访问控制原理

- **什么是访问控制?**
  - **访问控制在生活中经常遇到，例如：门锁、交通灯；**
  - **访问控制是允许或者禁止某人使用某项资源的能力。**
  - **主体：提出资源访问请求**
  - **客体：被访问资源实体**
  - **访问：对资源的使用**

  例如：读、写、删改等操作

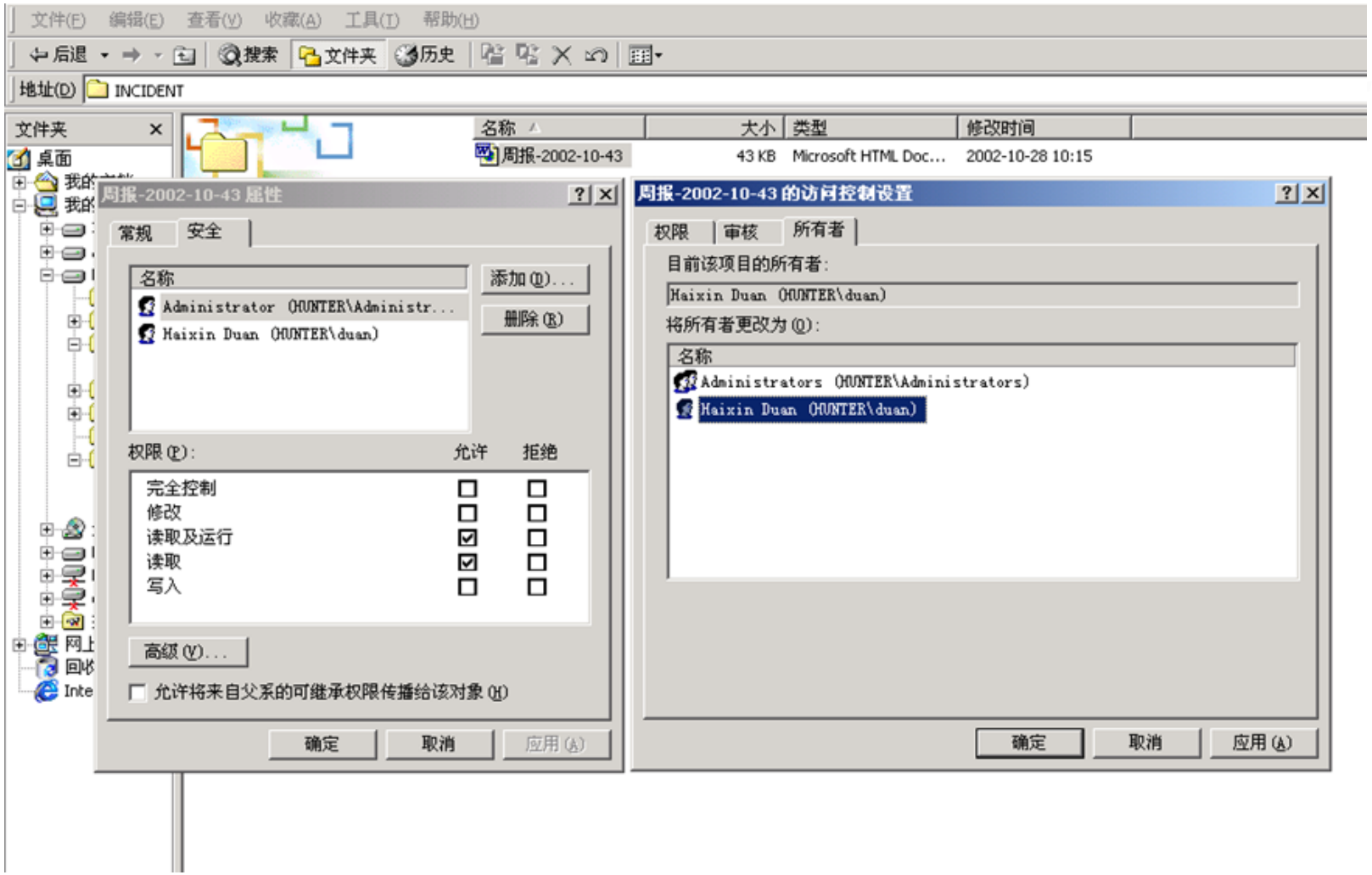
访问控制原理

- **访问可以被描述为一个三元组（s, o, a）**
  - **主体：Subject**
  - **客体：Object**
  - **访问：Access**

访问控制原理

- 访问控制模型（ISO版本）

访问控制原理


文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹 历史
地址(D) INCIDENT
文件夹
桌面
名称 大小 类型 修改时间
周报-2002-10-43 43 KB Microsoft HTML Doc... 2002-10-28 10:15
周报-2002-10-43 属性
常规 安全
名称
Administrator (HUNTER\Administr...
Haixin Duan (HUNTER\duan)
添加(D)...
删除(R)
权限(P): 允许 拒绝
完全控制
修改
读取及运行
读取
写入
高级(V)...
允许将来自父系的可继承权限传播给该对象(H)
确定 取消 应用(A)
周报-2002-10-43 的访问控制设置
权限 审核 所有者
目前该项目的所有者:
Haixin Duan (HUNTER\duan)
将所有者更改为(O):
名称
Administrators (HUNTER\Administrators)
Haixin Duan (HUNTER\duan)
确定 取消 应用(A)

访问控制原理

- **访问控制**
  - **访问控制是信息安全保障机制的核心内容，它是实现数据保密性和完整性机制的主要手段**
  - **访问控制是为了限制访问主体（或称为发起者，是一个主动的实体；如用户、进程、服务等），对访问客体（需要保护的资源）的访问权限，从而使计算机系统在合法范围内使用**
  - **访问控制机制决定用户及代表一定用户利益的程序能做什么，及做到什么程度。**

访问控制原理

- **访问控制模型**
  - **规范的访问控制模型是实现严格访问控制策略所必须**
  - **1985年美国军方提出了可信计算机系统评估准则TCSEC，描述了两种著名的访问控制策略：自主访问控制模型（DAC）和强制访问控制模型（MAC），对应有几个数学模型**
  - **1992年Ferraiolo和Kuhn提出基于角色的访问控制(RBAC)**
  - **为一些应用场景又提出了基于对象和基于任务的访问控制**

访问控制原理

- **基本的访问控制政策模型**
  - **自主访问控制（DAC）**

    Discretionary Access Control
  - **强制访问控制（MAC）**

    Mandatory Access Control
  - **基于角色的访问控制（RBAC）**

    Role-Based Access Control

访问控制原理

- **基本的访问控制政策模型**
  - **自主访问控制（DAC)**
  - **每个客体有一个所有者，所有者可以按照自己的意愿把客体的访问控制权限授予其他主体**
  - **控制灵活，易于管理，是目前应用最为普遍的访问控制政策**
  - **DAC的有效性依赖于资源的所有者对安全政策的正确理解和有效落实**

访问控制原理

- **基本的访问控制政策模型**
  - **自主访问控制（DAC）**

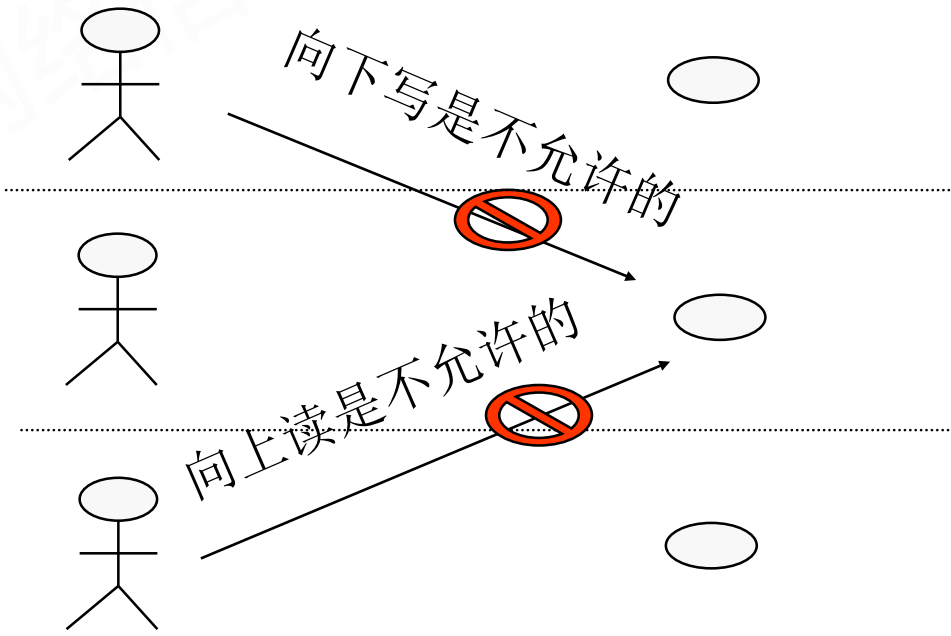
```
/bin/ls
[root@acl tmp]# chown root ls
[root@acl tmp]# ls -l
-rw-r--r--    1 nobody  nobody     770    Oct 18 15:16 4011.tmp
-rw-------    1 root    users      48     Oct 28 11:41 ls
srwxrwxrwx    1 root    root       0      Aug 29 09:04 mysql.sock
drwxrwxr-x    2 duan    uan        4096   Oct 23 23:41 ssl
[root@acl tmp]# chmod   o+rw   ls
[root@acl tmp]# ls -l
-rw-r--r--    1 nobody  nobody     770    Oct 18 15:16 4011.tmp
-rw----rw-    1 root    users      48     Oct 28 11:41 ls
srwxrwxrwx    1 root    root       0      Aug 29 09:04 mysql.sock
drwxrwxr-x    2 duan    duan       4096   Oct 23 23:41 ssl
[root@acl tmp]#
```

访问控制原理

- **基本的访问控制政策模型**
  - **强制访问控制（MAC)**
  - **每个主体和客体分配一个固定的安全级别，只有系统管理员才可以修改**
  - **普密<秘密<机密<绝密**
  - **只有在主体和客体的安全级别满足一定规则时，才允许访问**
  - **MAC通过定义的安全级别，达到访问控制**
  - **常用于军队和政府机构**

访问控制原理

- **基本的访问控制政策模型**
  - **强制访问控制（MAC)**
  - **例如：BLP模型是最早的一个安全模型，用于美国军方**
  - **BLP的特点：**
    - **禁止向下写**
    - **禁止向上读**
    - **低安全级信息向上流动**
    - **高读底合法，有安全漏洞**



访问控制原理

- **基本的访问控制政策模型**
  - **基于角色的访问控制（RBAC）**
  - **用户组（Group）**
    - **用户组：用户的集合，$G=\{s_1, s_2, s_3 \ldots\}$**
  - **角色（Role）**
    - **角色是完成一项任务必须访问的资源及相应操作权限的集合，**

      $R=\{(a_1,o_1), (a_2,o_2), (a_3,o_3)\ldots\}$

访问控制原理

- **基本的访问控制政策模型**
  - **基于角色的访问控制（RBAC)**
  - **授权管理：**
    - **根据任务需要定义角色**
    - **为角色分配资源和操作权限**
    - **给一个用户组指定一个角色**
  - **RBAC通过角色，隔离了主体和权限**

访问控制的设计原则

- （1）最小特权原则
- （2）开放式设计原则
- （3）特权的分隔原则
- （4）公共机制的最小化原则
- （5）经济性原则
- （6）心理可接受原则

访问控制的设计原则

- （1）最小特权原则
  - 每一用户和进程只应拥有最小访问权的集合，只能在为完成其任务所必须的那些权限所组成的最小保护域内执行。
  - 这一原则能够限制差错或恶意攻击产生的危险，是抑制特洛伊木马和实现可靠程序的基本措施。
  - 方便程序的正确性证明和维护，因为程序能涉及的范围减少了，使得证明与维护中考虑的因素相应地减少了。

访问控制的设计原则

- **（2）开放式设计原则**
  - **机制的安全性不应建立在秘密设计或攻击者的无能上，例如密码系统的设计**
  - **任何秘密应在口令或密钥中，而不是在机制本身**
  - **公开性的设计可以受到许多专家的审查与验证，也可以在用户间增加信任感。**

访问控制的设计原则

- **（3）特权的分隔原则**
  - **如有可能，对客体的访问应取决于不止一个条件被满足，即把访问某个客体的权利分解为多个子权利，分别由不同的主体掌握，只有这些子权利同时满足才能对客体进行访问。**
  - **例如，主密钥的恢复必须多于K个子密钥，使得少数不良分子就难以泄漏出主密钥**

访问控制的设计原则

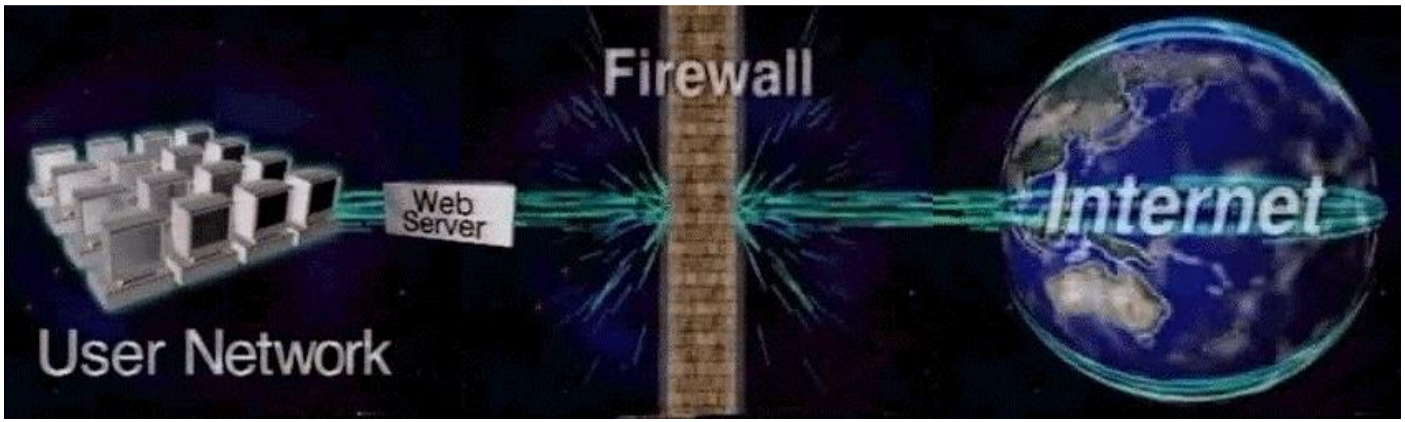
- **（4）公共机制的最小化原则**
  - **公共机制是指由多用户共享的机制**
  - **提供了隐蔽信道的可能性，不利于系统安全，应该最小化。**
  - **这一原则产生了提供分隔各用户的隔离机制**
  - **隔离是通过硬件的物理分离（如分布式系统）或利用虚拟机的逻辑分离实现的，例如：网闸**

本节大纲

- 访问控制原理
- 防火墙技术概述
- 防火墙核心技术
- 防火墙部署

防火墙技术概述

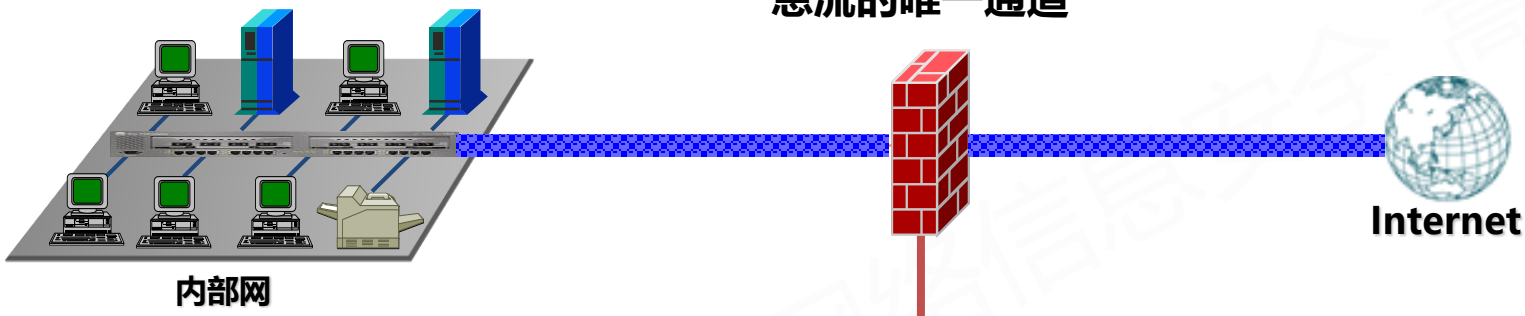
- **什么是防火墙?**
  - **防火墙是在两个网络(通常是用户内部网络和Internet)之间实施访问控制政策的一个或一组系统（硬件、软件的组合）**
  - **定义：在两个信任程度不同的网络之间设置的、用于加强访问控制的软硬件保护设施**



防火墙技术概述

- 什么是防火墙?

两个安全域之间信息流的唯一通道



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

能根据有关的安全政策控制（允许、拒绝、监视、记录、限流等）进出网络的访问行为。

防火墙技术概述

- **软件防火墙和硬件防火墙**
  - 硬件防火墙，速度快，适合局域网

    它是指把防火墙程序做到芯片里面

    由硬件执行这些功能，能减少CPU的负担，使路由更稳定。

    价格较贵，但效果较好，适用于中大型企业。

  - 软件防火墙，速度较慢，适合单机

    通过软件的方式来实现，价格较低，

    但这类防火墙只能通过一定的规则来达

    到限制一些非法用户访问内部网的目的。

防火墙技术概述

- **防火墙能做什么?**
  - **防火墙可以在网络边界实施访问控制政策**
  - **防火墙可以记录所有的访问**
  - **防火墙可以隐藏内部网络，限制暴露内部用户点**

防火墙技术概述

- **防火墙不能做什么?**
  - **防火墙自身不会正确的配置，需要用户定义访问控制规则**
  - **防火墙防外不防内，不能防止内部恶意的攻击者**
  - **防火墙无法控制没有经过它的连接**
  - **防火墙无法防范全新的威胁和攻击**
  - **防火墙不能很好的实现内容防范，比如病毒等**

防火墙技术概述

- **关于防火墙的争议**
  - **防火墙破坏了Internet端到端的特性，阻碍了新应用的发展**
  - **防火墙没有解决主要的安全问题，即网络内部的安全问题**
  - **防火墙给人一种误解，降低了人们对主机安全的意识**
- **关于防火墙的测试**
  - **防火墙测试标准：RFC2979**

防火墙技术概述

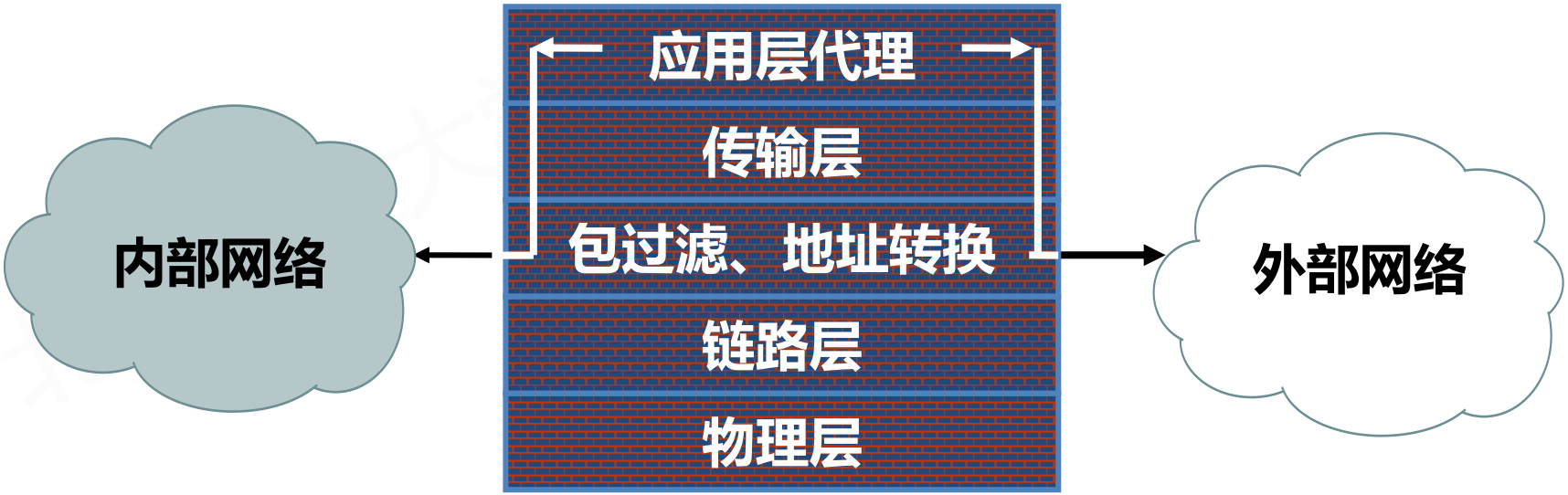
- **防火墙的发展趋势**
  - **优良的性能，支持万兆网络（10Gbps）**
  - **可扩展的结构和功能，与网络入侵检测等系统联动**
  - **简化的安装与管理**
  - **主动过滤（被动过滤——根据黑名单操作）**
  - **通过DPI（深度包检测）技术来防病毒与防黑客**

本节大纲

- 访问控制原理
- 防火墙技术概述
- 防火墙核心技术
- 防火墙部署

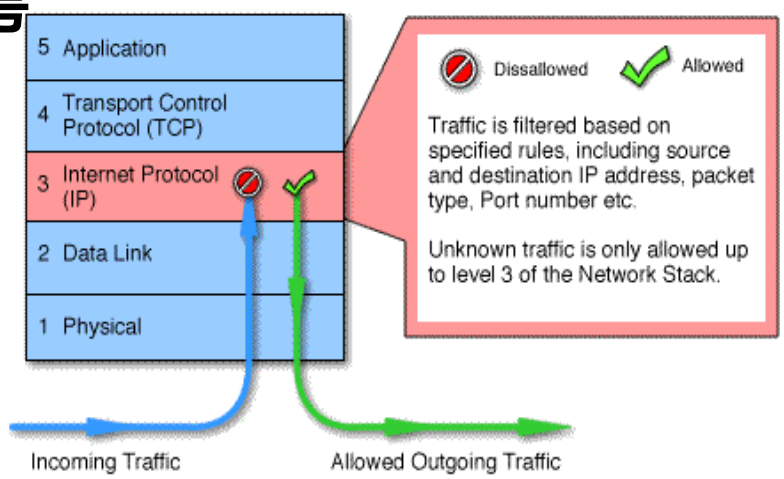
防火墙核心技术

- 包过滤技术(Packet filtering)
- 应用层代理(Proxy)
- 地址转换（NAT)



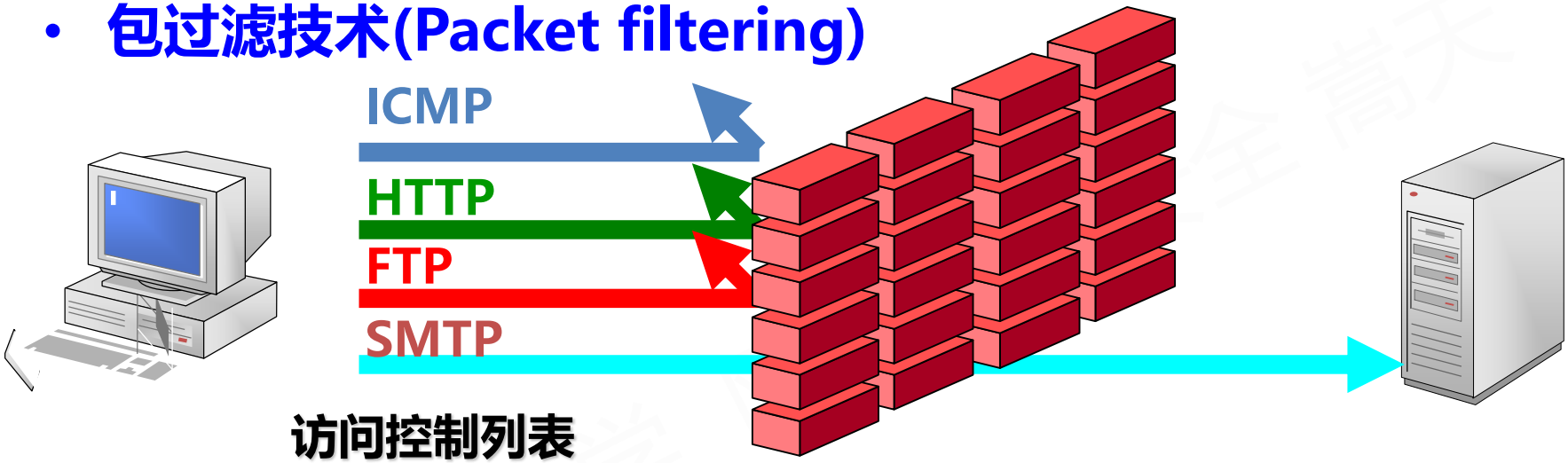
防火墙核心技术

- **包过滤技术(Packet filtering)**
  - **工作在网络层，称为Packet filter**
  - **基于以下信息对经过的每一个包进行检查：**
    - **IP 源地址和目标地址**
    - **TCP/UDP源端口号和目标端口号**
    - **协议 (TCP, UDP,ICMP, BGP等)**
    - **ICMP的消息类型**
    - **包的大小**



防火墙核心技术

- 包过滤技术(Packet filtering)



访问控制列表

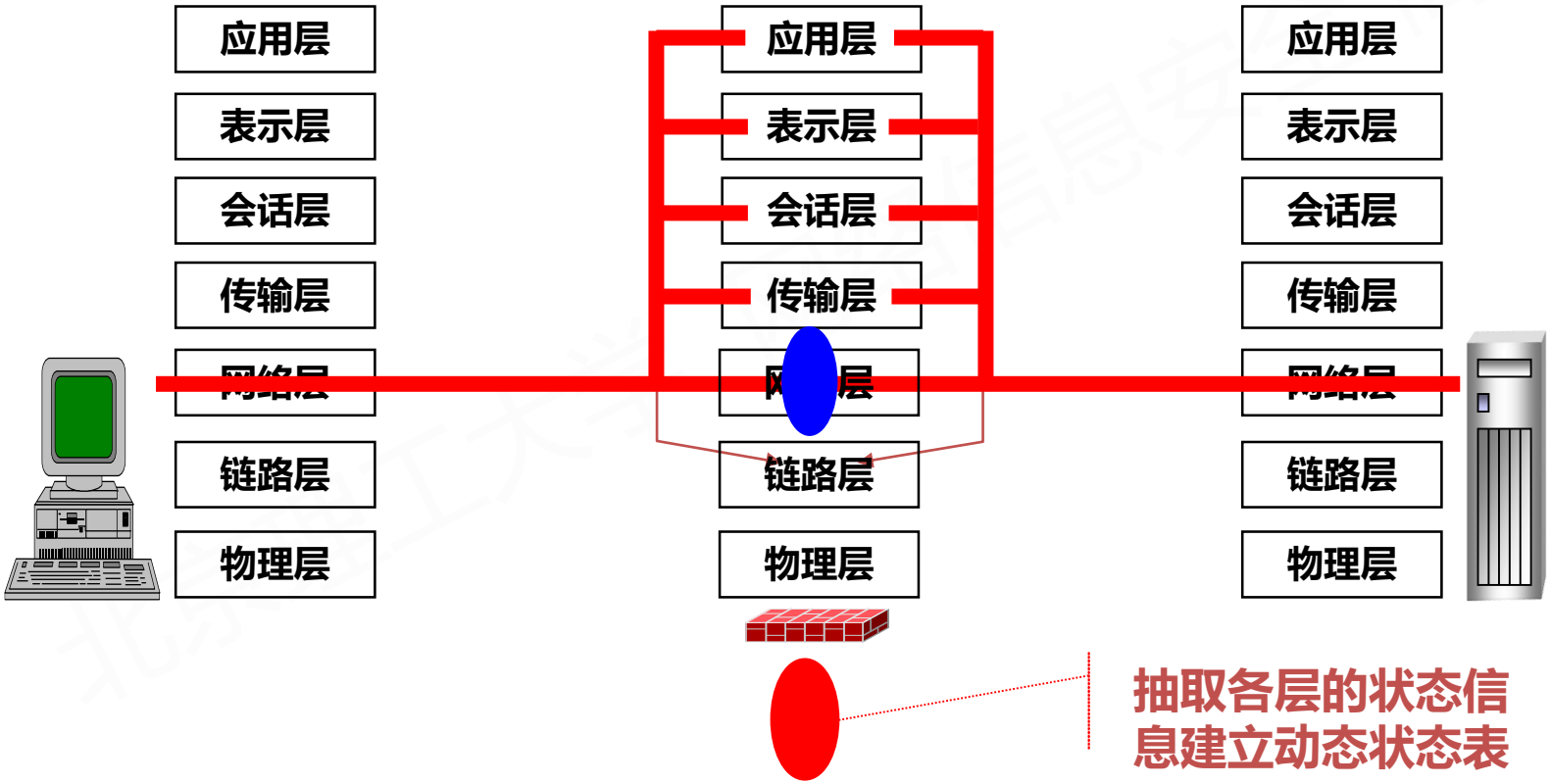
通讯协议	源端		目的端		动作方式
	地址	端口	地址	端口	
TCP	Any	Any	Any	25	允许
TCP	Any	Any	Any	21	拒绝
TCP	Any	Any	Any	80	拒绝
ICMP	Any	Any	Any	---	拒绝
Any	Any	Any	Any	Any	拒绝

防火墙核心技术

- **包过滤技术(Packet filtering)**
  - **在判断数据包时不关心包具体内容，可完成类似操作：**
    - **不让任何用户从外部网用Telnet登录**
    - **允许任何用户使用SMTP往内部网络发送电子邮件**
    - **不让用户登录和使用QQ等即时通信软件**
    - **不让用户访问特定网站**
  - **不能完成类似操作：**
    - **允许某个用户从外部网用Telnet登录而不允许其他用户登录**
    - **允许用户传送一些文件而不允许用户传送其他文件。**

防火墙核心技术

- 动态包过滤技术（状态检测技术）

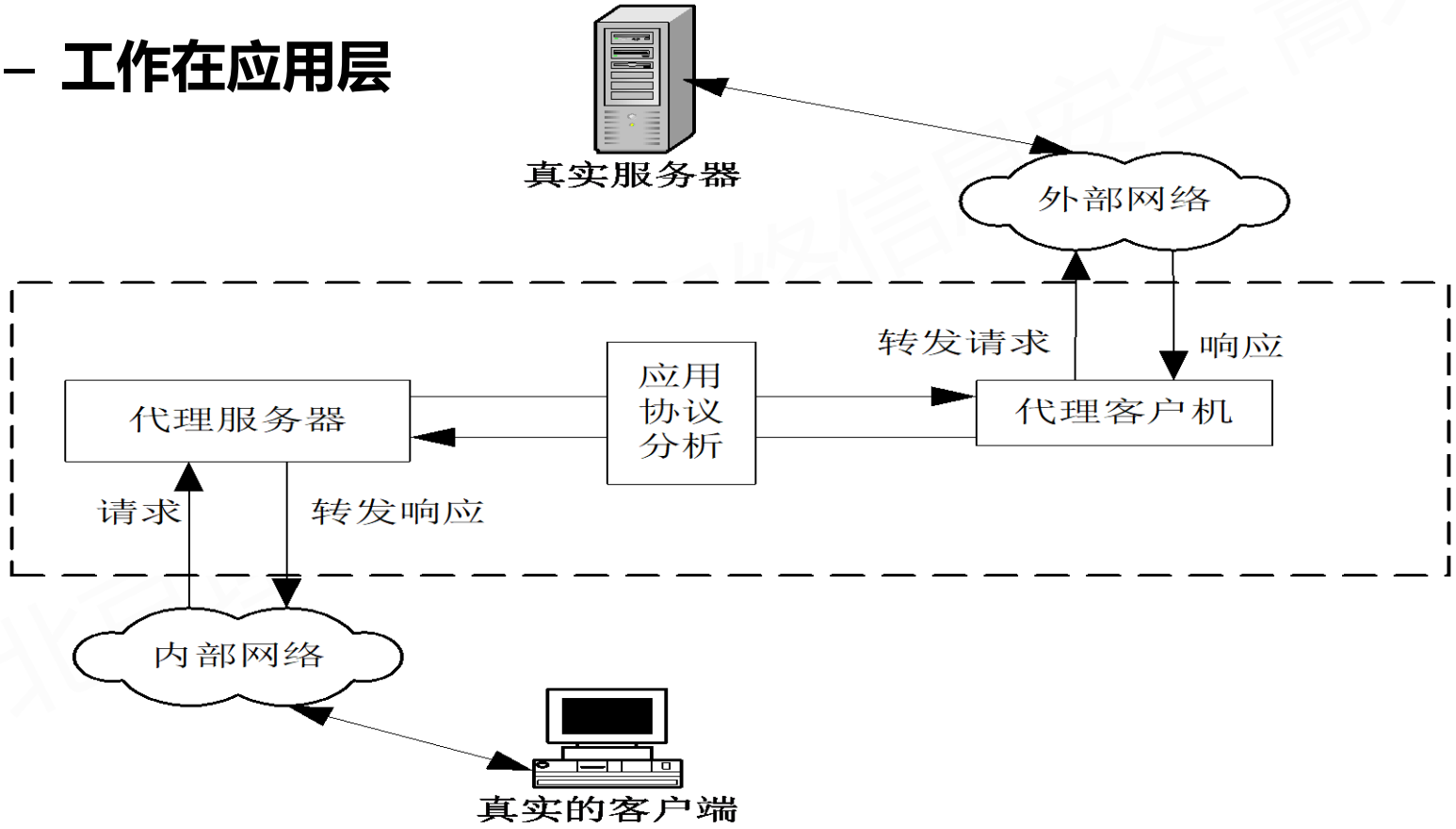


防火墙核心技术

- **包过滤技术(Packet filtering)**
  - **优点**
    - **可以保护所有的服务**
    - **对应用透明**
    - **较高的网络性能**
    - **成本较低**
  - **缺点**
    - **无法实施细粒度的访问控制政策**
    - **不能防止IP欺骗**
    - **规则配置复杂**
    - **降低路由器的性能**

防火墙核心技术

- **应用层代理(Application Layer)**
  - **工作在应用层**

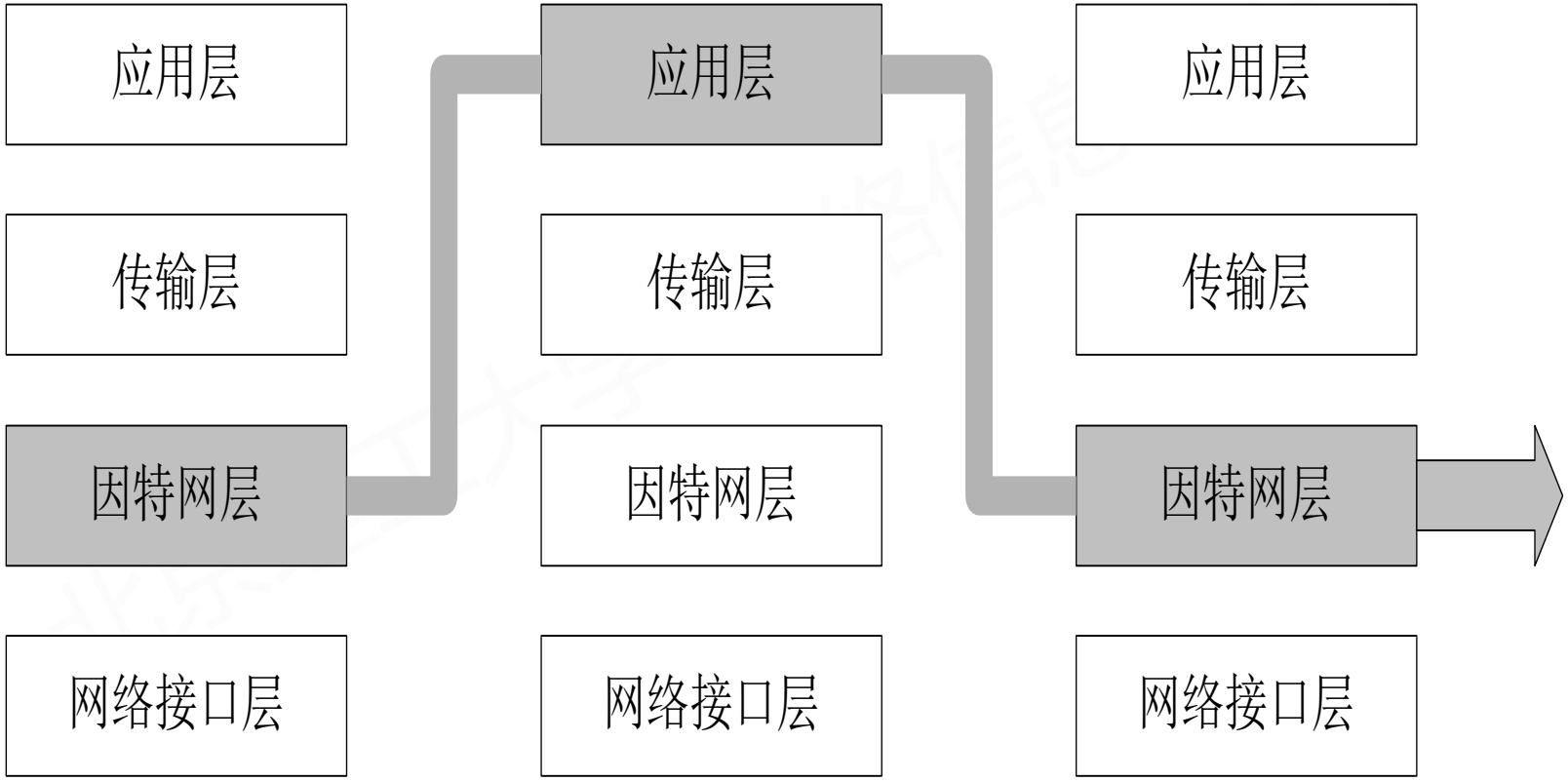


防火墙核心技术

- **应用层代理(Application Layer)**
  - **针对特定协议，比如telnet，http，smtp，pop等**
  - **可以支持身份认证功能**
  - **除了基于地址、协议、端口的控制以外，还可以支持应用层命令的过滤，比如FTP的GET, PUT等**
  - **常用软件：squid，wingate等**

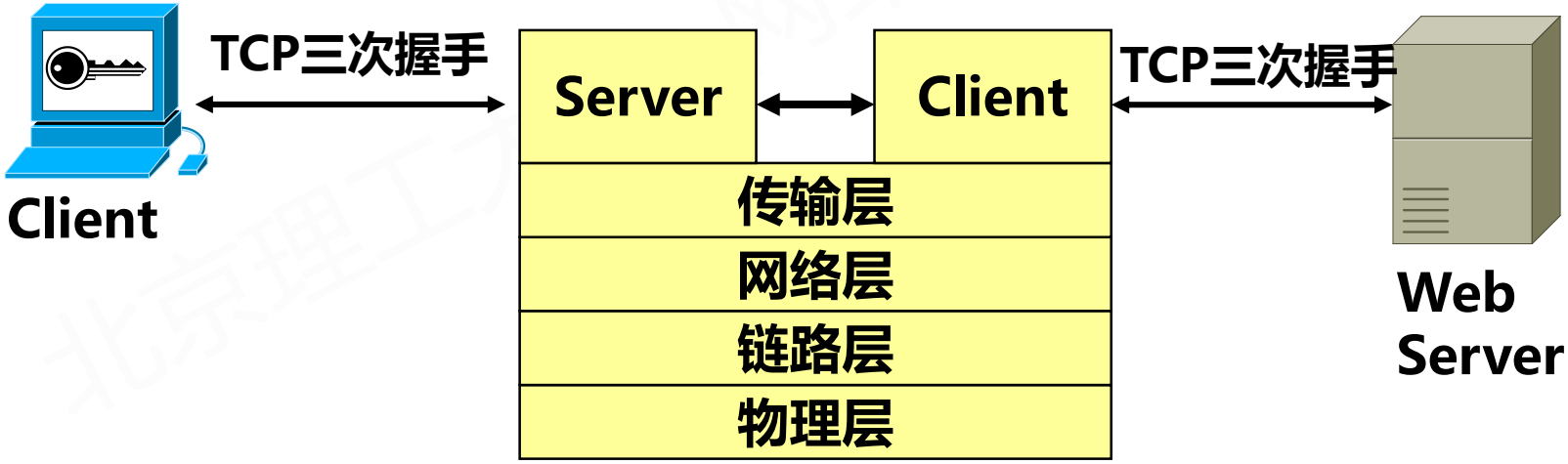
防火墙核心技术

- **应用层代理(Application Layer)**



防火墙核心技术

- **应用层代理(Application Layer)**
  - **Web应用层防火墙**

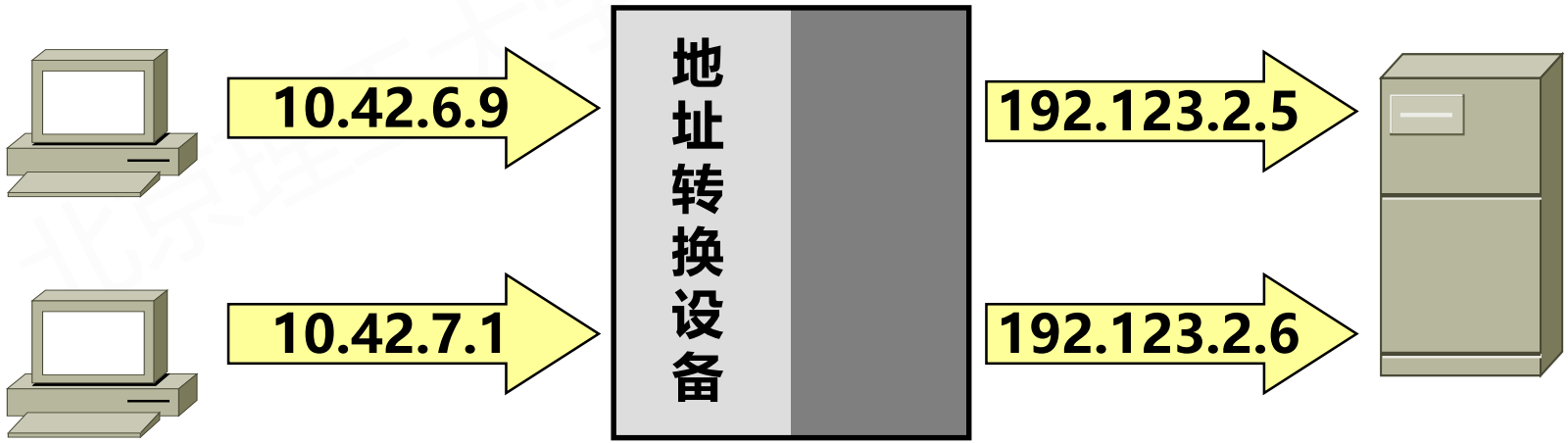


防火墙核心技术

- **应用层代理(Application Layer)**
  - **优点**
    - **参与TCP连接的全过程**
    - **在应用层上建立协议过滤**
    - **保持状态，可以检测并防范SYN Flood类型的攻击**
  - **缺点**
    - **速度相对较慢**
    - **性能的开销较大**
    - **防火墙本身易受攻击**

防火墙核心技术

- **地址转换（NAT, Network Address Translation）**
  - **类似路由器，工作在网络层**
  - **除了转发以外，完成地址转换**
  - **不能提供额外的安全性，但是可以隐蔽内部网络**



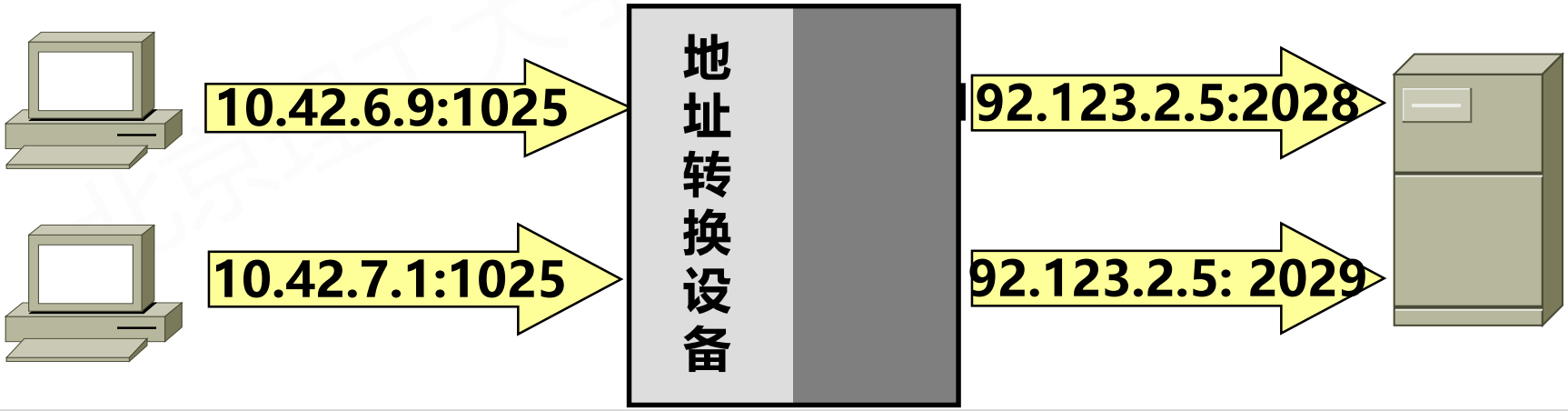
防火墙核心技术

- **地址转换（NAT）**
  - **防火墙规则实例**

序号	防火墙IP	防火墙端口	内部服务器IP	内部服务器端口
1	202.99.88.2	80	192.168.1.144	80
2	202.99.88.2	21	192.168.1.144	21

防火墙核心技术

- **地址转换（NAT）**
  - **转换方式**
    - **静态地址转换**
    - **动态地址转换**
    - **静态地址转换 + 端口映射（Port Mapping）**
    - **动态地址转换 + 端口映射**



防火墙核心技术

- **地址转换（NAT）**
  - **优点**
    - **节省IP地址资源**
    - **隐蔽内部的网络**
  - **缺点**
    - **地址转换破坏了IP包的完整性**
    - **动态地址转换必须保留状态**
    - **Log 变得困难**
    - **端口映射使得包过滤变得困难**

本节大纲

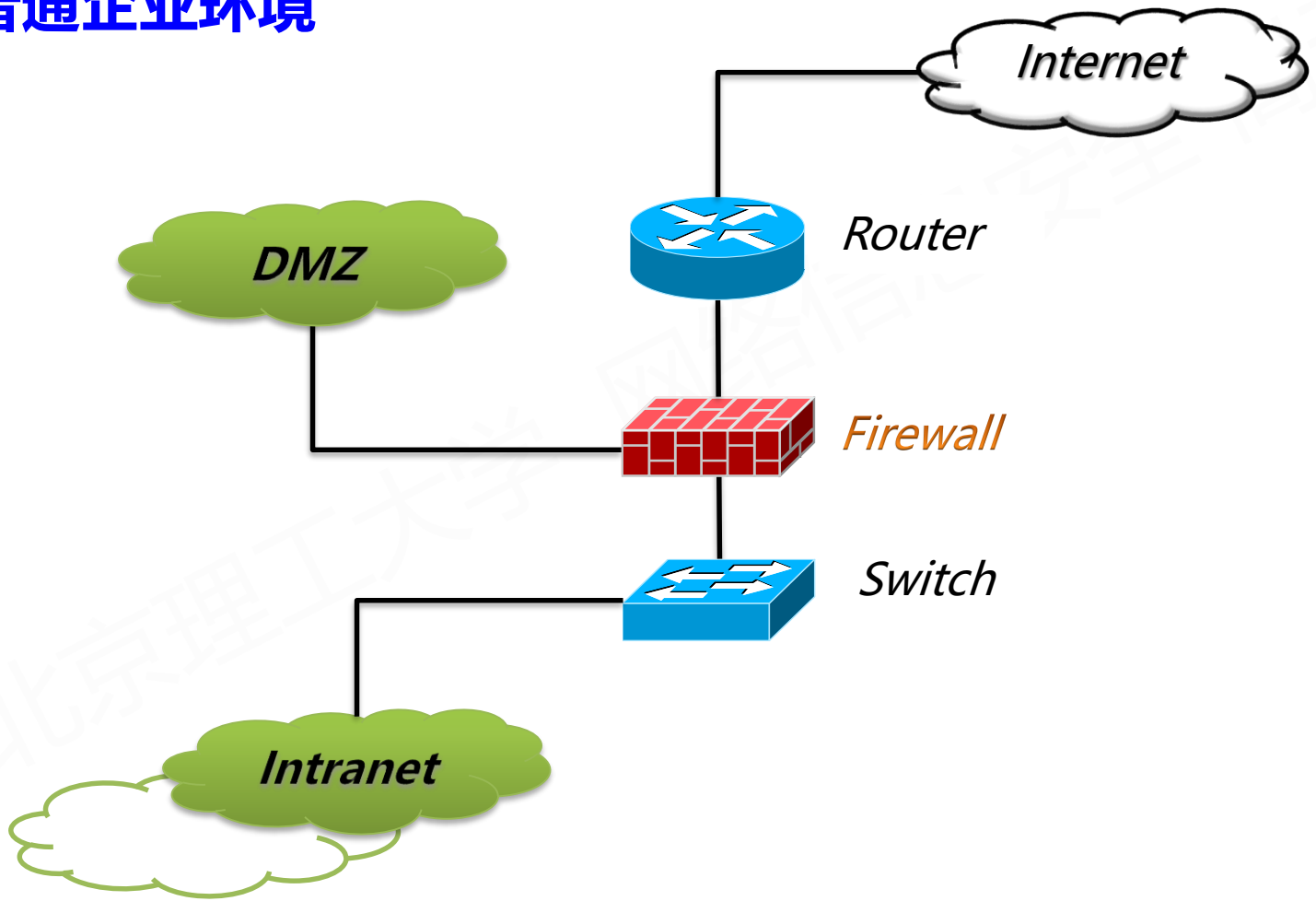
- 访问控制原理
- 防火墙技术概述
- 防火墙核心技术
- 防火墙部署

防火墙部署

- 一些基本概念
  - DMZ，Demilitarized Zone，非军事区，隔离区
    - 传统，两军交接或者前线
    - Mail服务器、Web服务器、数据库服务器等最容易受到攻击
    - 将上述服务器放到专门的子网中
  - 双机热备
    - 增加系统的鲁棒性（可靠性）
  - 部署原则
    - 网络环境、经济能力、安全级别等

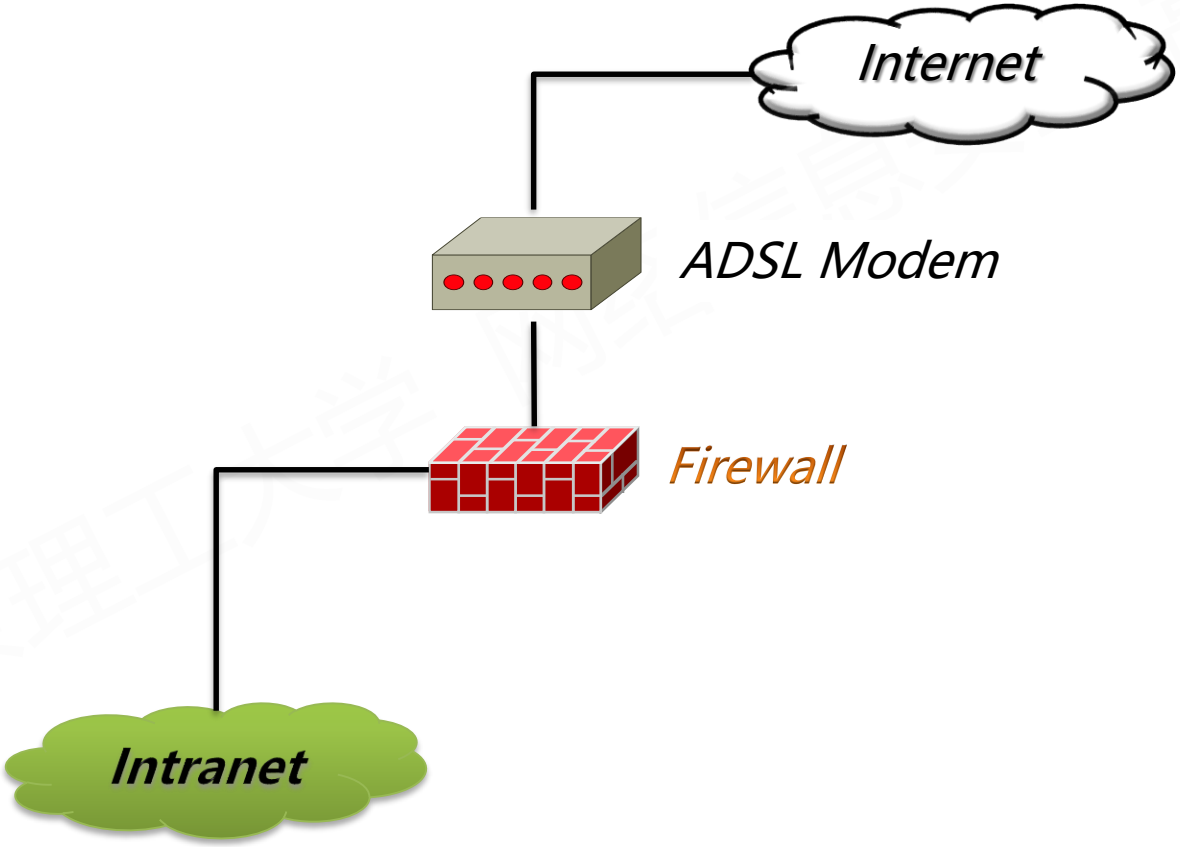
防火墙部署

- **普通企业环境**



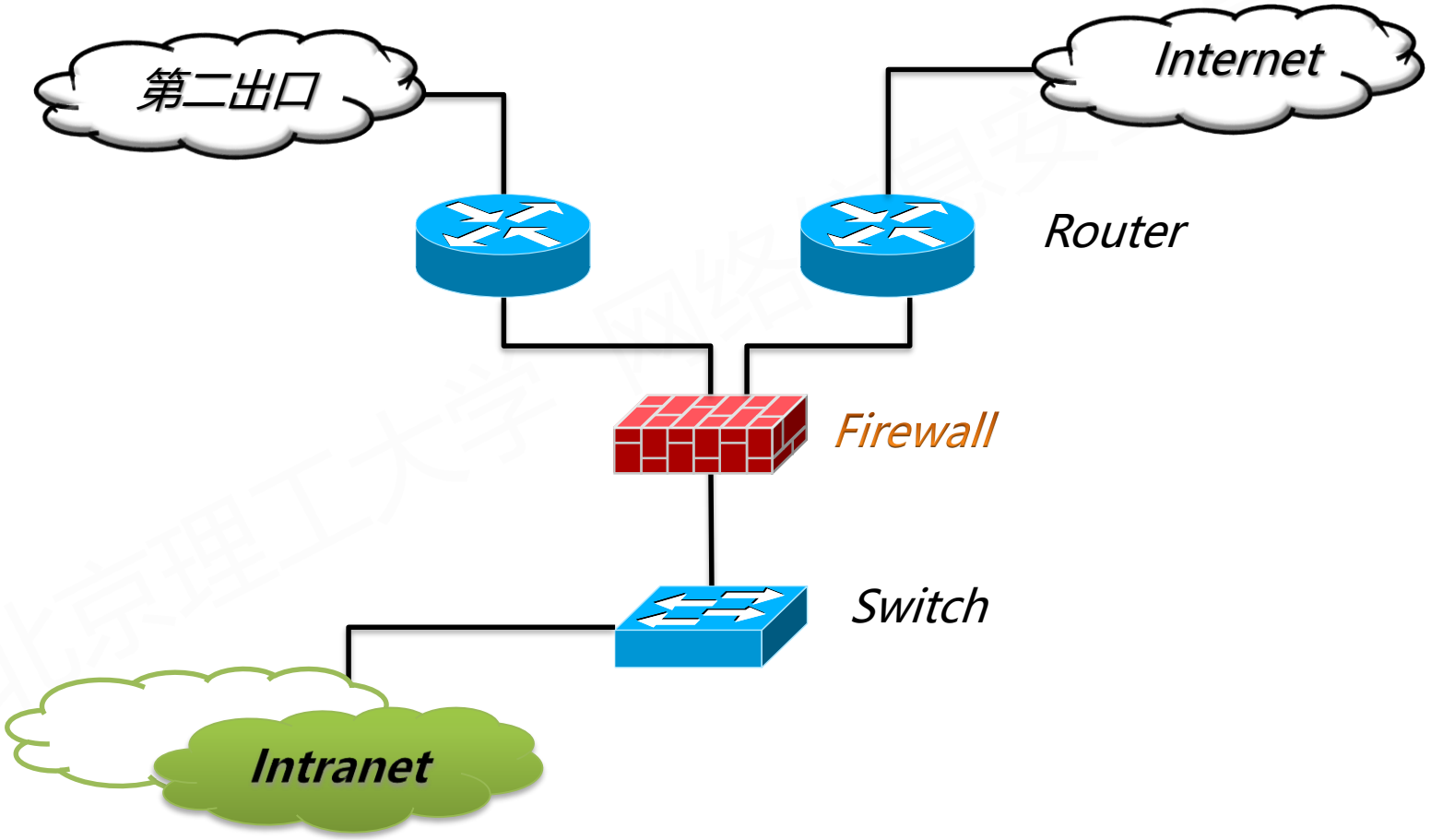
防火墙部署

- **家庭或者中小企业环境**



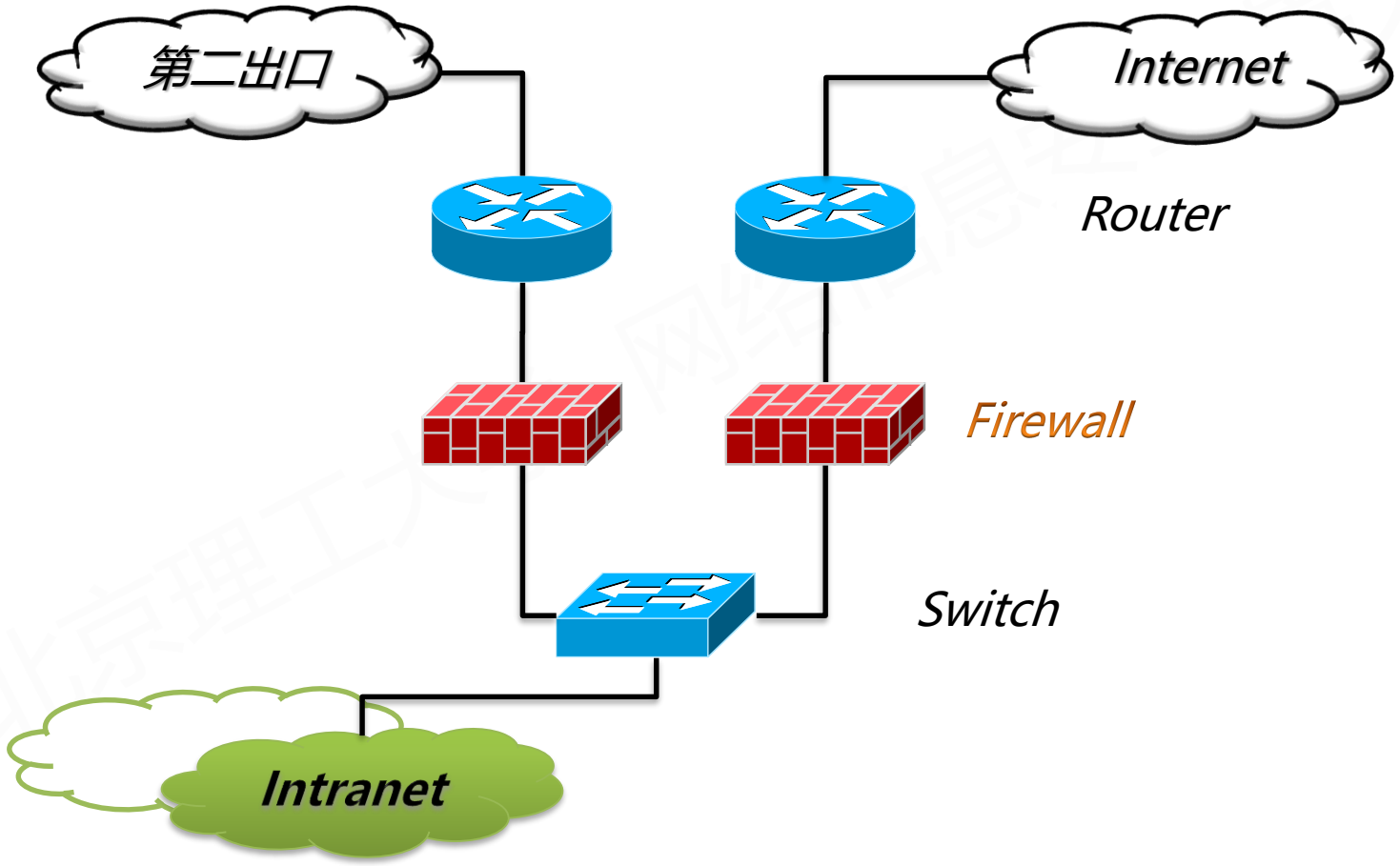
防火墙部署

- **单个防火墙实现多网络接入**



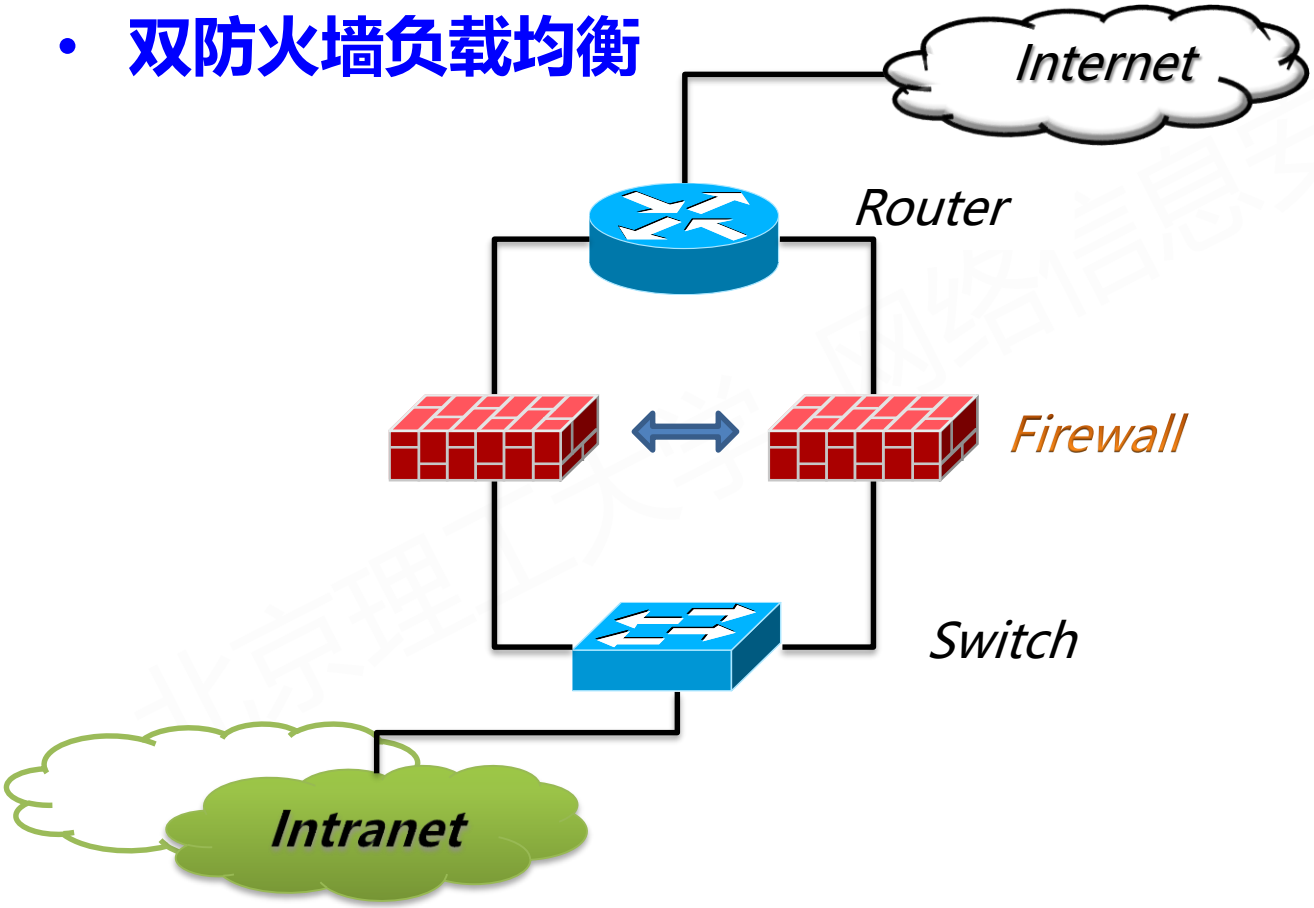
防火墙部署

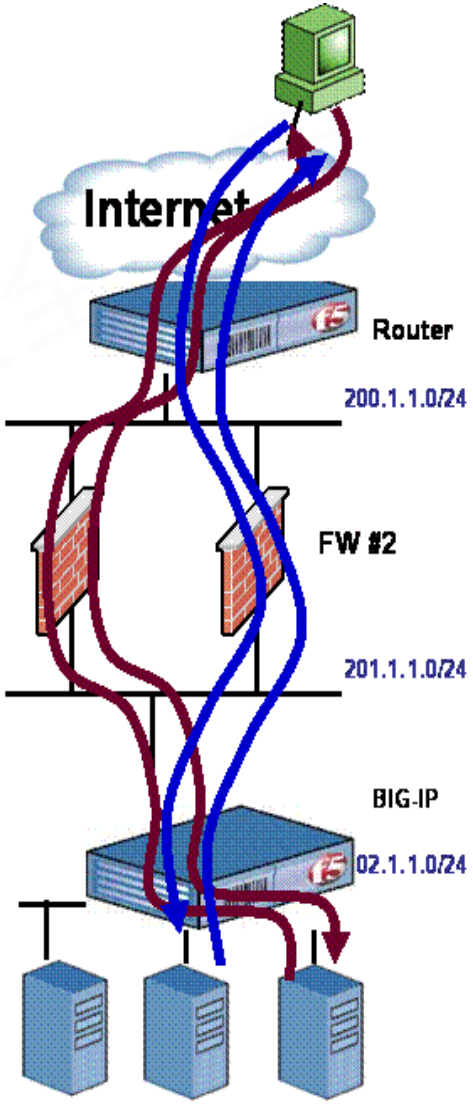
- **两台防火墙实现多网络接入**



防火墙部署

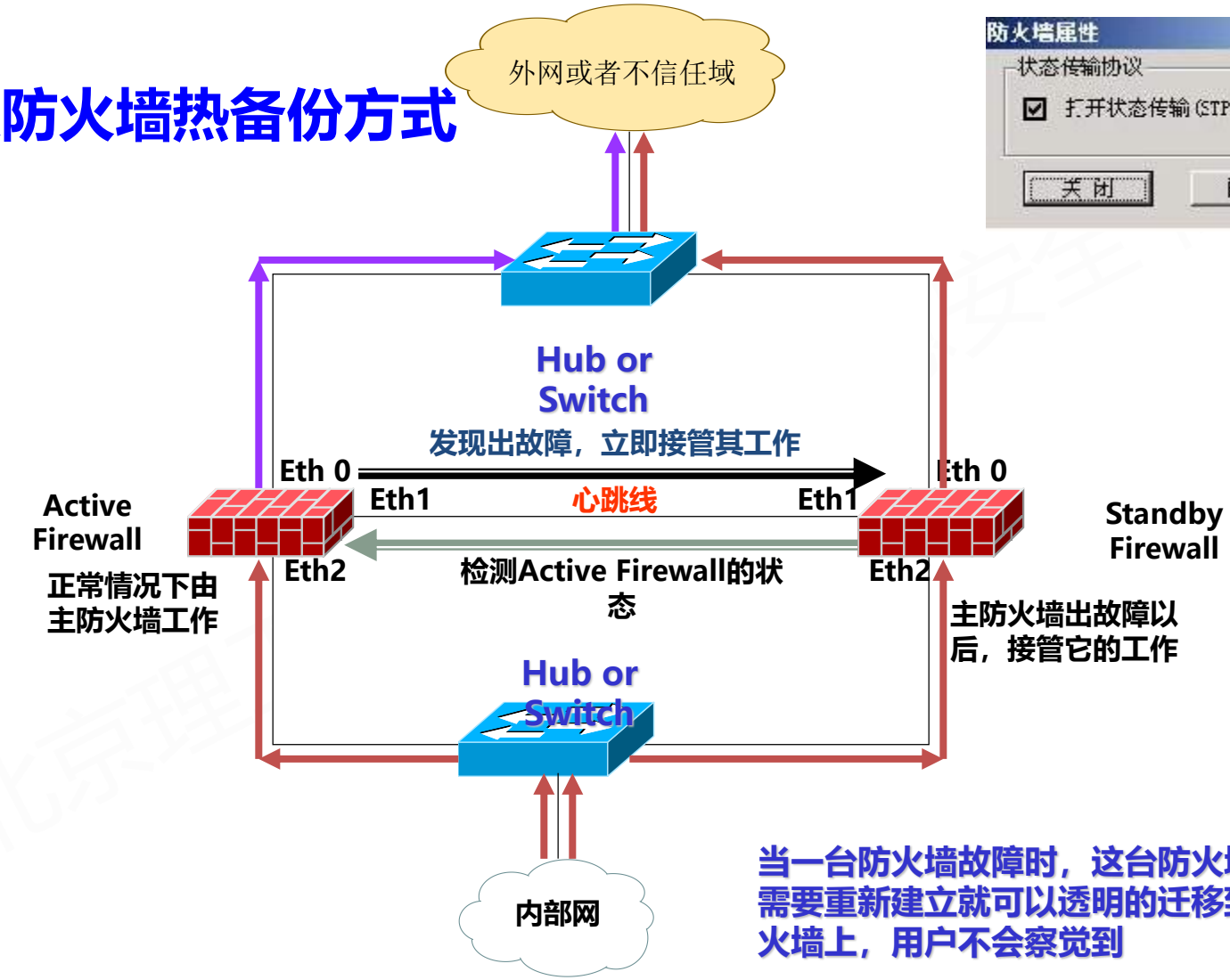
- 双防火墙热备份方式
- 双防火墙负载均衡





防火墙部署

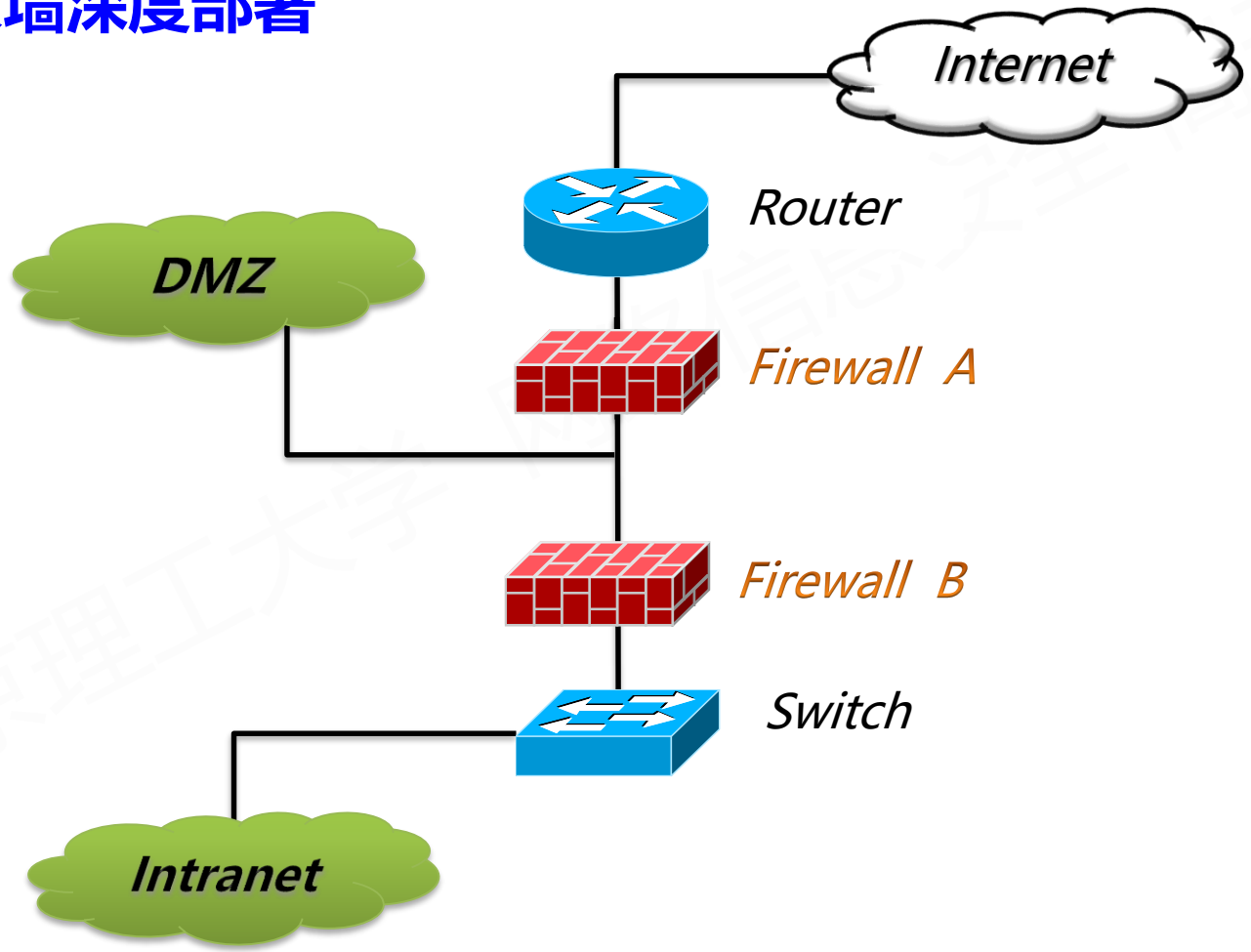
- **双防火墙热备份方式**



当一台防火墙故障时，这台防火墙的连接不需要重新建立就可以透明的迁移到另一台防火墙上，用户不会察觉到

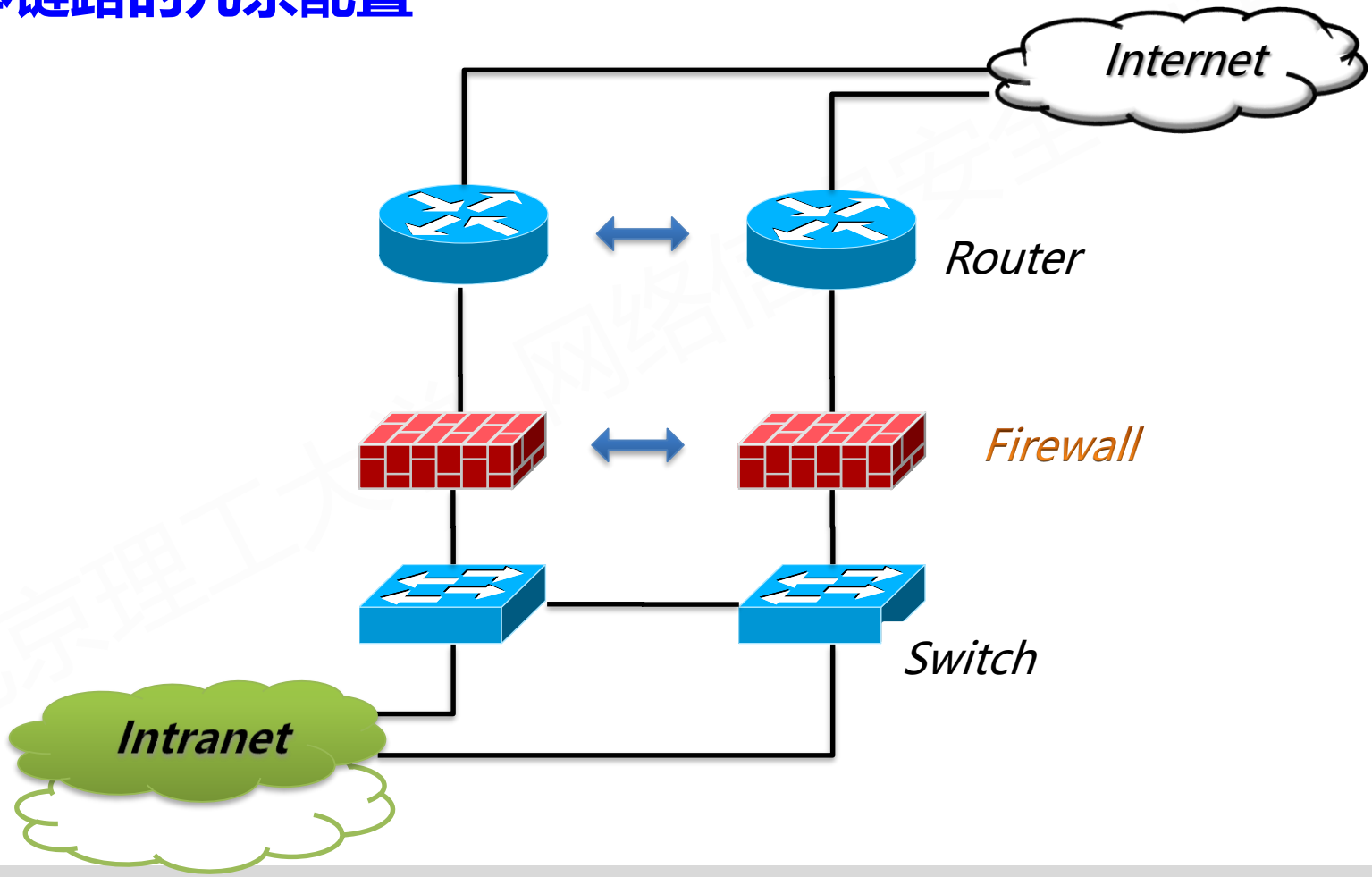
防火墙部署

- **双防火墙深度部署**



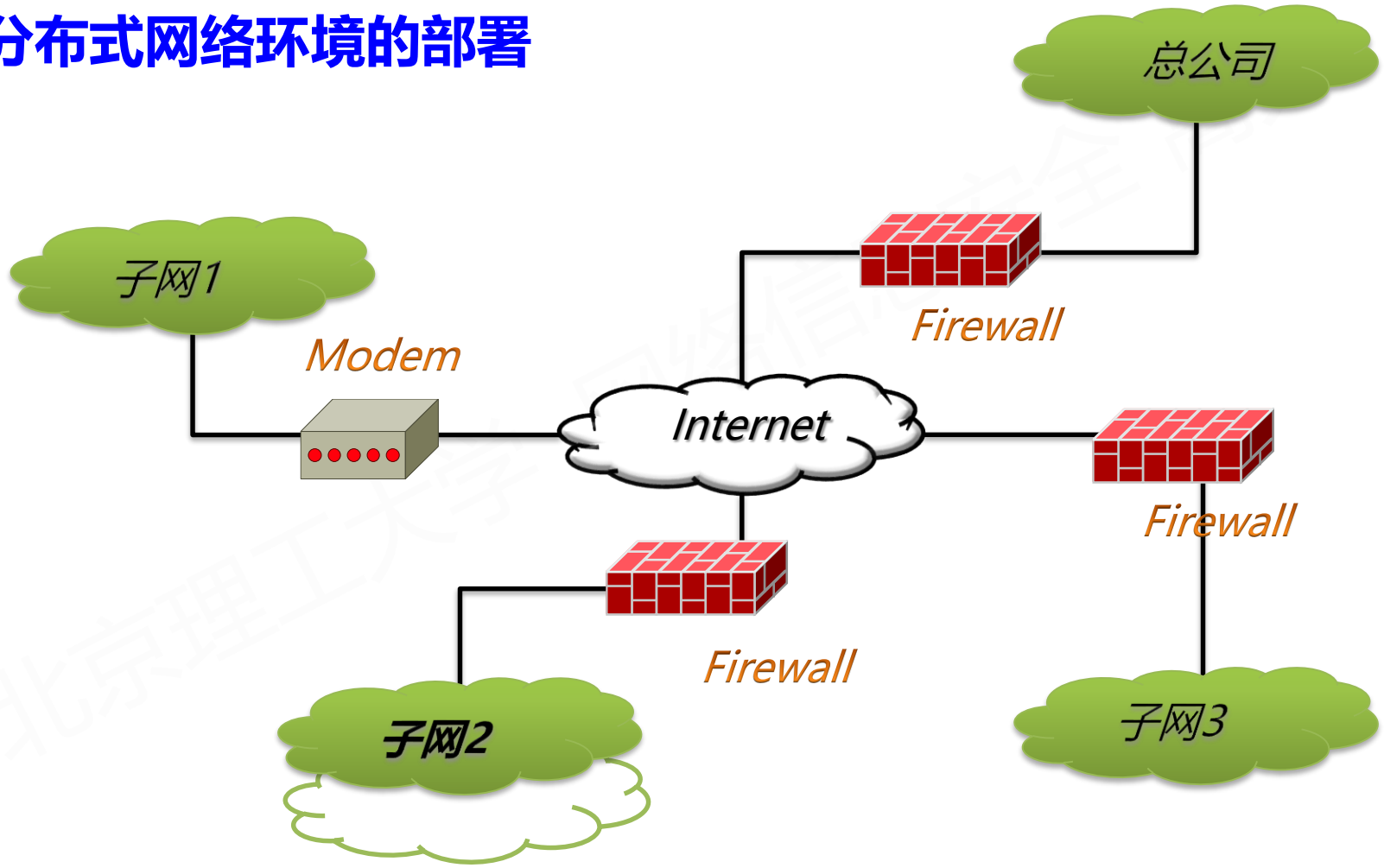
防火墙部署

- **整体链路的冗余配置**



防火墙部署

- **分布式网络环境的部署**

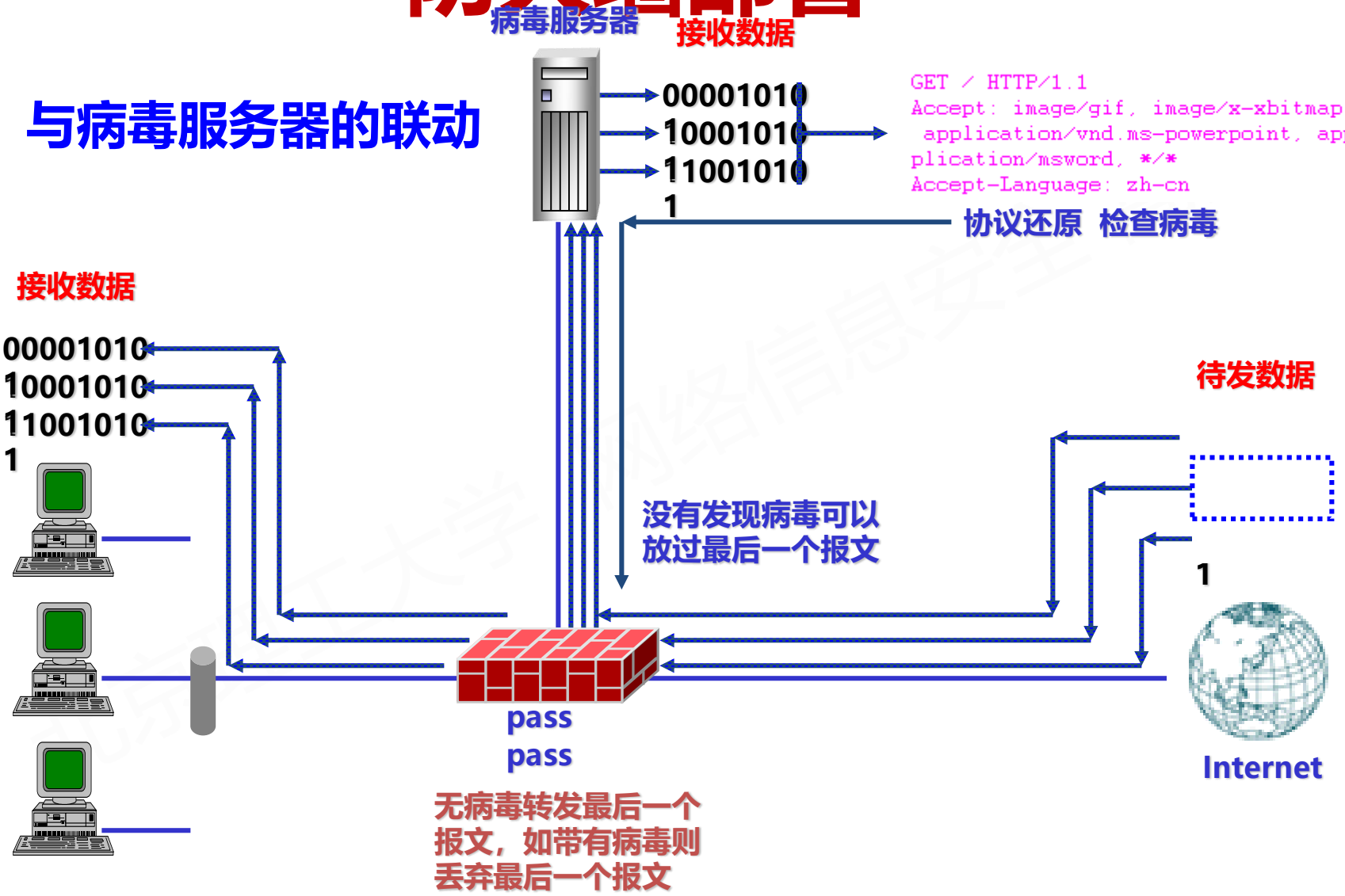


防火墙部署

- **防火墙与其他安全系统的联动**
  - **与病毒服务器的联动**
  - **与IDS的联动**
  - **支持第三方认证服务器**

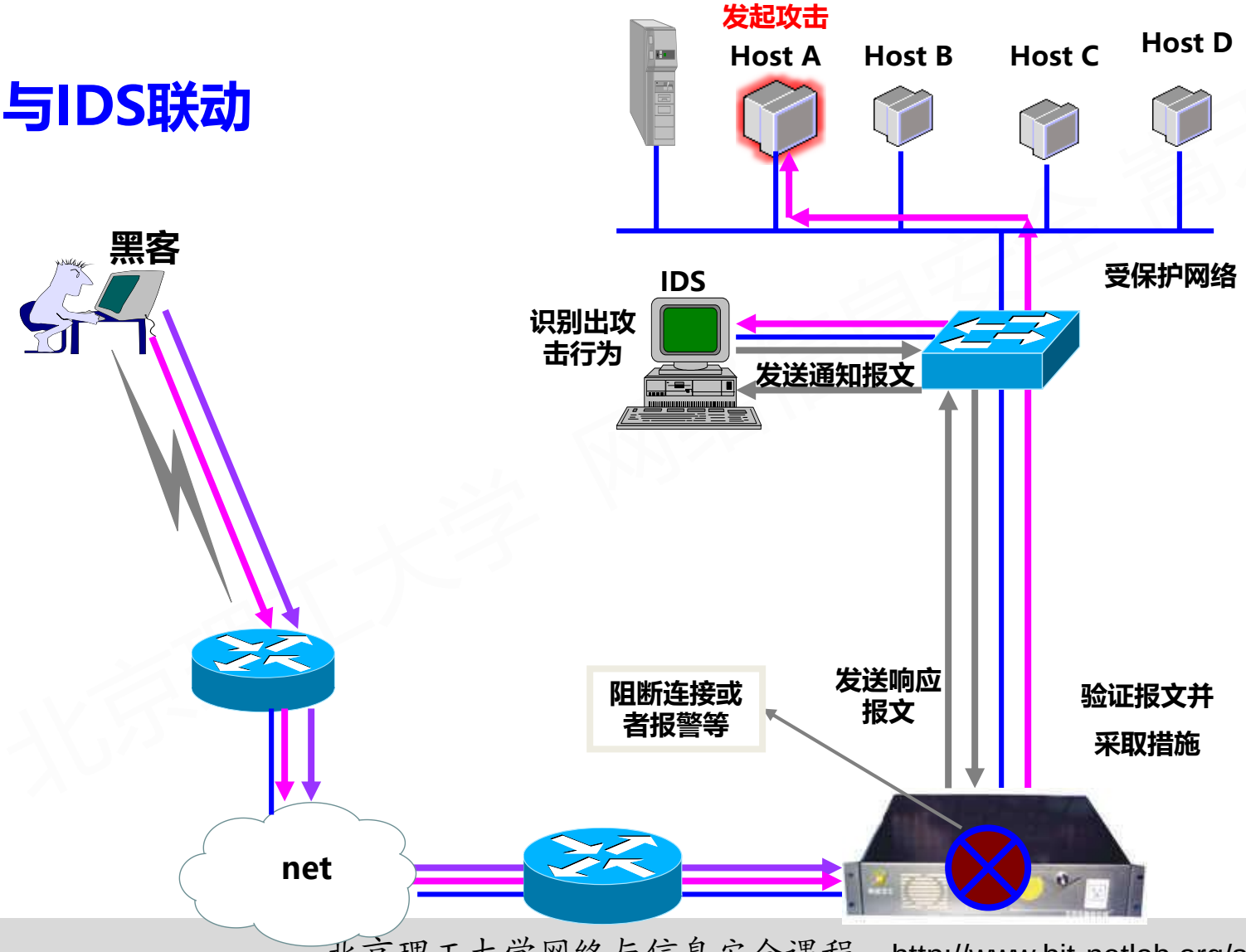
防火墙部署

- 与病毒服务器的联动



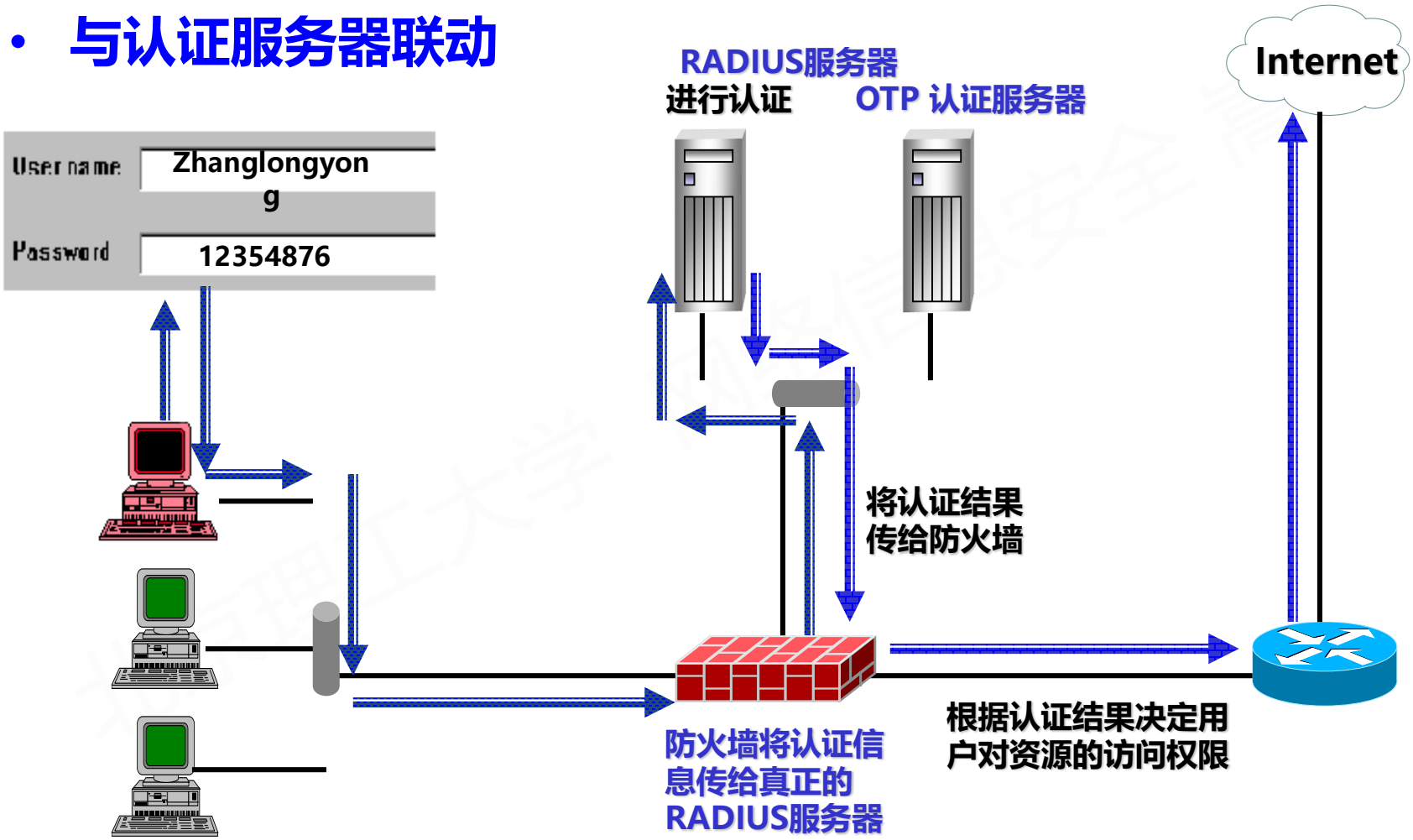
防火墙部署

- 与IDS联动



防火墙部署

- 与认证服务器联动



本节总结

- 经过本节的学习，我们知道
  - 访问控制的三种模式，DAC、MAC、RBAC
  - 防火墙概念
  - 防火墙的核心技术（包过滤等）
  - 防火墙的不同部署方式
  - 防火墙与其它设备的联动