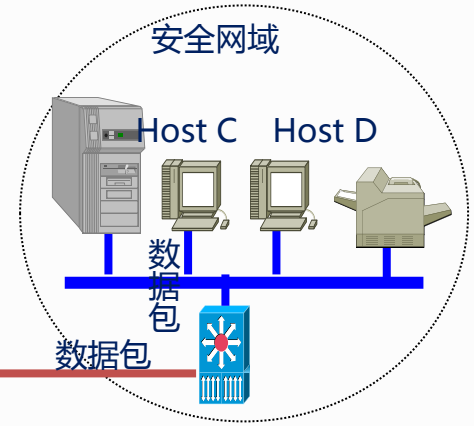
◘ 分组过滤防火墙工作原理

控制策略

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

查找对应的控制策略

根据策略决定如何处理该数据包



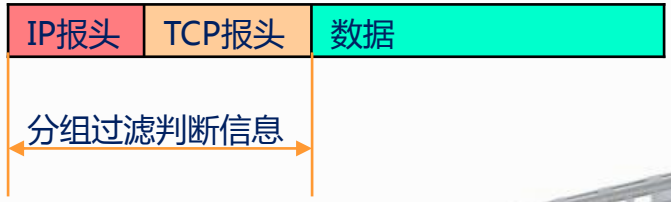
拆开数据包

数据包

数据包

数据包

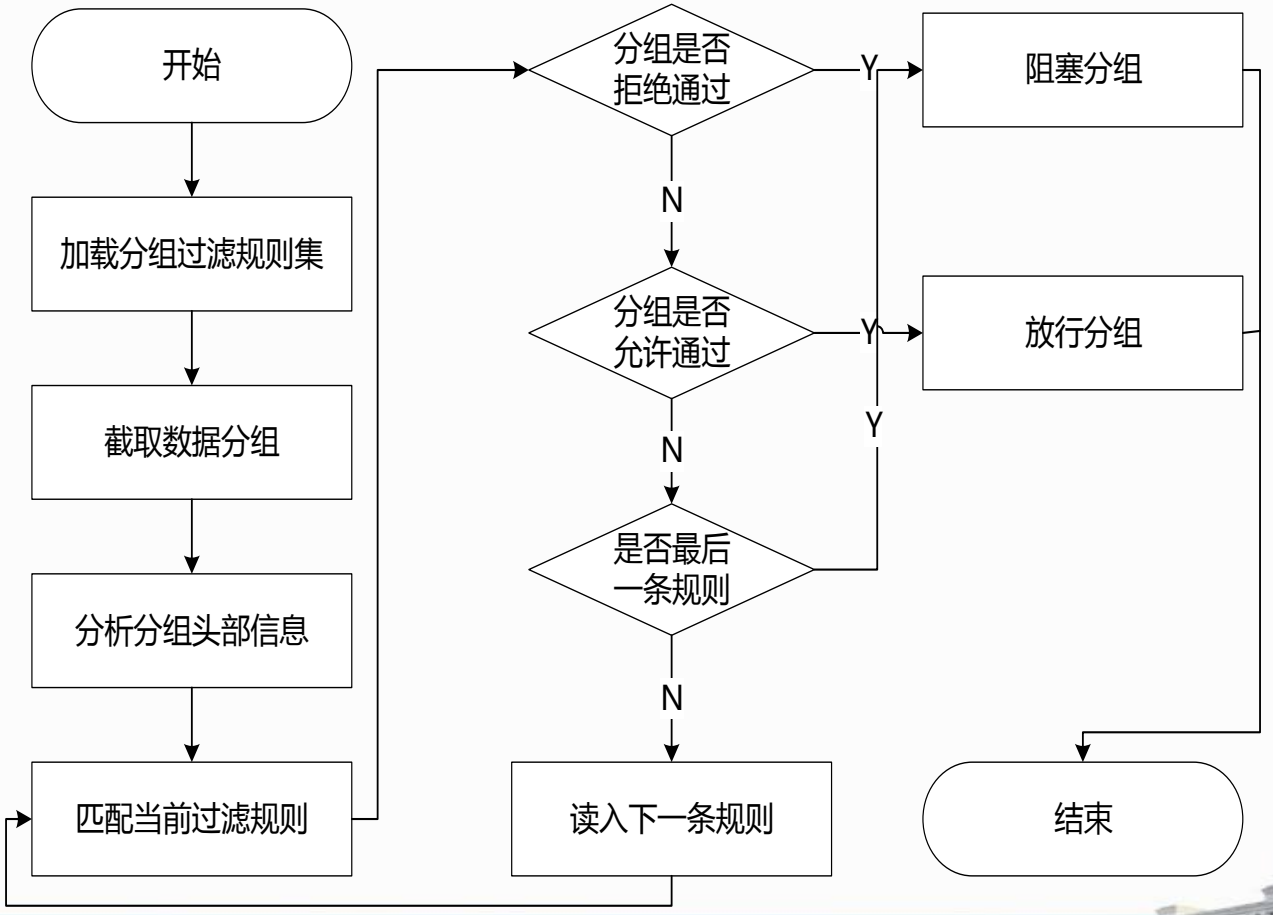
Host A



- 过滤依据主要是IP报头里面的信息，不能对应用层数据进行处理。

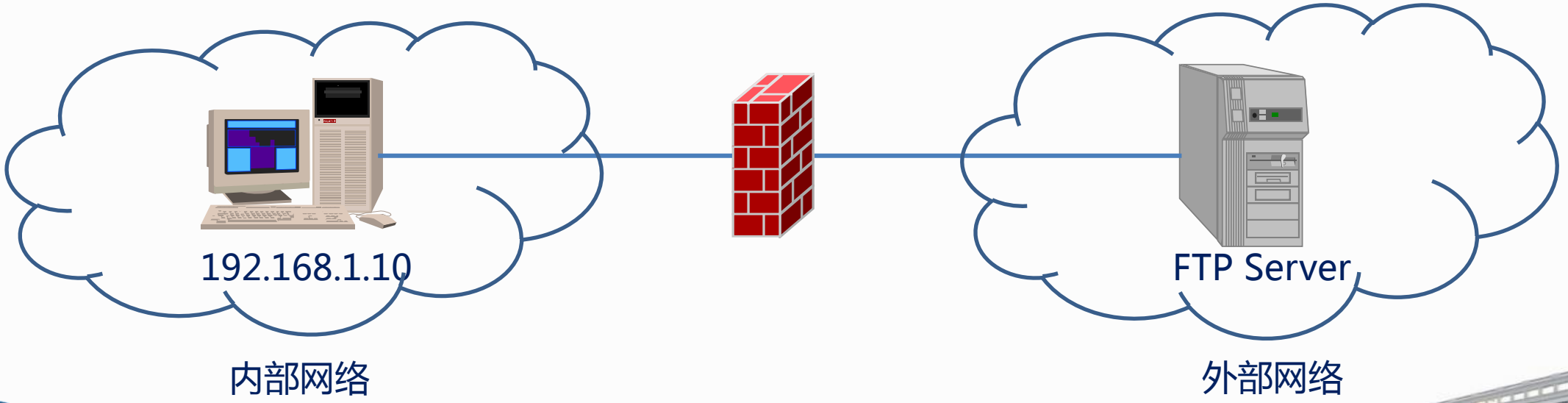
四、防火墙与网络隔离

- 防火墙与网络隔离
  - 分组过滤流程



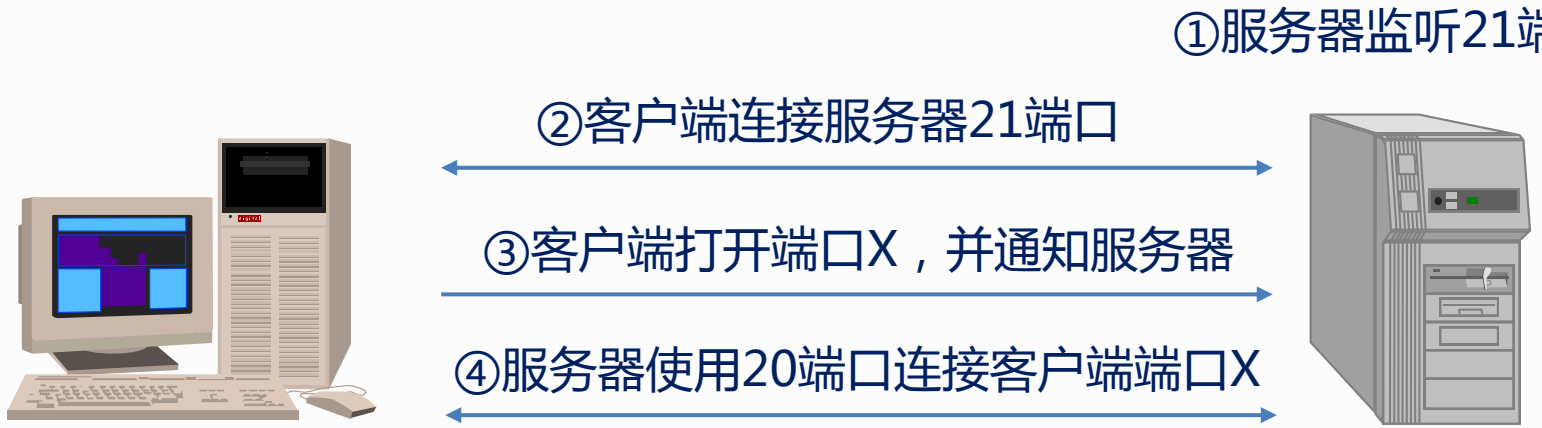
四、防火墙与网络隔离

- 分组过滤防火墙规则设置实例
  - 设置防火墙规则，允许内部网络中IP地址为192.168.1.10的主机采用主动模式访问外部网络中的FTP服务。



四、防火墙与网络隔离

- 分组过滤规则设置过程
  - 步骤一：需求分析（FTP主动模式）



四、防火墙与网络隔离

- 分组过滤规则设置过程
  - 步骤二：规则设定
    - 允许主机192.168.1.10与FTP服务器21端口建立连接
    - 允许FTP服务器20端口与主机192.168.1.10建立连接

序号	动作	源IP	目的IP	源端口	目的端口	协议类型
1	允许	192.168.1.10	*	*	21	TCP
2	允许	*	192.168.1.10	21	*	TCP
3	允许	*	192.168.1.10	20	*	TCP
4	允许	192.168.1.10	*	*	20	TCP

四、防火墙与网络隔离

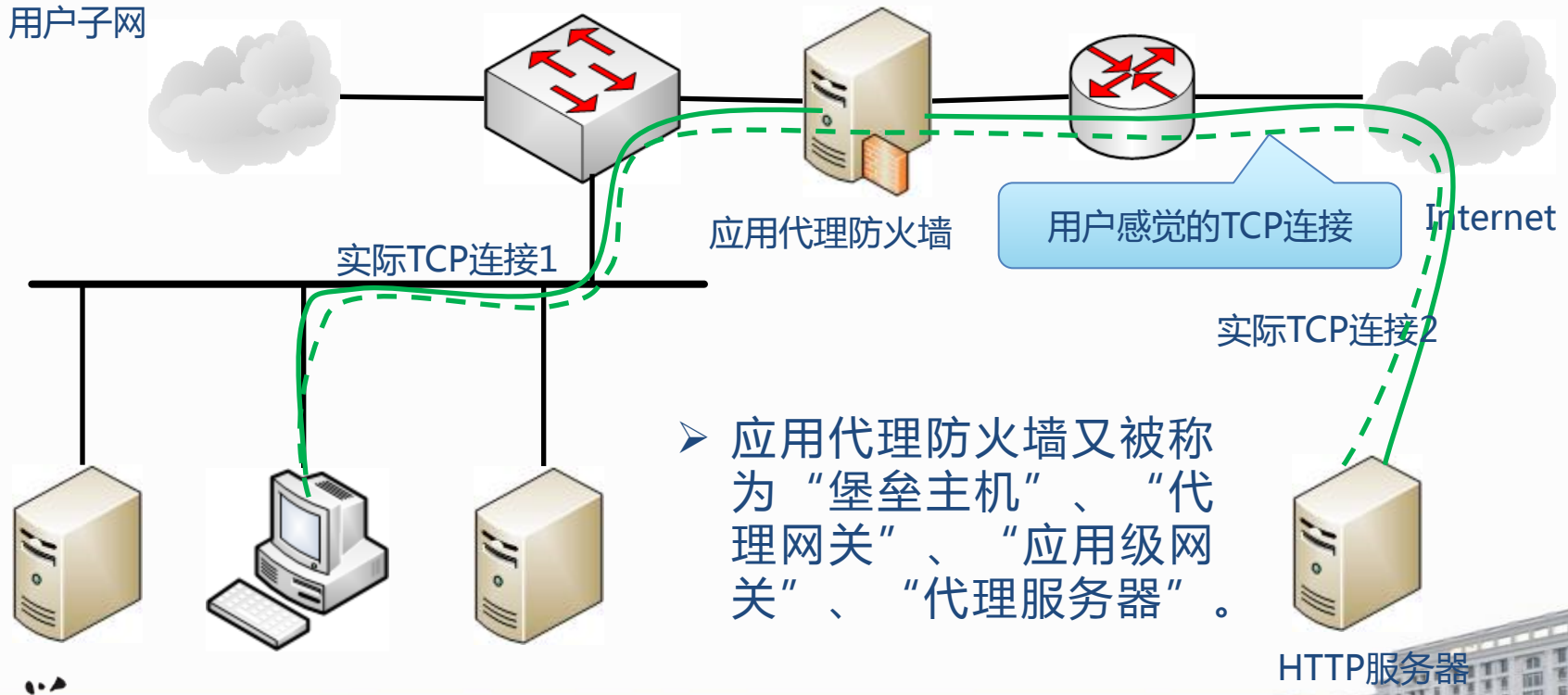
- 分组过滤规则设置的基本原则
  - 双向性原则：协议总是双向的，协议包括一方发送一个请求而另一方返回一个应答。在制定包过滤规则时，要注意包是从两个方向来到防火墙的。
  - 内外性原则：在制定分组过滤规则时，必须准确理解“往内”与“往外”的包和“往内”与“往外”的服务这几个词的语义。
  - 默认拒绝原则：网络的安全策略中的有两种方法，默认拒绝（没有明确地被允许就应被拒绝）与默认允许（没有明确地被拒绝就应被允许）。从安全角度来看，用默认拒绝应该更合适。

四、防火墙与网络隔离

- 分组过滤防火墙的特点
  - 优点
    - 容易实现，费用少，对性能的影响不大，对流量的管理较出色。
  - 缺点
    - 过滤规则表管理复杂，随着规则表规模加大出现漏洞的可能性也会增加；
    - 只对数据包头进行检查，没有身份验证机制，不能分辨用户；
    - 不能进行应用层的深度检查，因此不能发现传输的恶意代码及攻击数据包；
    - 容易遭受源地址欺骗，源地址改为内部地址往往可以绕过包过滤防火墙。

四、防火墙与网络隔离

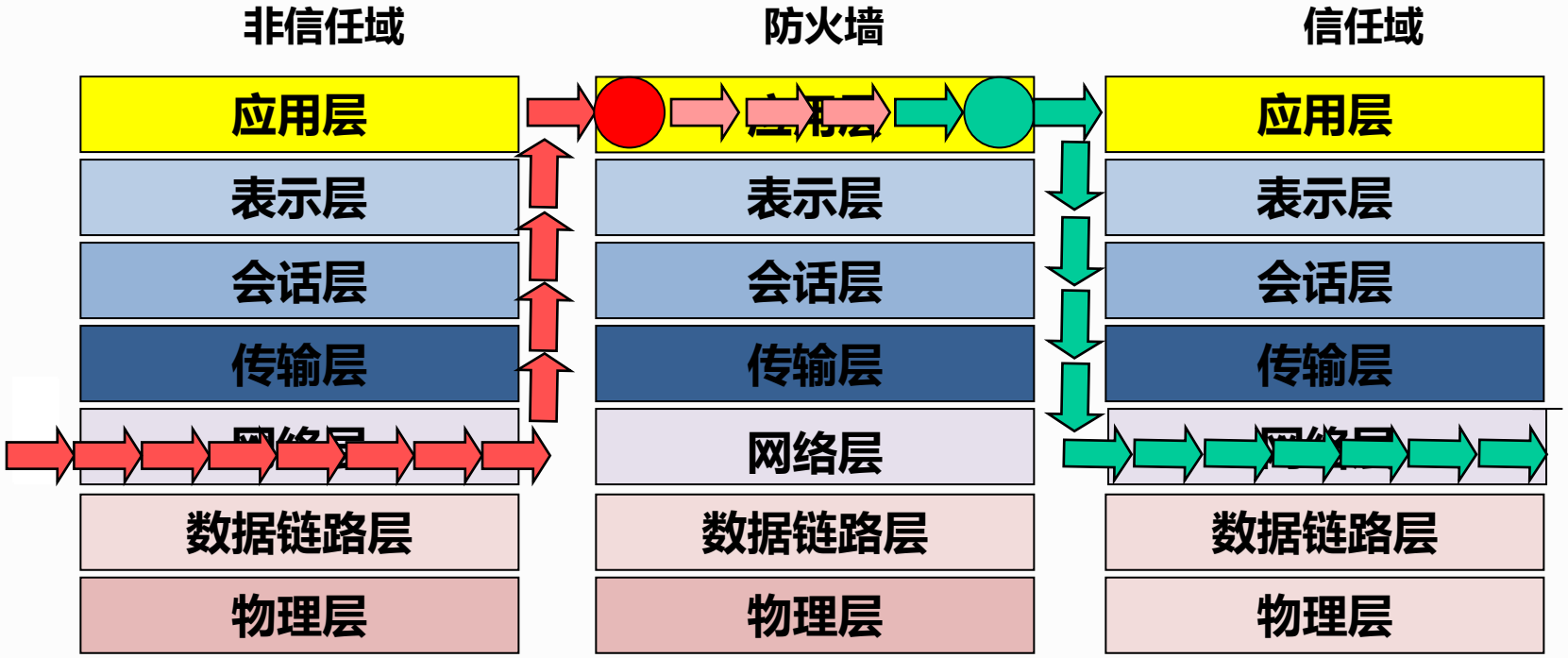
◘ 应用代理防火墙



- 应用代理防火墙又被称为“堡垒主机”、“代理网关”、“应用级网关”、“代理服务器”。

四、防火墙与网络隔离

- 应用代理防火墙工作层次

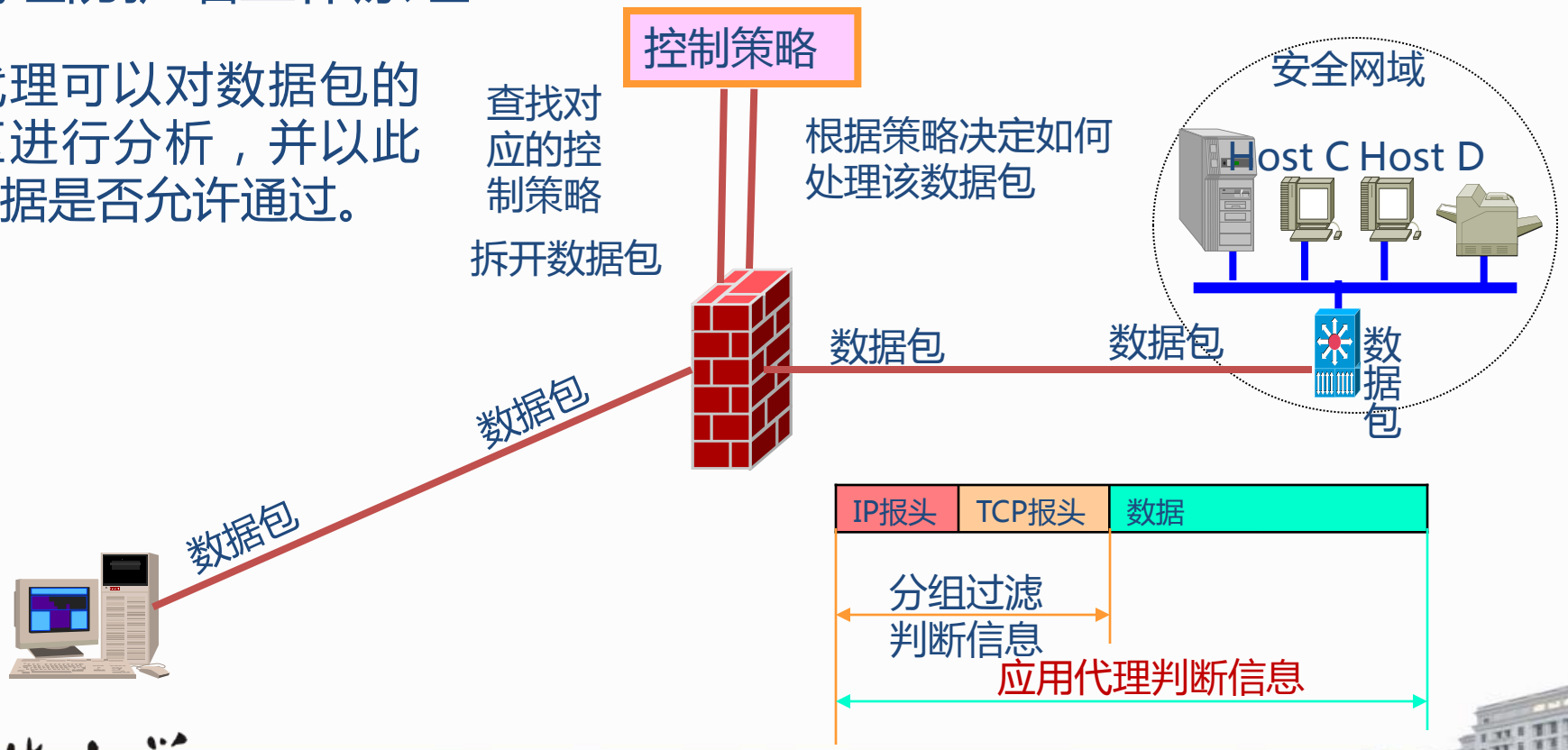


- 应用代理逻辑位置在OSI 7层协议的应用层上，所以主要采用协议代理服务(proxy services)。

四、防火墙与网络隔离

◘ 应用代理防护墙工作原理

- 应用代理可以对数据包的数据区进行分析，并以此判断数据是否允许通过。

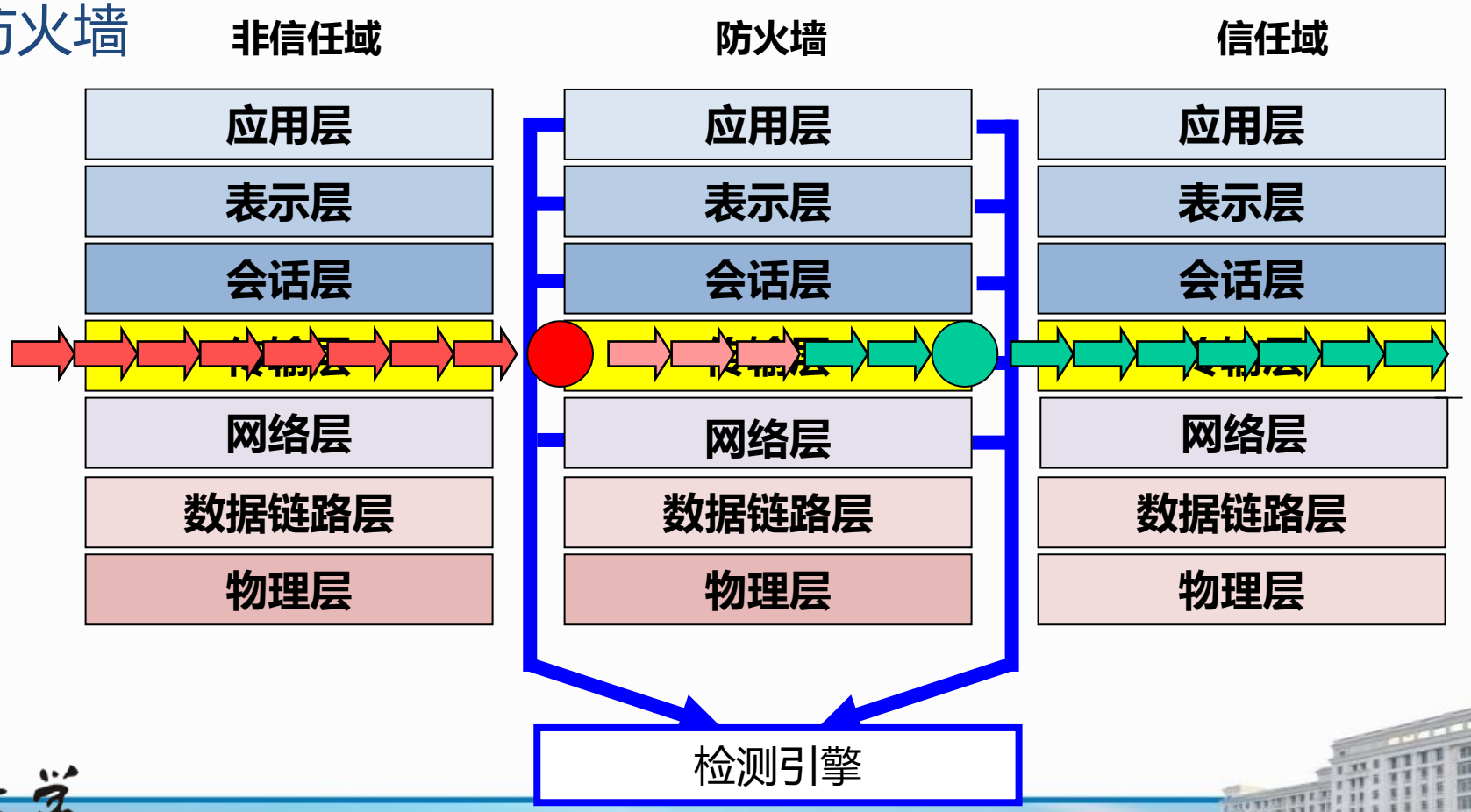


四、防火墙与网络隔离

- 应用代理防火墙的特点
  - 优点
    - 可以提供更细致的日志；
    - 可以执行诸如身份验证等功能，同时能隐藏内部IP地址；
    - 能够进行应用级的过滤。例如，应用代理防火墙可以禁止FTP的“put”命令，从而保证用户不能往匿名FTP服务器上写入数据。
  - 缺点
    - 工作在OSI模型最高层，因此开销较大；
    - 对每项服务必须使用专门设计的代理服务器；
    - 配置的方便性较差，对用户不透明。例如使用HTTP代理，需要用户配置自己的IE，从而使之指向代理服务器。

四、防火墙与网络隔离

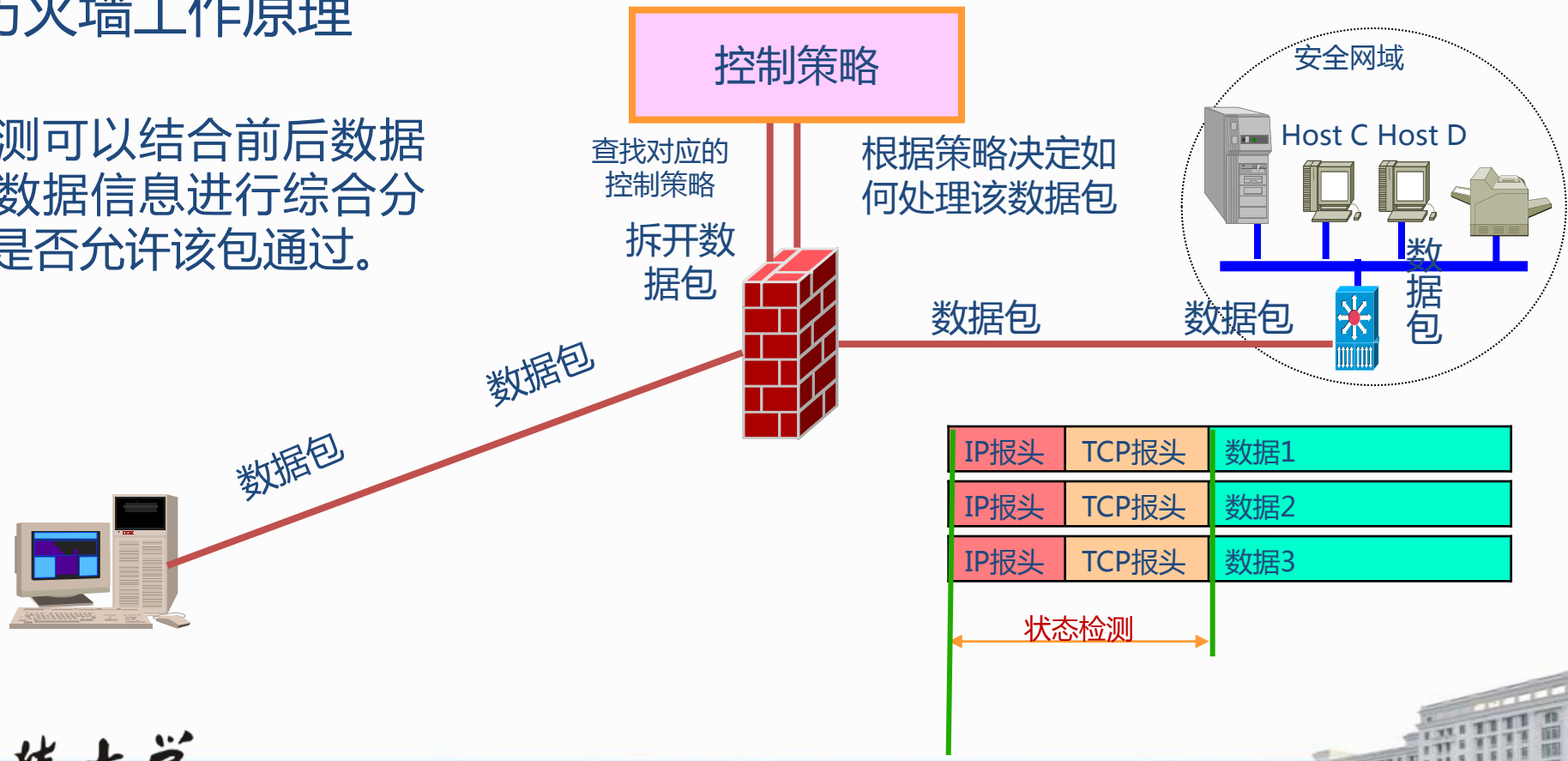
- 状态检测防火墙



四、防火墙与网络隔离

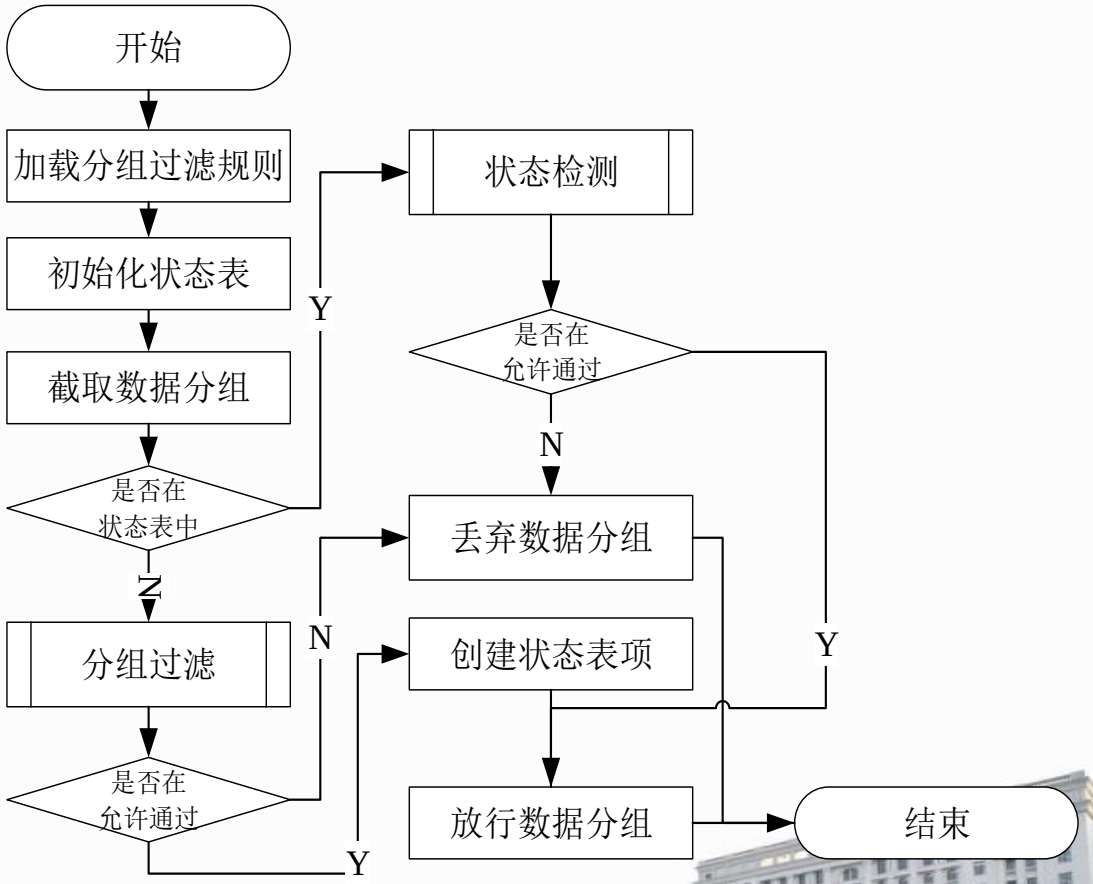
◘ 状态防火墙工作原理

➢ 状态检测可以结合前后数据包里的数据信息进行综合分析决定是否允许该包通过。



四、防火墙与网络隔离

- 状态检测防火墙工作流程
  - 状态检测技术是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。



四、防火墙与网络隔离

- 状态检测防火墙的特点
  - 优点
    - 比分组过滤技术安全性高，比应用代理技术效率高。
  - 缺点
    - 大多数状态检测防火墙的规则仍然与普通的包过滤相似。也有的状态检测防火墙对应用层的信息进行检查。例如可以通过检查内网发往外网的FTP协议数据包中是否有put命令来阻断内网用户向外网的服务器上传数据。但只检测特定字符串，不能实施代理功能，不能隐藏客户端地址。

四、防火墙与网络隔离

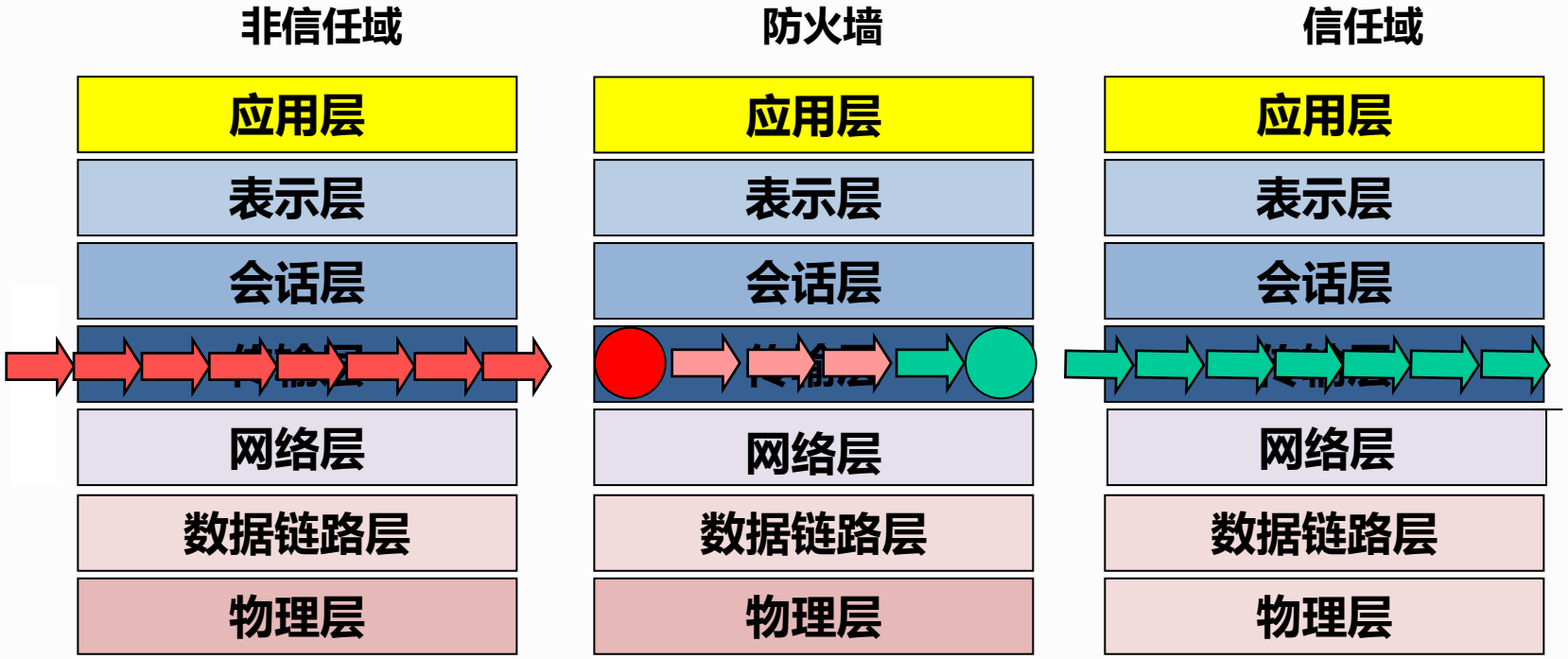
- 状态检测表VS分组过滤表

序号	动作	源IP	目的IP	源端口	目的端口	协议类型

源地址	目的地址	协议	源端口	目的端口	超时（秒）
192.168.1.10	202.114.112.6	TCP	32141	21	1.5
202.114.112.6	192.168.1.10	TCP	20	23333	20

四、防火墙与网络隔离

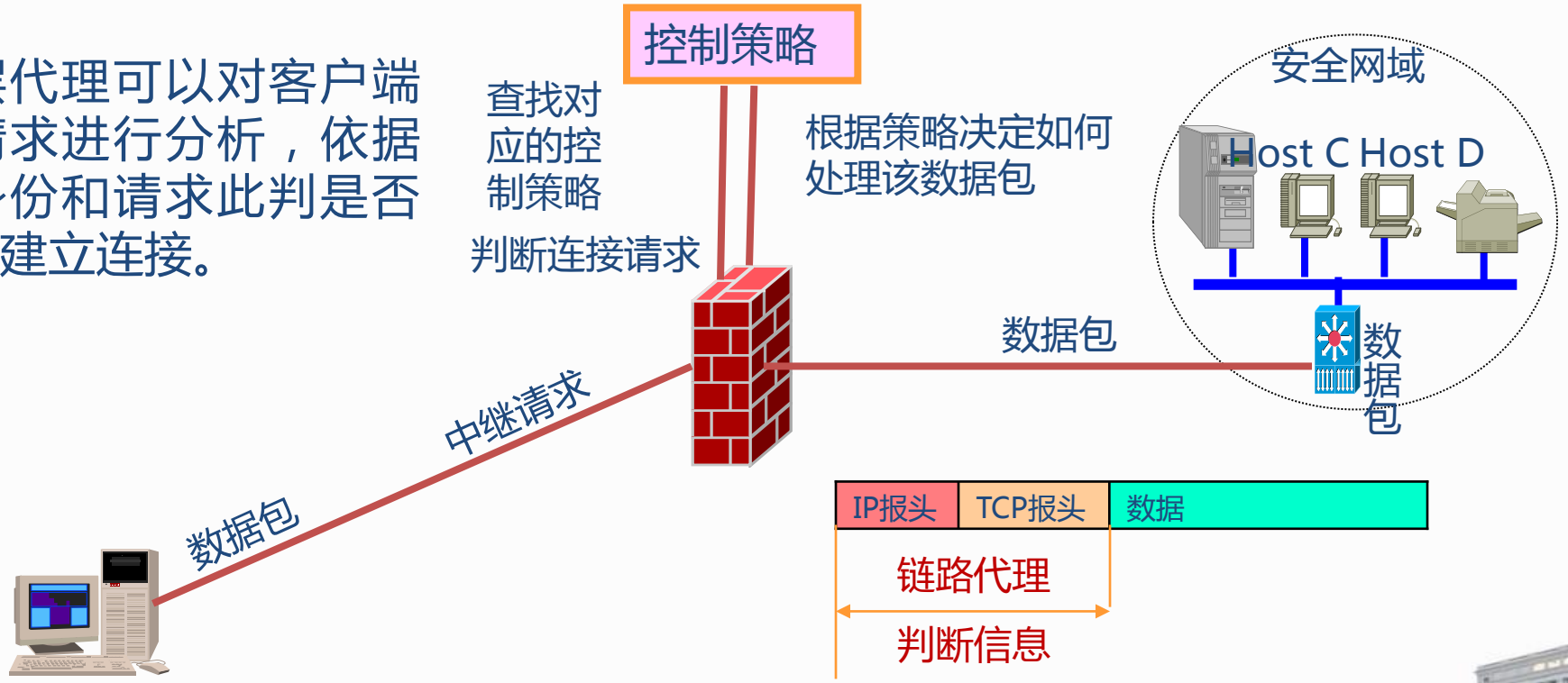
- 链路层代理（SOCKS）防火墙



四、防火墙与网络隔离

◘ 链路层代理（SOCKS）防火墙工作原理

- 链路层代理可以对客户端连接请求进行分析，依据客户身份和请求此判是否否允许建立连接。

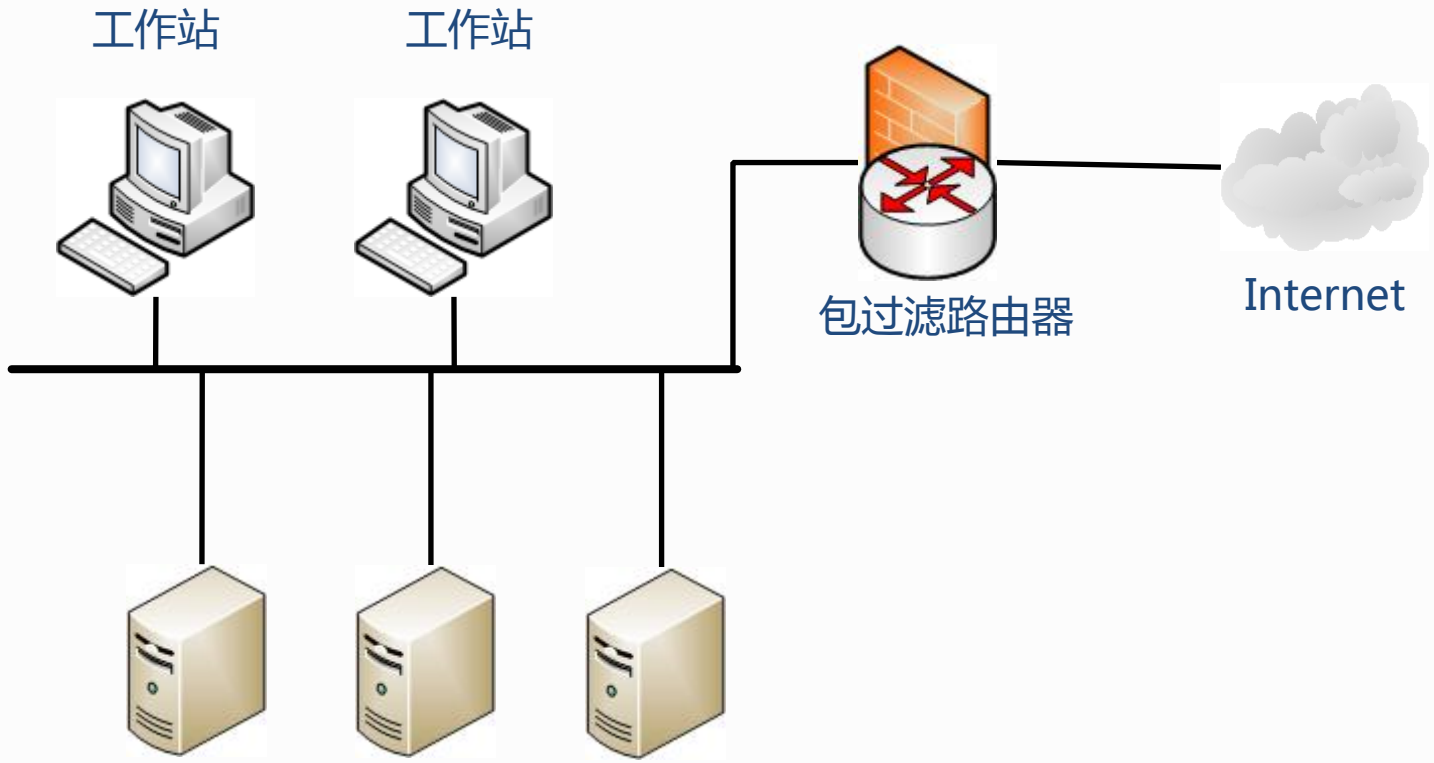


四、防火墙与网络隔离

- 链路层代理防火墙的特点
  - 优点
    - 可以支持不同的应用层协议（Sock4支持TCP，Socks5支持TCP/UDP）；
    - 支持用户级的认证，可针对具体会话进行安全管理
  - 缺点
    - 对客户端不透明
    - 无法针对特定的应用协议进行安全管理

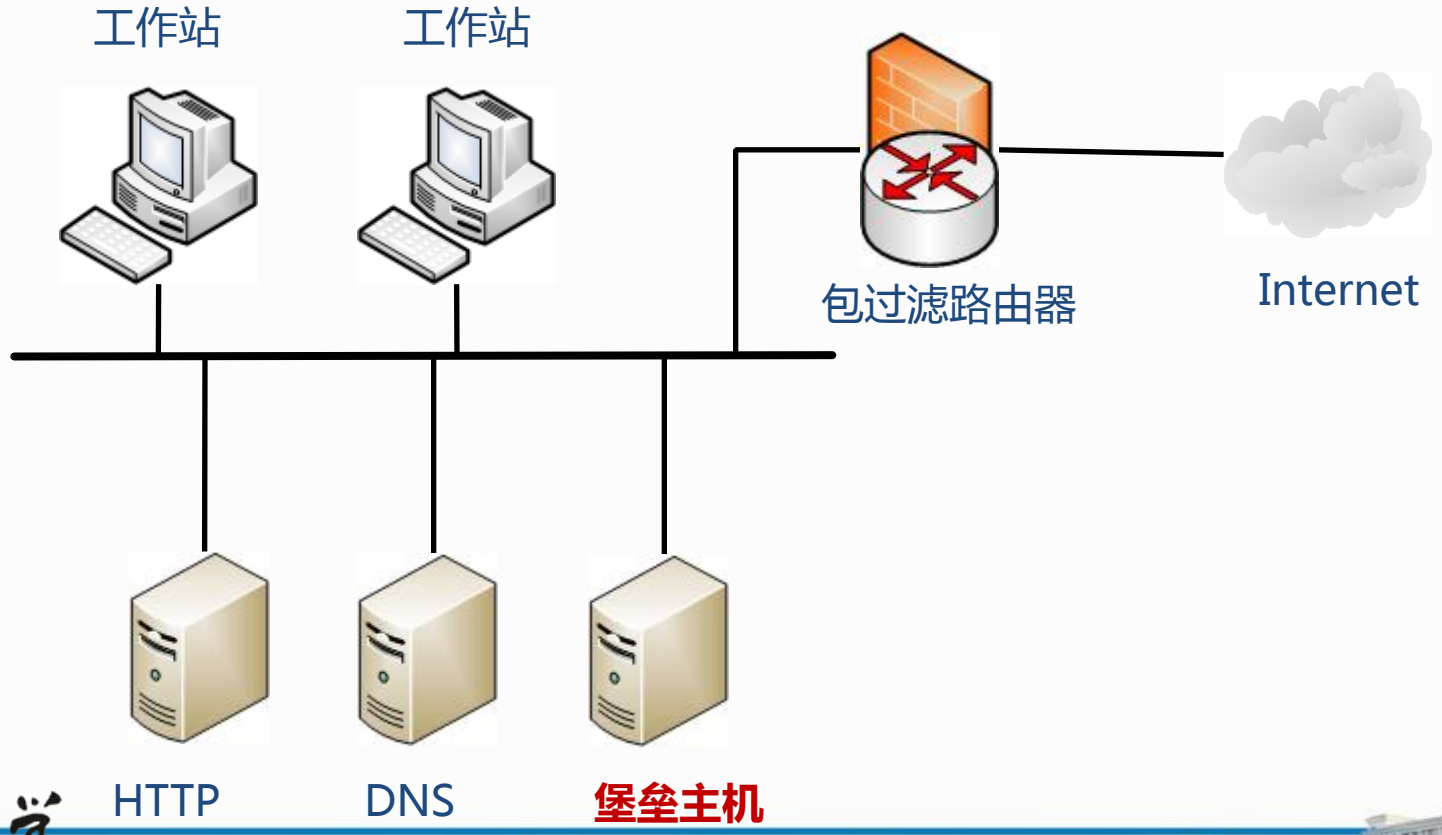
四、防火墙与网络隔离

- 防火墙的典型体系结构——包过滤路由器模型



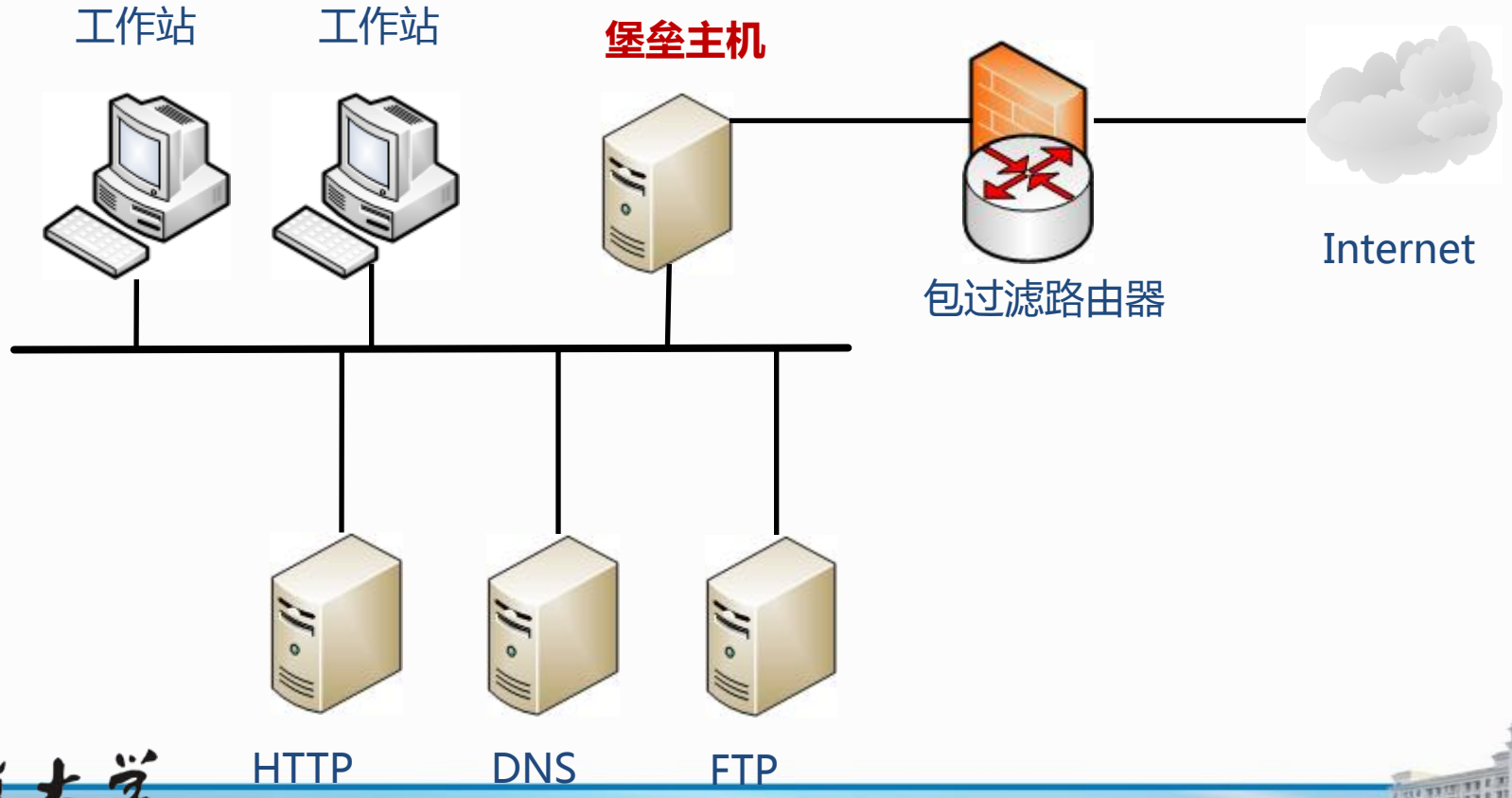
四、防火墙与网络隔离

- 防火墙的典型体系结构——单宿主堡垒主机模型



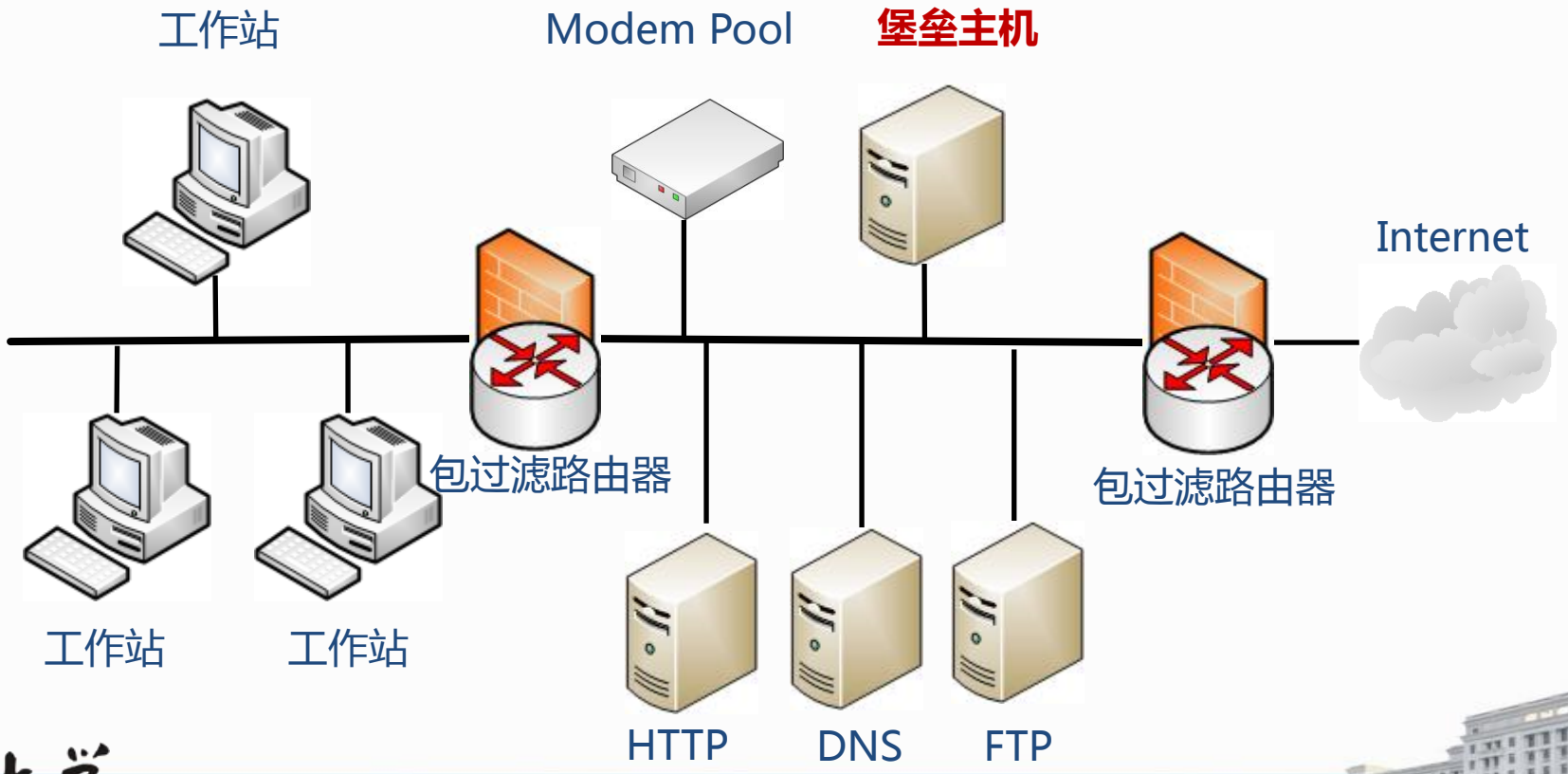
四、防火墙与网络隔离

- 防火墙的典型体系结构——双宿主堡垒主机模型



四、防火墙与网络隔离

- 防火墙的典型体系结构——子网屏蔽防火墙模型



四、防火墙与网络隔离

◘ 防火墙功能总结

- 防火墙是网络安全的屏障，例如过滤掉不安全的服务协议，保护网络免受基于路由的攻击；
- 防火墙可以强化网络安全策略，例如提供认证和审计策略；
- 防火墙可以阻止内部信息外泄，例如划分不同安全等级，限制信息流动方向；
- 防火墙可以作为实现某些网络功能的便利平台，比如NAT，VPN等。

四、防火墙与网络隔离

- 防火墙的局限性
  - 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。

四、防火墙与网络隔离

- 防火墙常见技术指标
  - 性能指标
    - 吞吐量：防火墙在不丢包的情况下能够达到的最大包转发速率；
    - 延时：数据包通过防火墙所用的时间；
    - 最大并发数：防火墙能够同时处理的点对点连接的最大数目；
    - 平均无故障时间：系统平均能够正常运行多长时间，才发生一次故障；
  - 功能指标
    - 工作模式、自身防御能力、支持服务类型、认证功能、安全管理、其他功能（NAT，VPN）

四、防火墙与网络隔离

- 防火墙实例——Iptables 与 Netfilter
  - netfilter
    - 位于Linux内核中的包过滤功能体系
    - 称为Linux防火墙的“内核态”
  - iptables
    - 位于/sbin/iptables，用来管理防火墙规则的工具
    - 称为Linux防火墙的“用户态”

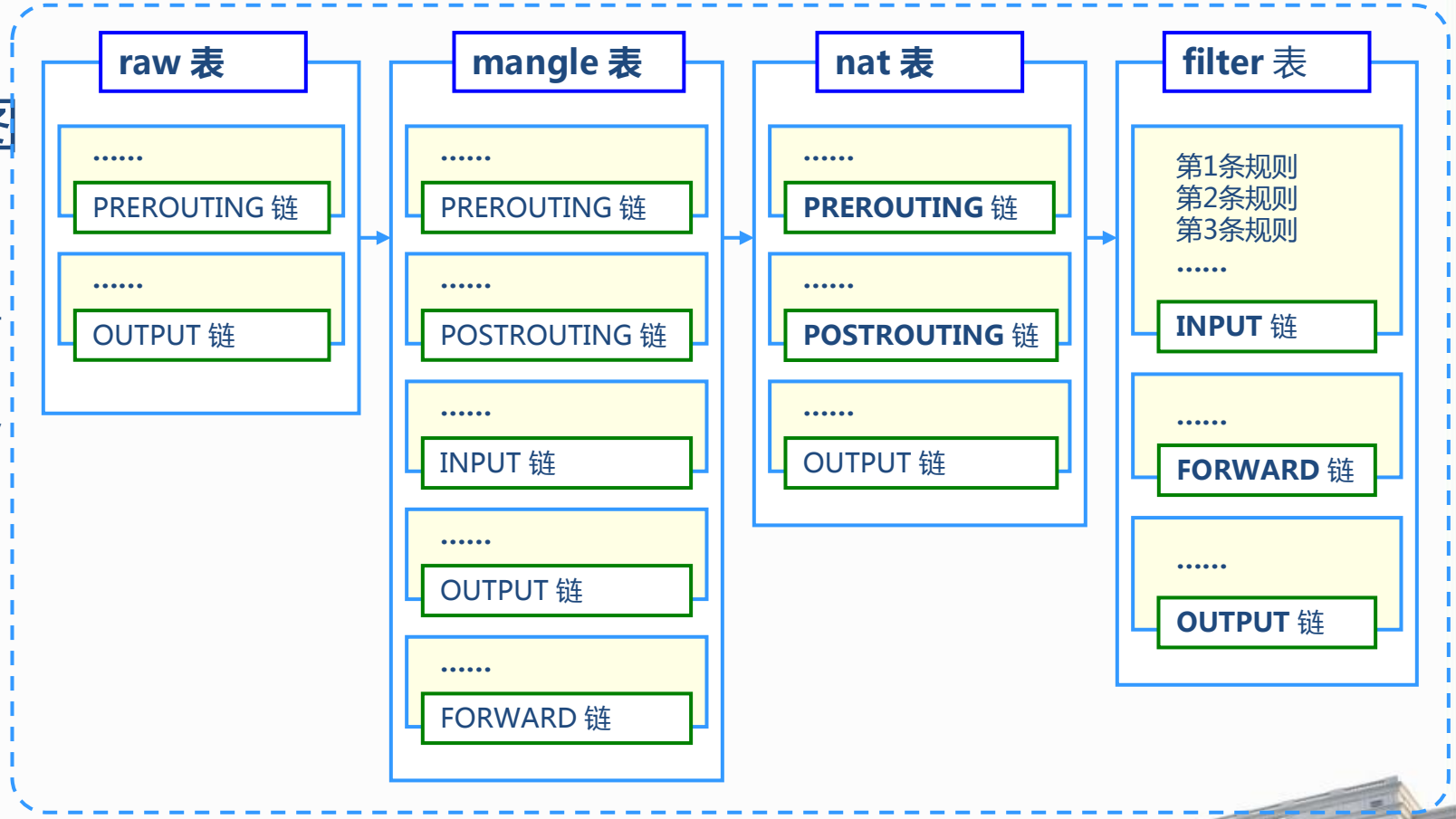
四、防火墙与网络隔离

- 防火墙实例——Iptables 与 Netfilter
  - Netfilter是Linux核心中的一个通用架构，它提供了一系列的“表”（tables），每个表由若干“链”（chains）组成，而每条链可以由一条或数条“规则”（rules）组成。实际上，netfilter是表的容器，表是链的容器，而链又是规则的容器，这些表通过Iptables进行管理。
    - Filter表：主要用于过滤数据包，该表根据系统管理员预定义的一组规则过滤符合条件的数据包；
    - NAT表：主要用于网络地址转换；
    - Mangle表：主要用于对指定数据包进行更改；
    - raw表：主要用于提高性能。

四、防火墙与网络隔离

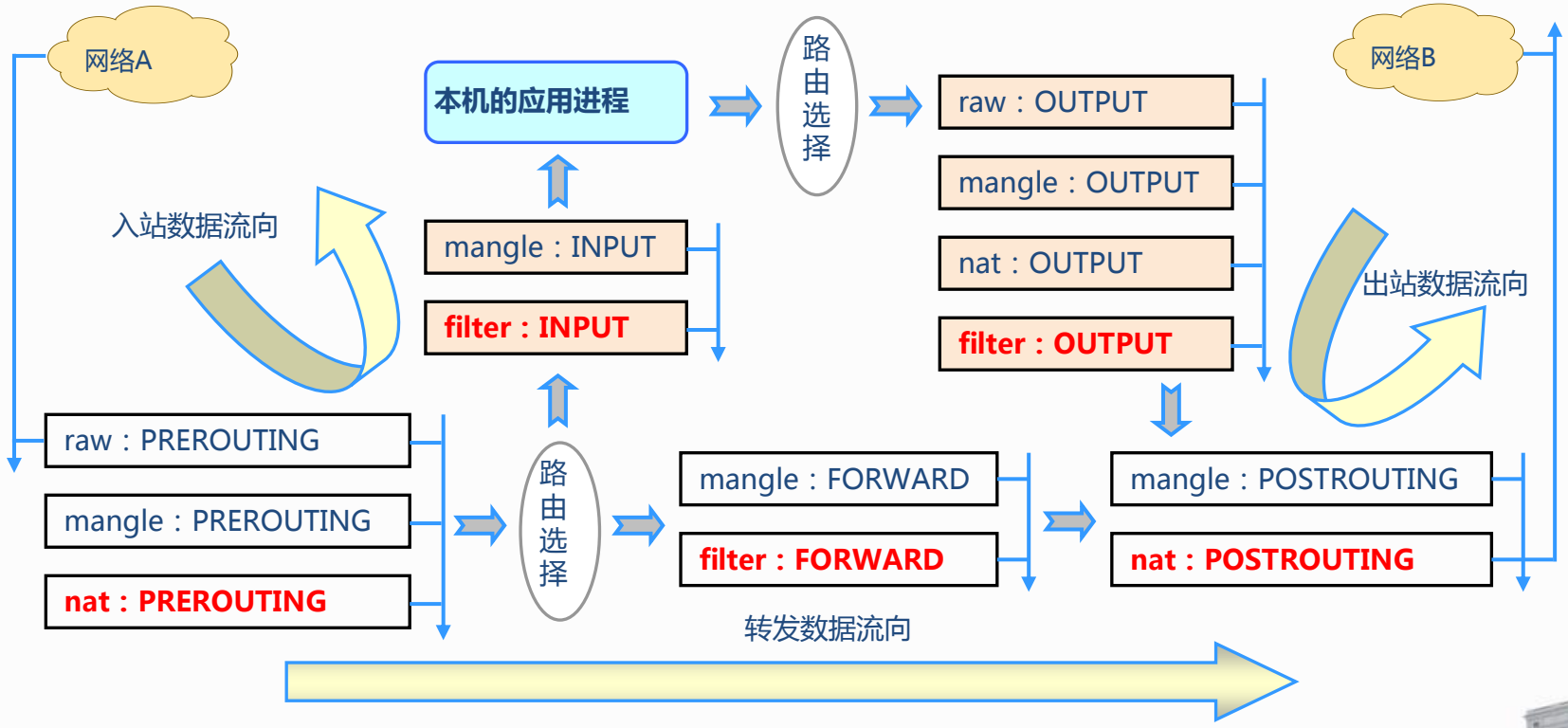
□默认的表、链结构示意图

- INPUT链：处理入站数据包
- OUTPUT链：处理出站数据包
- FORWARD链：处理转发数据包
- POSTROUTING链：在进行路由选择后处理数据包
- PREROUTING链：在进行路由选择前处理数据包



四、防火墙与网络隔离

规则匹配流程图



四、防火墙与网络隔离

Iptables的基本语法

- iptables [-t 表名] 选项 [链名] [条件] [-j 控制类型]

```
[root@localhost ~]# iptables -t filter -I INPUT -p icmp -j REJECT
```

```
C:\Users\Administrator> ping 192.168.4.254
正在 Ping 192.168.4.254 具有 32 字节的数据:
来自 192.168.4.254 的回复: 无法连到端口。
来自 192.168.4.254 的回复: 无法连到端口。
……
```

阻止ping测试

注意事项

- 不指定表名时，默认指filter表
- 不指定链名时，默认指表内的所有链
- 除非设置链的默认策略，否则必须指定匹配条件
- 选项、链名、控制类型使用大写字母，其余均为小写

四、防火墙与网络隔离

添加新的规则

- -A：在链的末尾追加一条规则；
- -I：在链的开头（或指定序号）插入一条规则。

```
[root@localhost ~]# iptables -t filter -A INPUT -p tcp -j ACCEPT
[root@localhost ~]# iptables -I INPUT -p udp -j ACCEPT
[root@localhost ~]# iptables -p 用来指定协议 p -j ACCEPT
```

四、防火墙与网络隔离

- 查看规则列表
  - -L：列出所有的规则条目；-n：以数字形式显示地址、端口等信息；-v：以更详细的方式显示规则信息；--line-numbers：查看规则时，显示规则的序号。

```
[root@localhost ~]# iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
REJECT     icmp --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-
unreachable
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0
```

-n -L 可合写为 -nL

四、防火墙与网络隔离

◘ 删除、清空规则

➢ -D：删除链内指定序号（或内容）的一条规则；-F：清空所有的规则。

```
[root@localhost ~]# iptables -D INPUT 3
[root@localhost ~]# iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0           0.0.0.0/0
```

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -t nat -F
[root@localhost ~]# iptables -t mangle -F
[root@localhost ~]# iptables -t raw -F
```

清空所有表的所有链

四、防火墙与网络隔离

- 设置默认策略
  - -P：为指定的链设置默认规则

```
[root@localhost ~]# iptables -t filter -P FORWARD DROP
[root@localhost ~]# iptables -P OUTPUT ACCEPT
```

默认策略要么是ACCEPT、要么是DROP

四、防火墙与网络隔离

- 常用管理选项汇总

类别	选项	用途
添加新的规则	-A	在链的末尾追加一条规则
	-I	在链的开头（或指定序号）插入一条规则
查看规则列表	-L	列出所有的规则条目
	-n	以数字形式显示地址、端口等信息
	-v	以更详细的方式显示规则信息
	--line-numbers	查看规则时，显示规则的序号
删除、清空规则	-D	删除链内指定序号（或内容）的一条规则
	-F	清空所有的规则
设置默认策略	-P	为指定的链设置默认规则

四、防火墙与网络隔离

◘常见的通用匹配条件

- 协议匹配：-p 协议名；地址匹配：-s 源地址、-d 目的地址；接口匹配：-i 入站网卡、-o 出站网卡

```
[root@localhost ~]# iptables -I INPUT -p icmp -j DROP
[root@localhost ~]# iptables -A FORWARD -p ! icmp -j ACCEPT
```

```
[root@localhost ~]# iptables -A FORWARD -s 192.168.1.11 -j REJECT
[root@localhost ~]# iptables -I INPUT -s 10.20.30.0/24 -j DROP
```

```
[root@localhost ~]# iptables -A INPUT -i eth1 -s 192.168.0.0/16 -j DROP
[root@localhost ~]# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
[root@localhost ~]# iptables -A INPUT -i eth1 -s 172.16.0.0/12 -j DROP
```

外网接口

四、防火墙与网络隔离

- 常用的隐含匹配条件
  - 端口匹配：--sport 源端口、--dport 目的端口

```
[root@localhost ~]# iptables -A FORWARD -s 192.168.4.0/24 -p udp --dport 53 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p tcp --dport 20:21 -j ACCEPT
```

- 常见匹配条件汇总

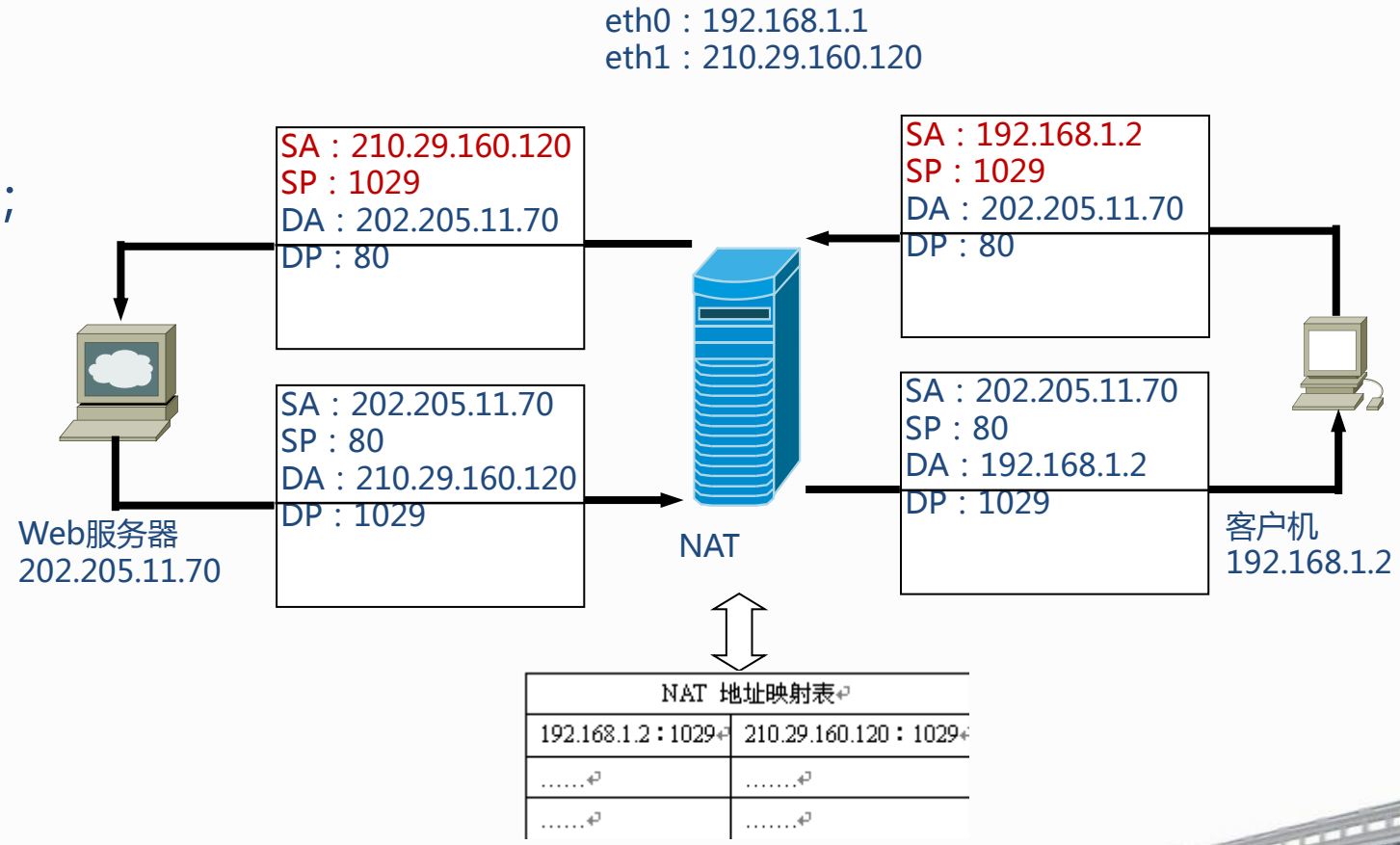
类别	条件类型	用法
通用匹配	协议匹配	-p 协议名
	地址匹配	-s 源地址、-d 目的地址
	接口匹配	-i 入站网卡、-o 出站网卡
隐含匹配	端口匹配	--sport 源端口、--dport 目的端口

- 测试点 6-2
  - 简述防火墙的典型技术分类与特点。
  - 简述防火墙的典型体系架构及特点。
  - 如果允许IP地址为192.168.1.212的内网主机访问外部网络的Web服务，但禁止该主机使用邮件服务（SMTP，POP3），请给出防火墙应当配置的规则
  - 在Linux系统中通过Iptables配置上述过滤规则，并验证规则的有效性。（选做）

五、地址转换与虚拟专网

网络地址转换NAT

- 隐藏了内部网络的结构；
- 内部网络可以使用私有IP地址；
- 公开地址不足的网络可以使用这种方式提供IP复用功能。

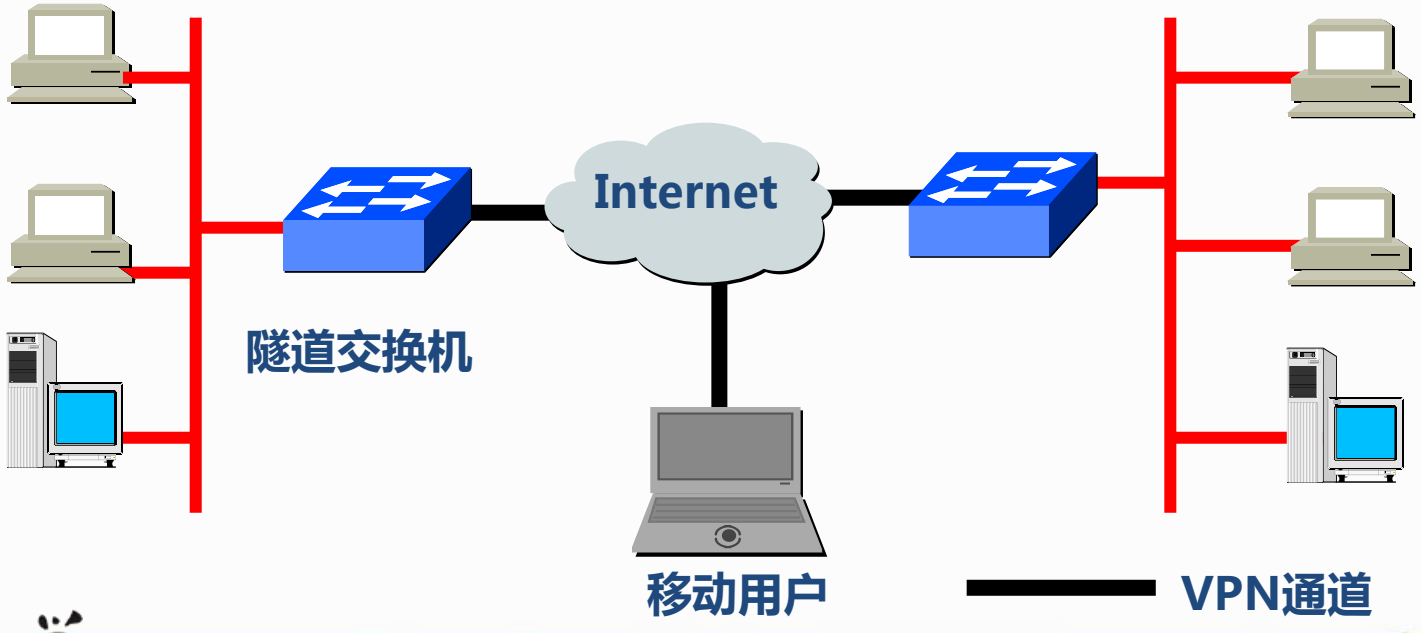


五、地址转换与虚拟专网

- 网络地址转换NAT的实现方式
  - 静态转换（Static NAT）
    - 是指将内部网络的私有IP地址与公有IP地址进行一一对应的转换。
  - 动态转换（Dynamic NAT）
    - 是指将内部网络的私有IP地址转换为公用IP地址时，IP地址是不确定的，是随机的。
  - 网络地址端口转换（NAPT）
    - 是指改变外出数据包的源端口并进行端口转换，内部网络的所有主机均可共享一个合法外部IP地址实现对Internet的访问，从而可以最大限度地节约IP地址资源。

五、地址转换与虚拟专网

- 虚拟专网VPN
  - VPN（Virtual Private Network）技术是指在公共网络中建立专用网络，数据通过安全的“加密管道”在公共网络中传播。



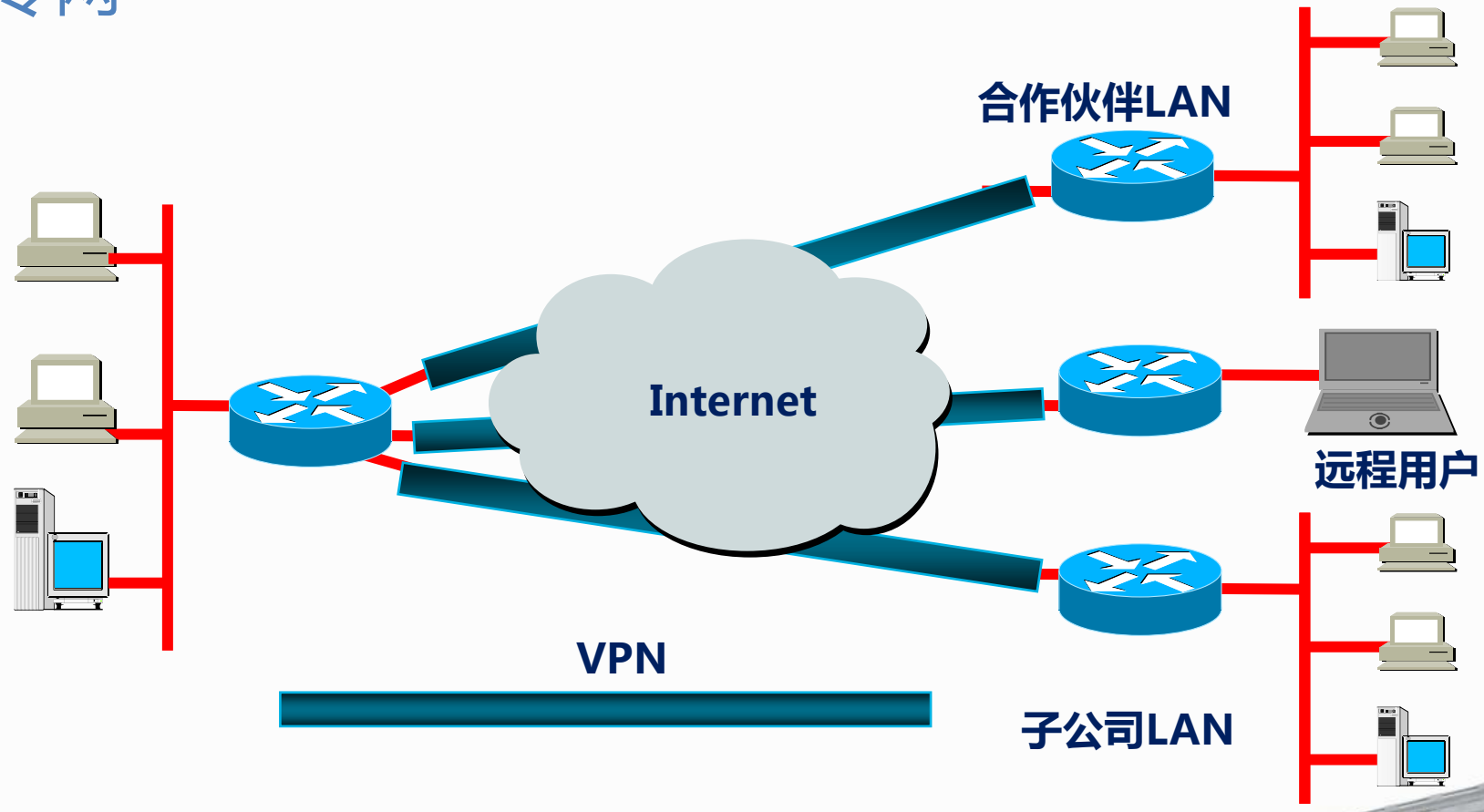
五、地址转换与虚拟专网

VPN的功能

- 保证数据的完整性：接收到的数据必须与发送时的一致，要有抵抗不法分子篡改数据的能力；
- 保证通道的机密性：提供强有力的加密手段，必须使偷听者不能破解拦截到的通道数据；
- 提供动态密钥交换功能：提供密钥中心管理服务器，必须具备防止数据重演(Replay)的功能，保证通道不能被重演；
- 提供安全防护措施和访问控制：要有抵抗黑客通过VPN通道攻击企业网络的能力，并且可以对VPN通道进行访问控制(Access Control)。

五、地址转换与虚拟专网

- VPN的分类
  - 内部VPN
  - 远程访问VPN
  - 外联网VPN



五、地址转换与虚拟专网

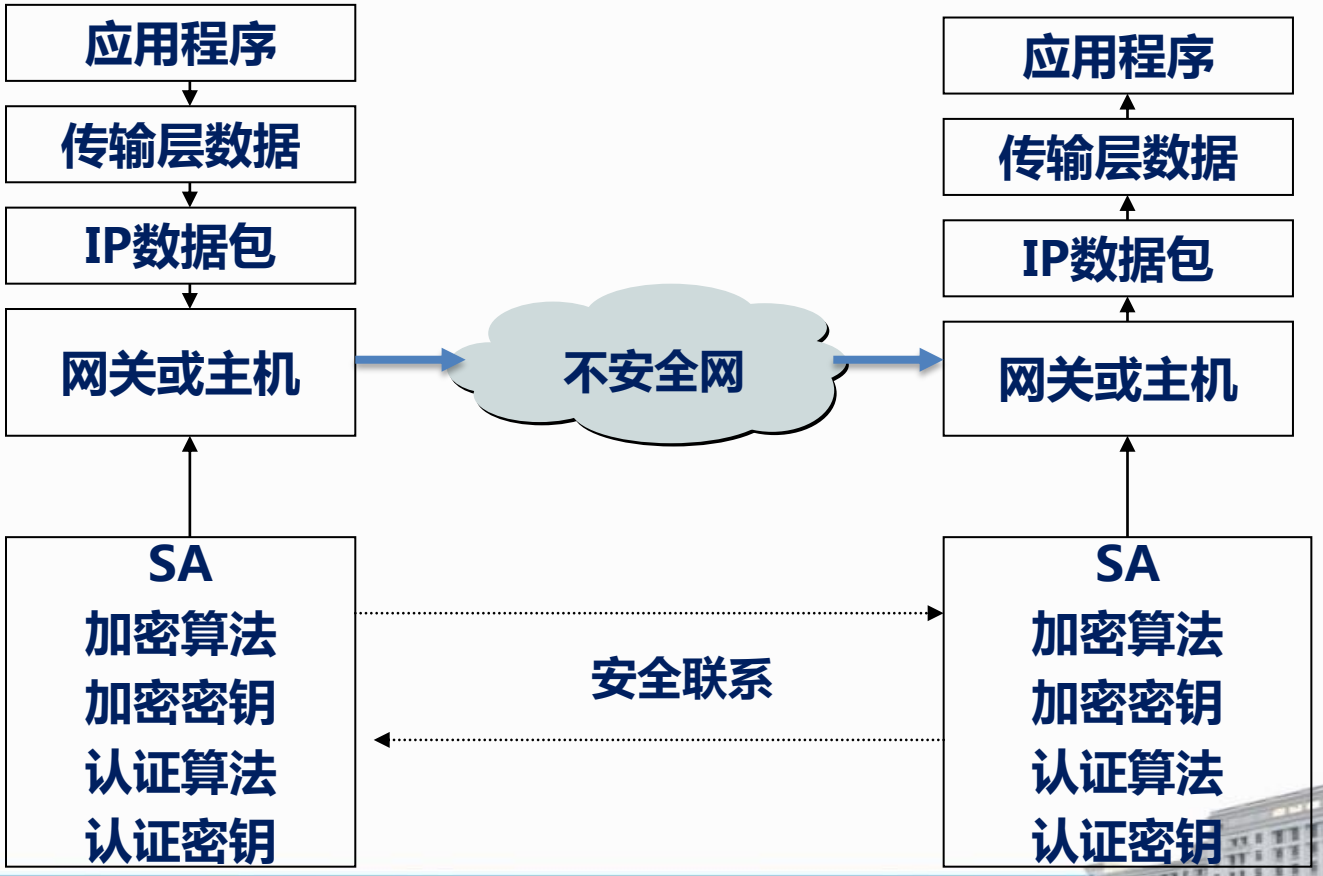
VPN的实现

- VPN通过采用专用的隧道协议实现对网络报文的封装和透明传输。

OSI七层模型	安全协议
会话层 传输层	SOCK V5 SSL
网络层 数据链路层 物理层	IPSec PPTP/L2TP

五、地址转换与虚拟专网

- IPsecVPN工作原理
  - AH
  - ESP
  - IKE



第六讲 网络隔离技术

- 测试点6-3
  - NAT有几种转换方式？简述其工作原理与特点。
  - VPN可提供哪些基本安全功能？如果一个企业需要在分支机构间提供安全通信，以及让出差的员工访问内部资源，请给出一个基于VPN技术的解决方案

六、物理隔离

- 什么是物理隔离？
  - 所谓“物理隔离”是指内部网在任何情况下不得直接或间接地连接公共网。物理安全的目的是保护路由器、工作站、各种网络服务器等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击。
  - 《计算机信息系统国际联网保密管理规定》第二章保密制度第六条规定：“涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离。

六、物理隔离

物理隔离的类型

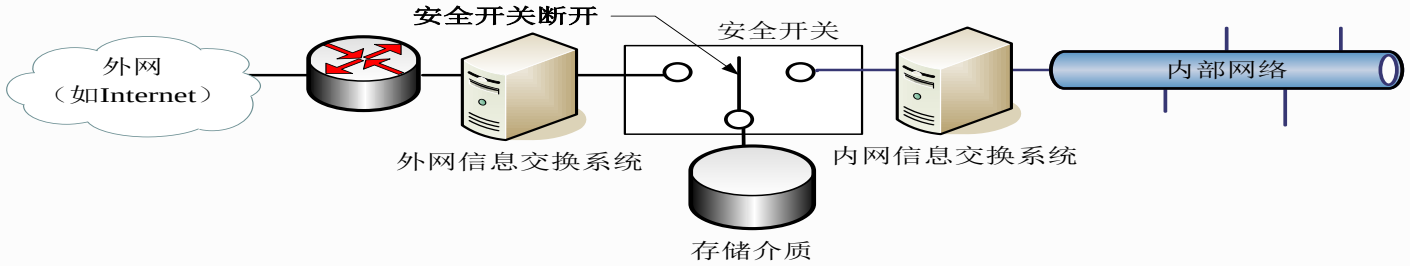
- 双网双机：两台计算机共用一套外部设备，通过开关选择两套计算机系统。
- 双硬盘物理隔离卡：通过增加一块隔离卡、一块硬盘，将硬盘接口通过添加的隔离卡转接到主板，网卡也通过该卡引出两个网络接口。
- 单硬盘物理隔离：增加一块隔离卡，引出两个网口，并对原有硬盘划分安全区、非安全区。（非严格的物理隔离）
- 隔离网关（网闸）:内、外部主机是完全网络隔离的，支持文件、数据或信息的交换。

六、物理隔离

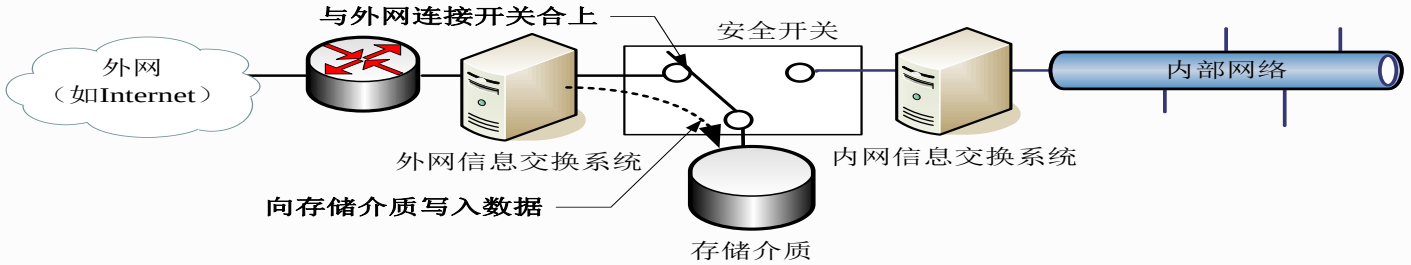
- 物理隔离的工作模式
  - 单向隔离：在端上依靠由硬件访问控制信息交换分区实现信息在不同的安全域信息单向流动。
  - 协议隔离：通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。
  - 网闸隔离：位于两个不同安全域之间，通过协议转换的手段，以信息摆渡的方式实现数据交换。只有被系统明确要求传输的信息可以通过。

六、物理隔离

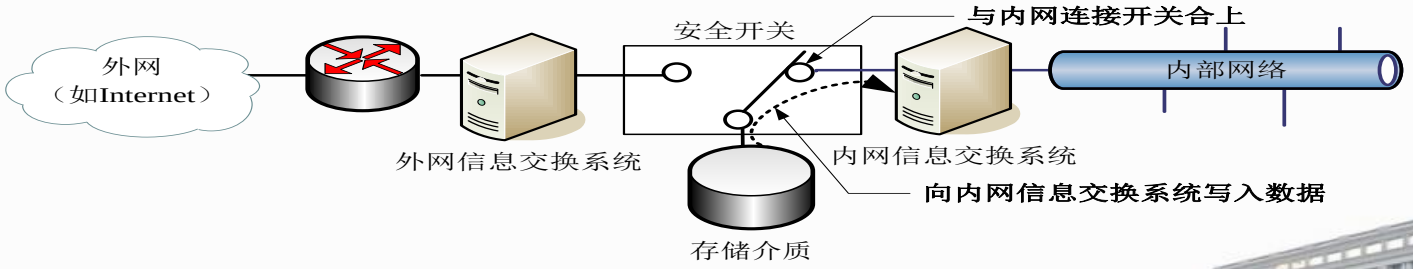
- 网闸工作示意图



（a） 存储介质、外网、内网三者之间完全断开



（b） 从外网向存储介质写入数据



（c） 从存储介质向内网信息交换系统写入数据

六、物理隔离

- 物理隔离VS逻辑隔离
  - 物理隔离的哲学是要安全就不连网，要绝对保证安全。
  - 逻辑隔离的哲学是在保证网络正常使用下，尽可能安全。

	隔离网闸	防火墙
政策归类	安全隔离与信息交换	防火墙
功能定位	安全第一，通信第二	通信第一，安全第二
硬件体系	多机系统	单机系统
通信协议	专用私有协议	公用协议
安全级别	内外皆防	防外

第六讲 网络隔离技术

- 测试点 6-4
  - 简述物理隔离的类型与工作模式。

结束语

感谢聆听!

特别说明：PPT中所有来自于网络的图片和素材仅用于教学，并保证在未经原作者同意的情况下，不用于任何商业目的。