千锋教育
www.mobiletrain.org

做真实的自己·用良心做教育

千锋网络安全学院

防火墙

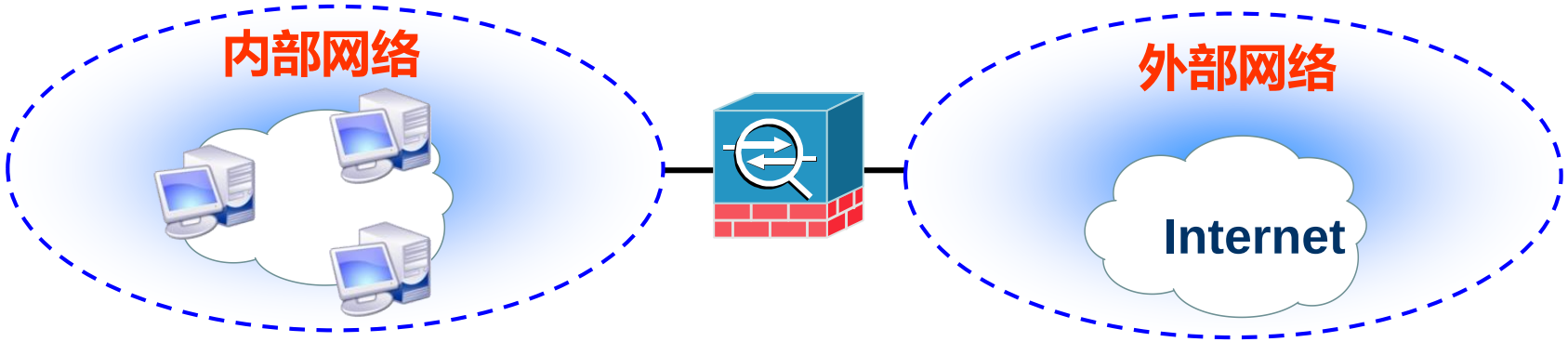
网络安全

目录

防火墙的基本概念

防火墙的定义：是一款具备安全防护功能网络设备：

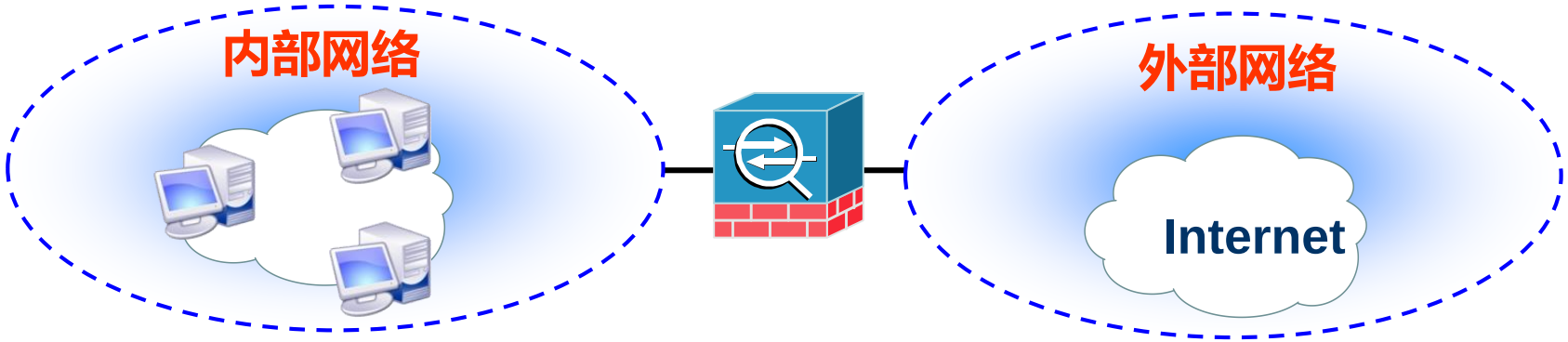
- 隔离网络：
  - 将需要保护的网络与不可信任网络进行隔离，隐藏信息并进行安全防护



防火墙基本功能

防火墙基本功能：

- 访问控制
- 攻击防护
- 冗余设计
- 路由、交换
- 日志记录
- 虚拟专网VPN
- **NAT**



防火墙产品及厂家

防火墙产品：H3C U200系列

- H3C SecPath U200-CS-AC
- 设备类型： 企业级防火墙
- 网络端口： 1个配置口(CON);5GE;1个mini插槽,可通过该插槽扩展网络接口;外置一个CF扩展槽(选配)
- 入侵检测： Dos,DDoS
- 管理： 支持标准网管 SNMPv3，并且兼容SNMP v2c、SNMP v1,支持NTP时间同步,支持Web方式进行远程配置管理,支持SNMP/TR-069网管协议,支持H3C SecCenter安全管理中心进行设备管理
- VPN支持： 支持
- 安全标准： FCC,CE
- 控制端口： console
- 其他性能： 防火墙、VPN可同时扩展卡巴

防火墙产品及厂家

防火墙产品：juniper550M

主要参数

并发连接数	128000	VPN支持	支持
安全过滤带宽(MB)	500	用户数限制	无限制
网络吞吐量(Mpps)	600		

基本参数

VPN支持

并发连接数范围	50万-100万	并发连接数	128000
控制端口	RS-232	最大安全过滤带宽(MB)	501-1000
安全过滤带宽(MB)	500	网络吞吐量(Mpps)	600
用户数限制范围	无用户数限制	用户数限制	无限制
入侵检测	Dos	管理	SNMP

防火墙产品及厂家

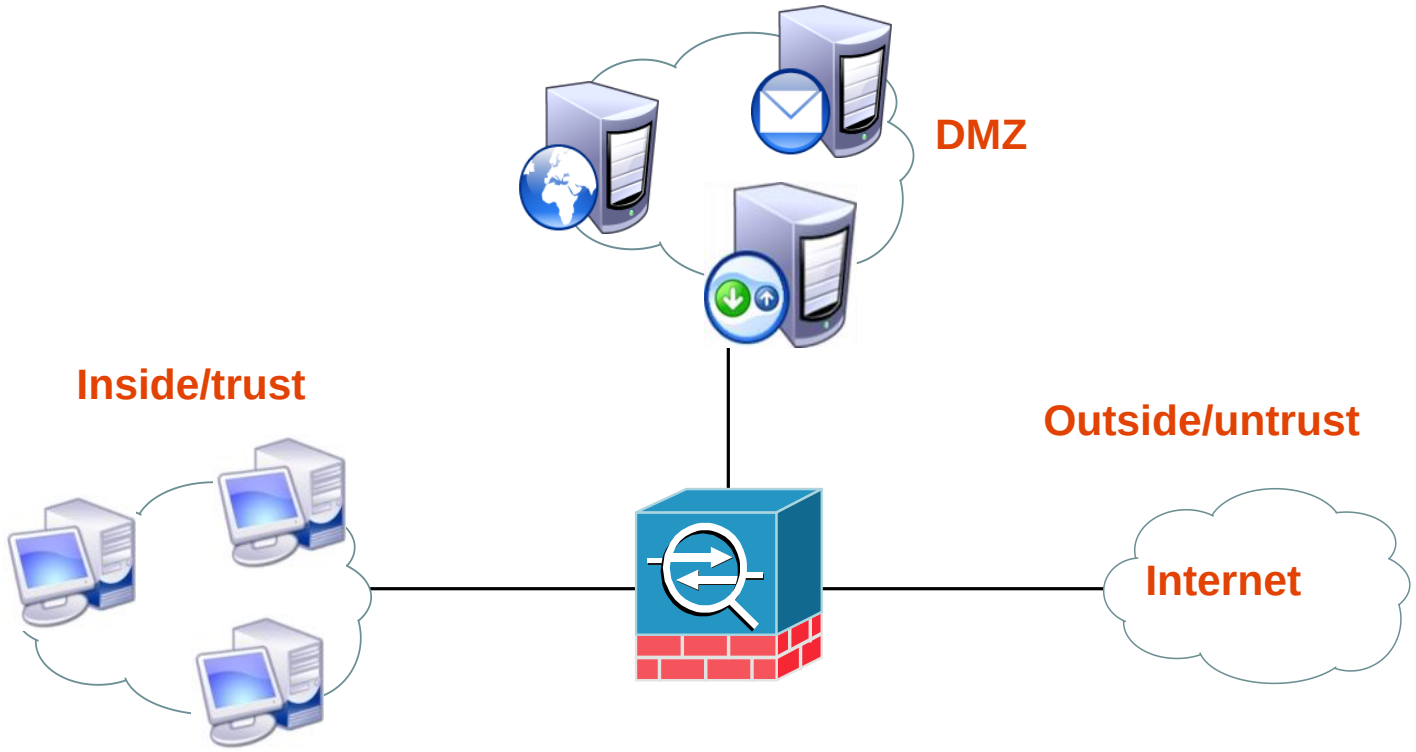
防火墙产品：天融信

基本参数	用手机客户端查配置更方便
防火墙类型	传统防火墙
产品型号	NGFW4000(TG-420A)
产品类型	企业级
硬件参数	
固定接口	10个10/100/1000Base-T端口
网络与软件	
网络管理	包括GUI、WEB界面、命令行界面等。支持远程集中管理功能
并发连接数	＞800000
VPN	支持VPN功能

区域隔离

防火墙区域概念：

- 内部区域
- DMZ区域：称为“隔离区”，也称“非军事化区/停火区”
- 外部区域



防火墙的分类

- 按防火墙形态
  1. 软件防火墙
  2. 硬件防火墙
- 按技术实现
  1. 包过滤防火墙
  2. 状态检测包过滤防火墙
  3. 应用（代理）防火墙
  4. WAF防火墙
  5. 应用层防火墙

	单机防火墙	网络防火墙
产品形态	软件	硬件或者软件
安装点	单台独立的 Host	网络边界处
安全策略	分散在各个安全点	对整个网络有效
保护范围	单台主机	一个网段
管理方式	分散管理	集中管理
功能	功能单一	功能复杂、多样
管理人员	普通计算机用户	专业网管人员
安全措施	单点安全措施	全局安全措施
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	

防火墙的发展历史

- **包过滤防火墙**

  最早的防火墙技术之一，功能简单，配置复杂

- **应用网关/应用代理防火墙**

  最早的防火墙技术之二，连接效率低，速度慢

- **状态检测防火墙**

  现代主流防火墙，速度快，配置方便，功能较多

- DPI**防火墙**（Deep Packet Inspection）

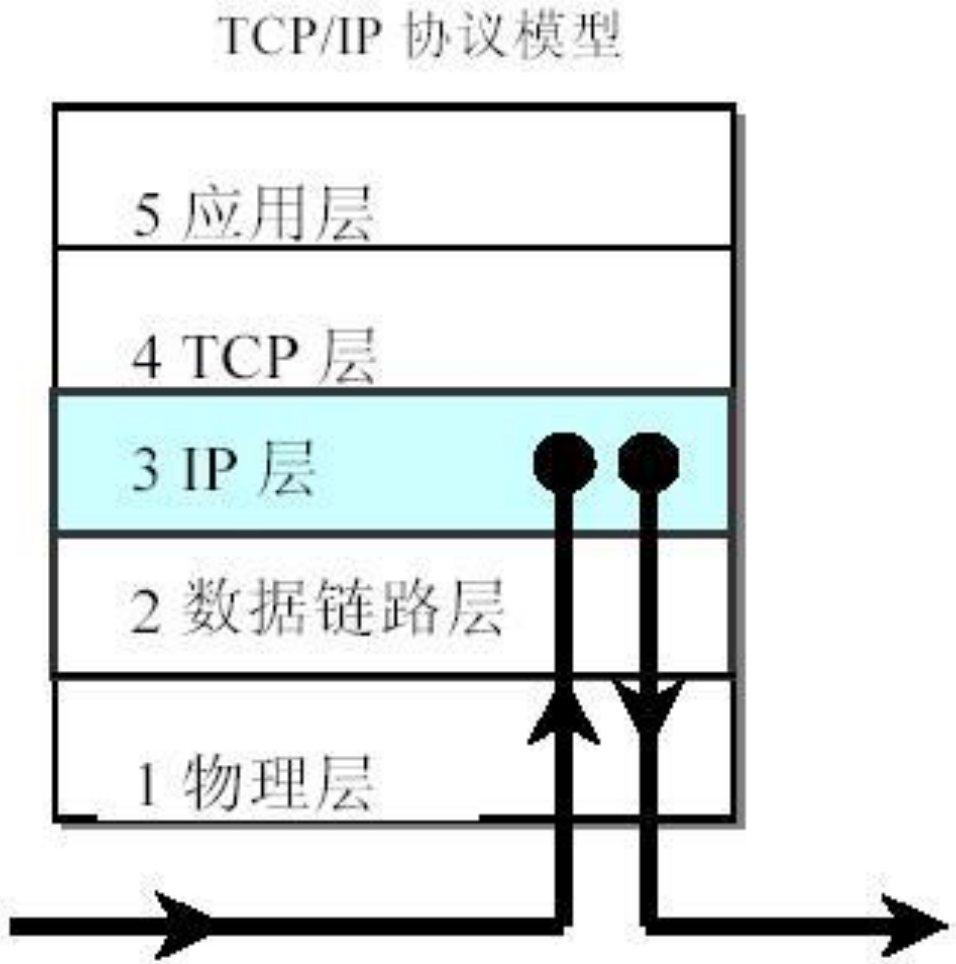
  未来防火墙的发展方向，能够高速的对第七层数据进行检测

包过滤防火墙

- 也叫分组过滤防火墙（Packet Filtering）。
- 根据分组包的源、目的地址，端口号及协议类型、标志位确定是否允许分组包通过。所根据的信息来源于IP、ICMP、TCP或UDP等协议的数据包头（Packet Header）。

- 优点：高效、透明
- 缺点：对管理员要求高、处理信息能力有限

数据包过滤



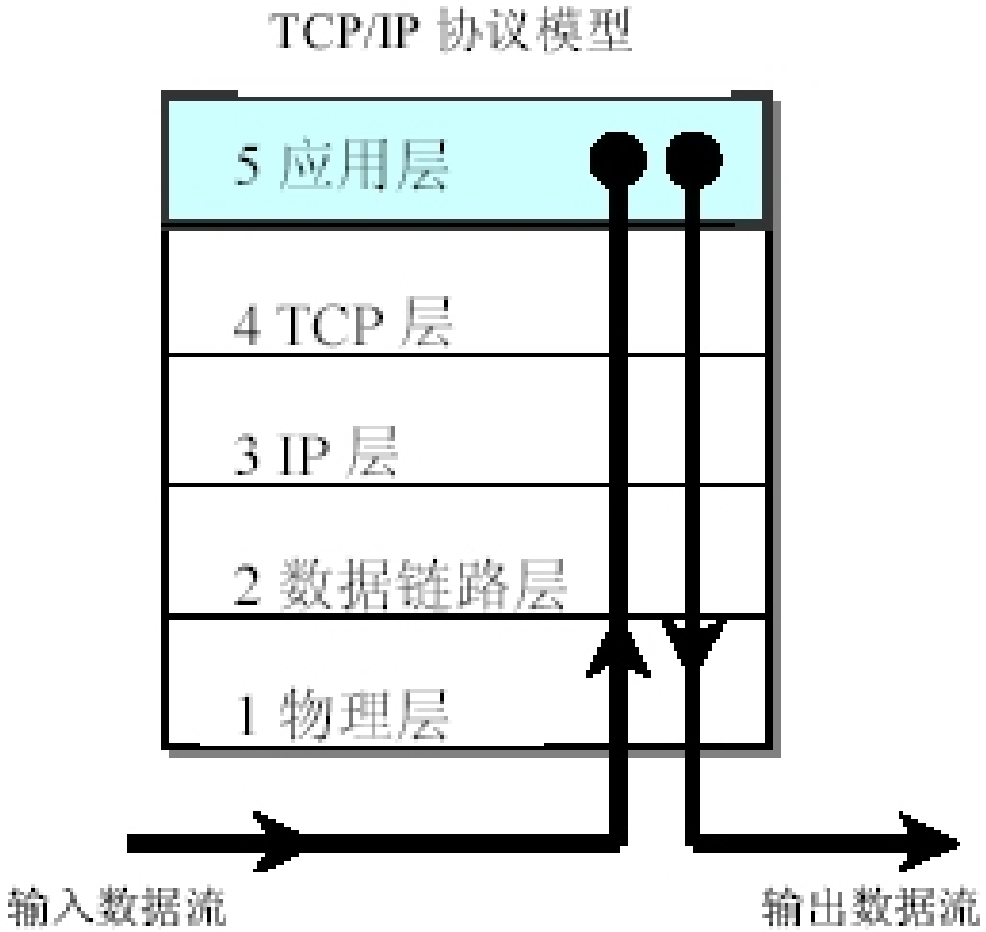
应用网关型防火墙

- 也叫应用代理防火墙

  每个代理需要一个不同的应用进程，或一个后台运行的服务程序，对每个新的应用必须添加针对此应用的服务程序，否则不能使用该服务。

- 优点：安全性高，检测内容
- 缺点：连接性能差、可伸缩性差

应用代理

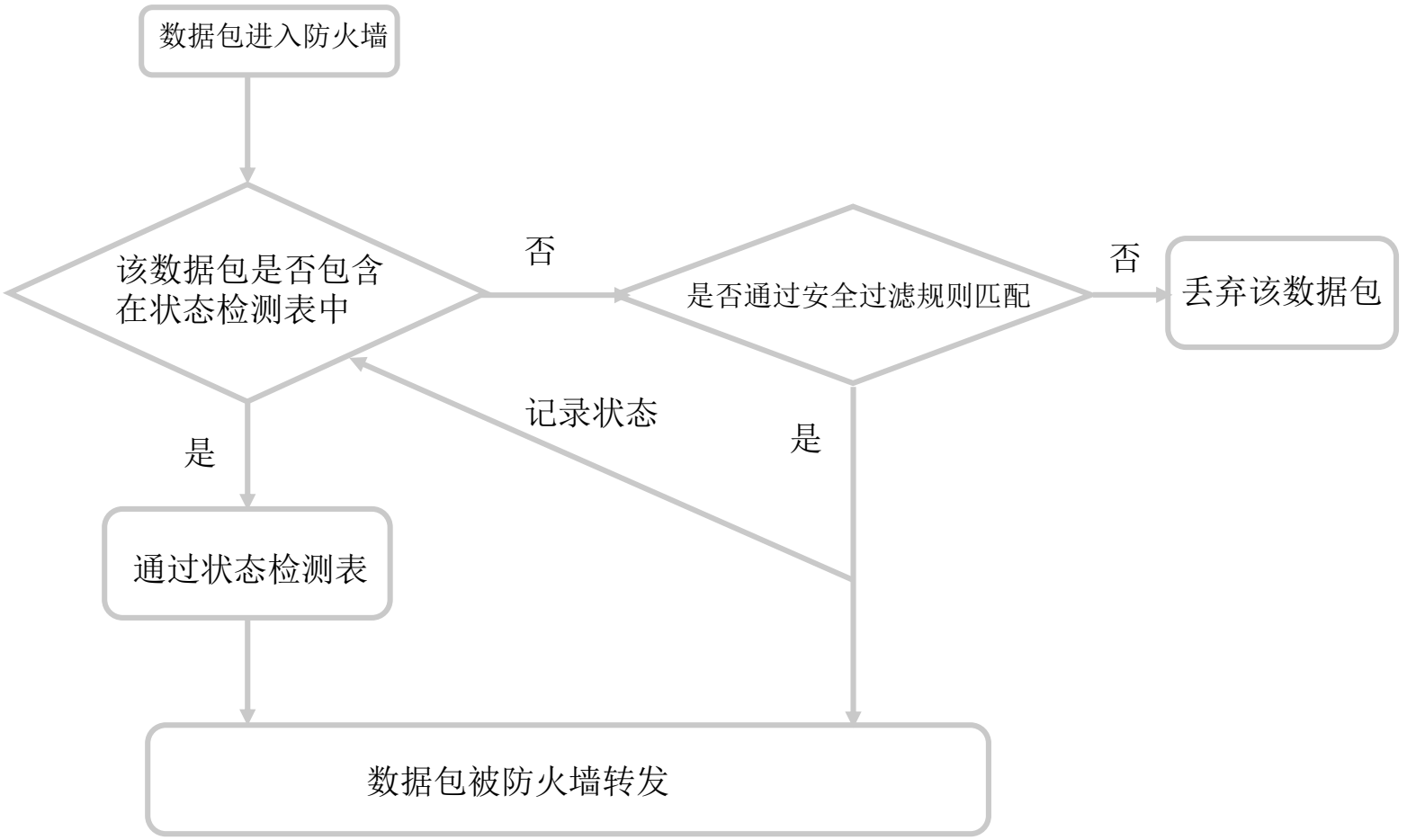


状态检测防火墙

- 从传统包过滤发展而来，除了包过滤检测的特性外，对网络连接设置状态特性加以检测。

- 优点
  - 减少检查工作量，提高效率
  - 连接状态可以简化规则的设置
- 缺点：对应用层检测不够深入

状态检测防火墙处理示意图



衡量防火墙性能的5大指标

1、**吞吐量**：在不丢包的情况下单位时间内通过的数据包数量

2、**时延**：数据包第一个比特进入防火墙到最后一比特从防火墙输出的时间间隔

3、**丢包率**：通过防火墙传送时所丢失数据包数量占所发送数据包的比率

4、**并发连接数**：防火墙能够同时处理的点对点连接的最大数目

5、**新建连接数**：在不丢包的情况下每秒可以建立的最大连接数

防火墙的典型应用

标准应用

1、透明模式

2、路由模式

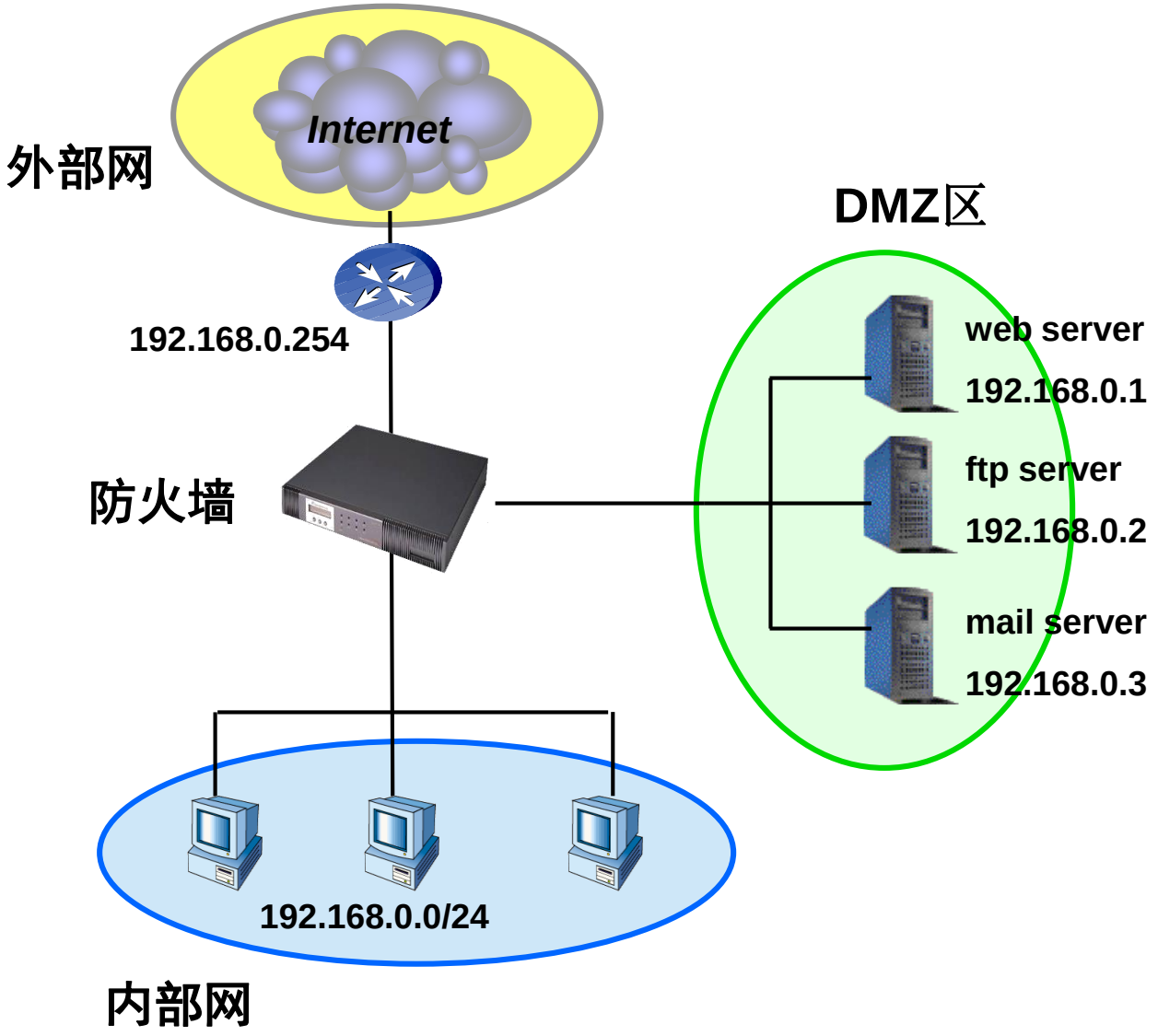
3、混杂模式

标准应用—透明模式

- 透明模式/桥模式一般用于用户网络已经建设完毕，网络功能基本已经实现的情况下，用户需要加装防火墙以实现安全区域隔离的要求。

- 一般将网络分为内部网、DMZ区和外部网

标准应用—透明模式

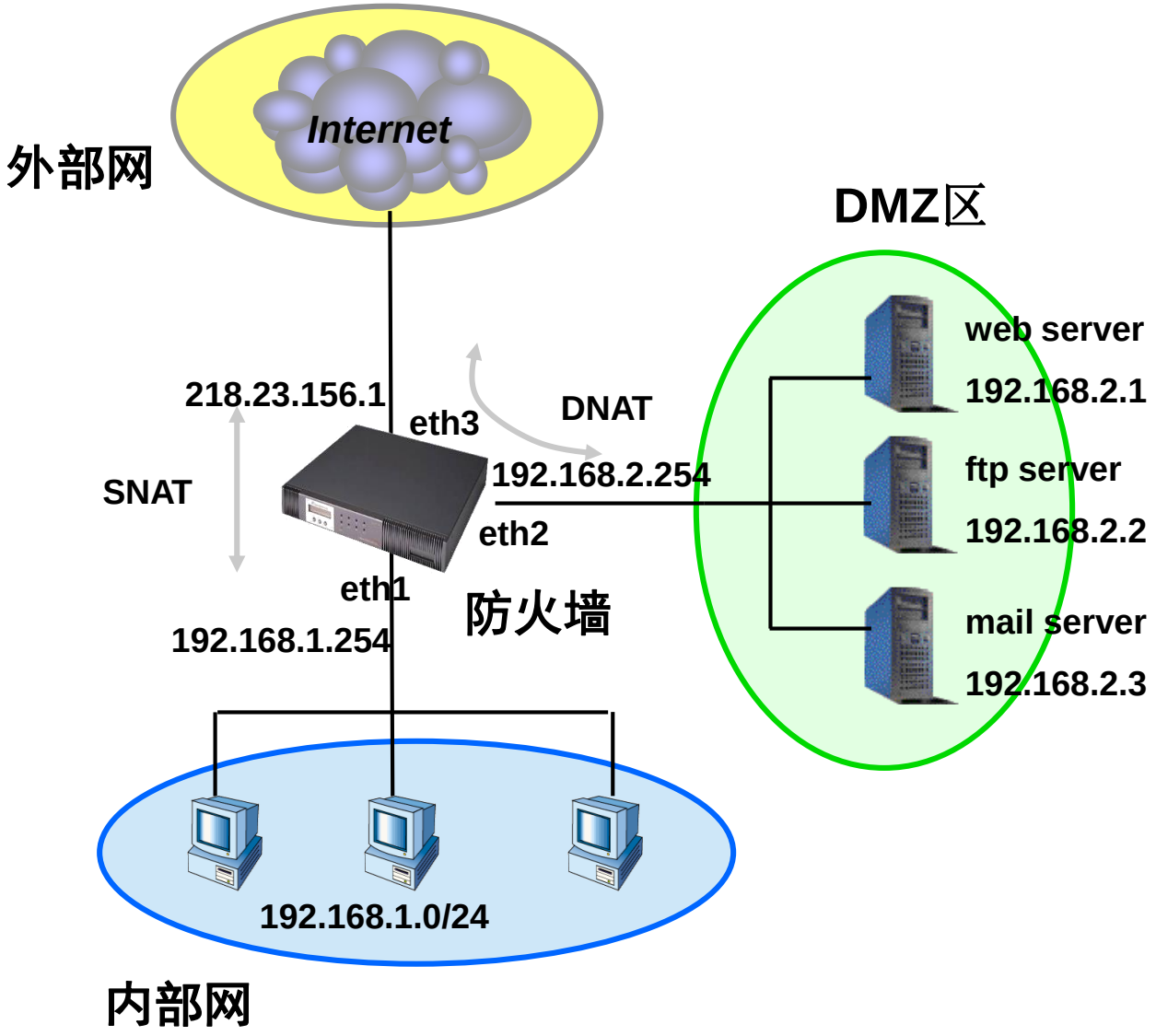

外部网
Internet
192.168.0.254
防火墙
DMZ区
web server
192.168.0.1
ftp server
192.168.0.2
mail server
192.168.0.3
192.168.0.0/24
内部网

标准应用—路由/NAT模式

- 路由/NAT模式一般用于防火墙当作路由器和NAT设备连接上网的同时，提供安全过滤功能。

- 一般将网络分为内部网、DMZ区和外部网

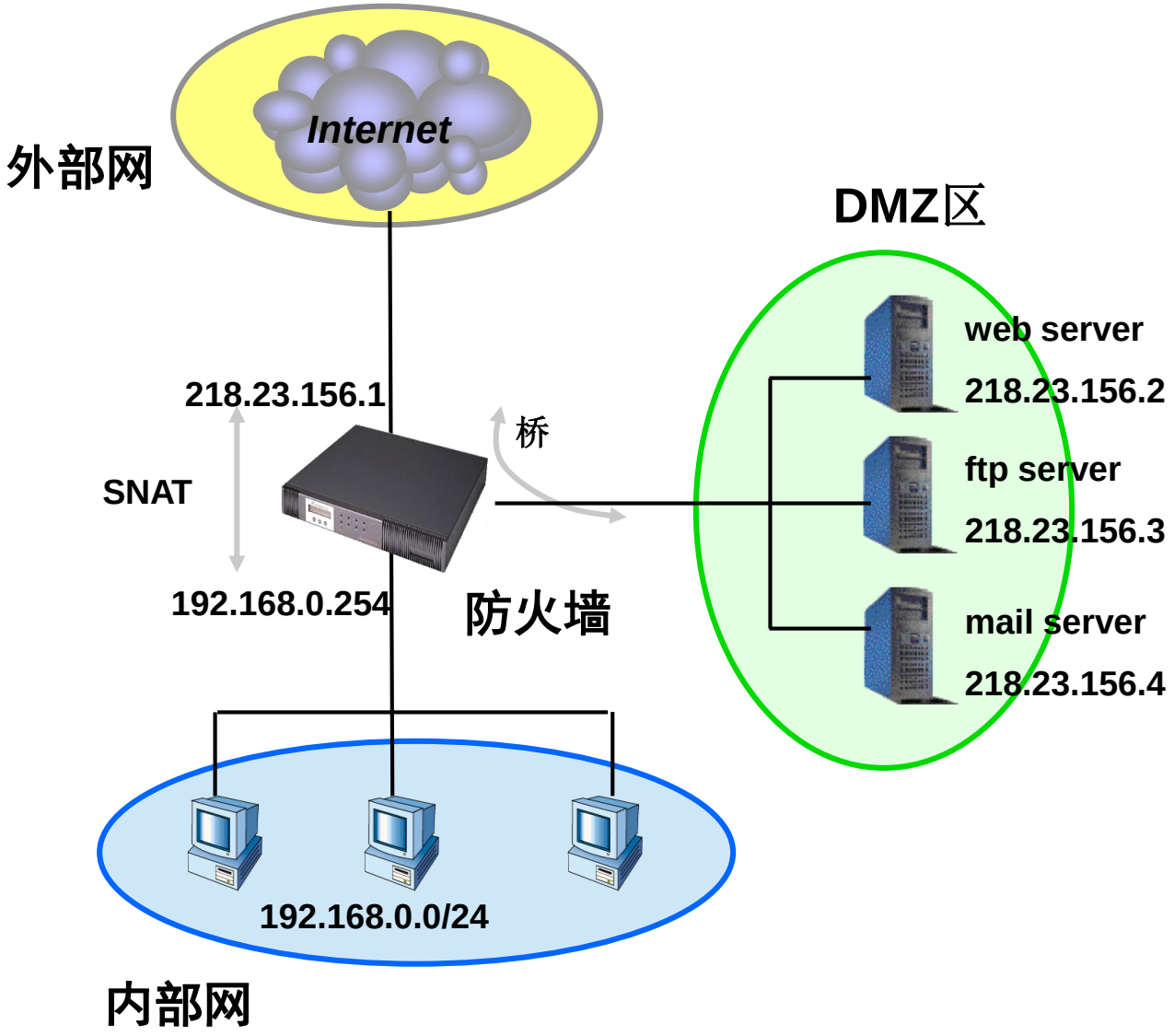
标准应用—路由/NAT模式



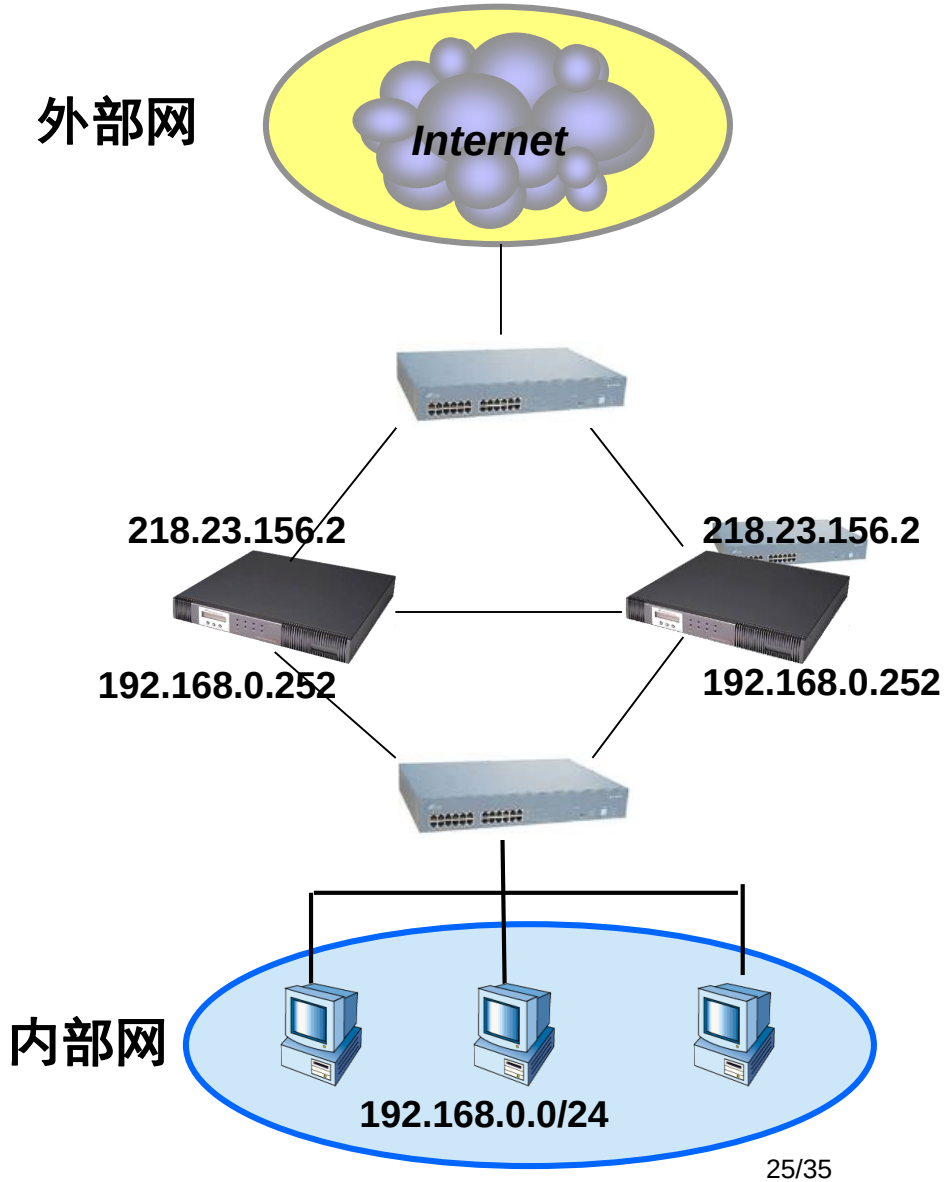
标准应用—混杂模式

- 一般网络情况为透明模式和路由模式的混合。

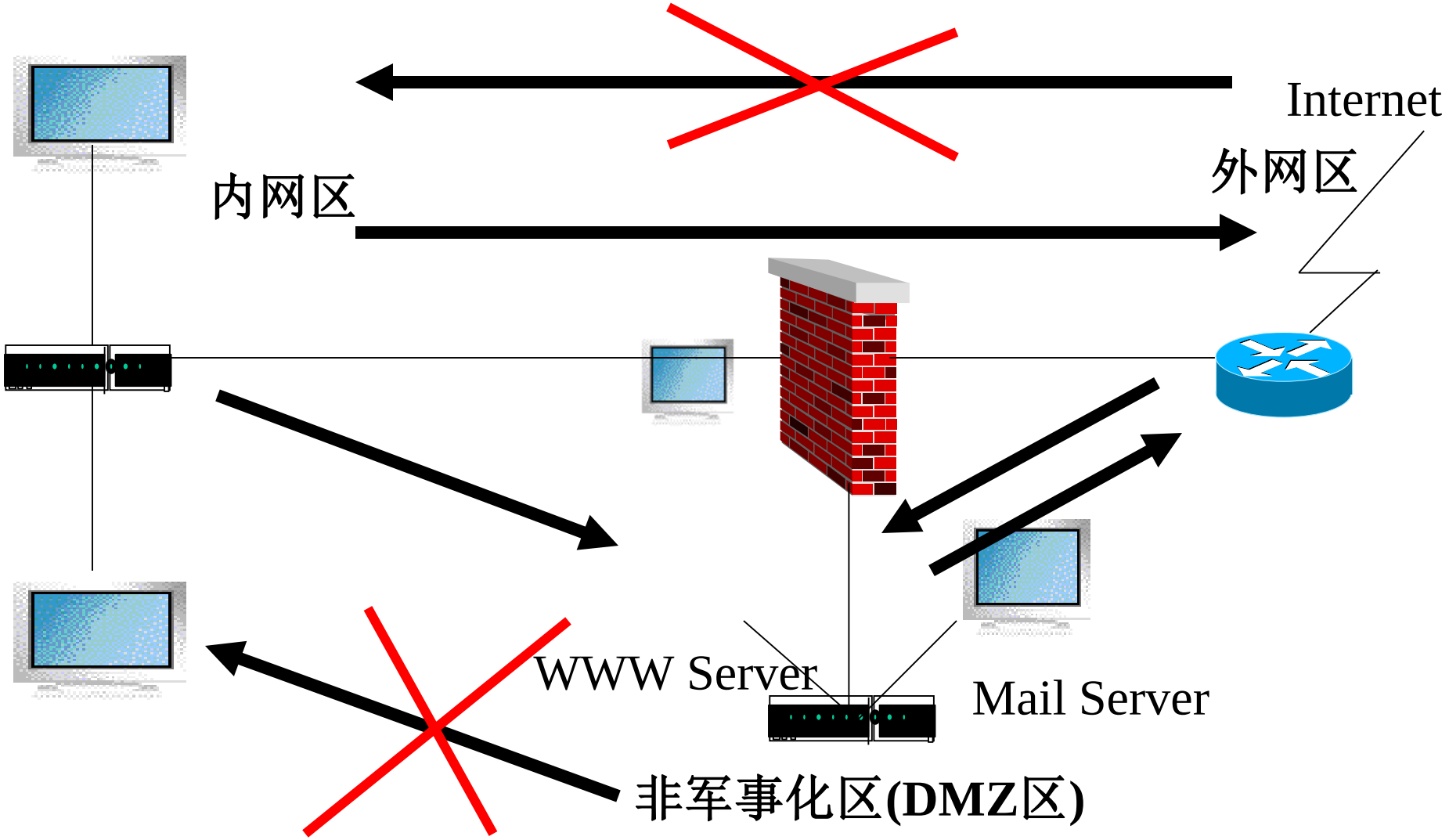
标准应用—— 混杂模式


Internet
外部网
DMZ区
web server
218.23.156.2
ftp server
218.23.156.3
mail server
218.23.156.4
218.23.156.1
桥
SNAT
192.168.0.254
防火墙
192.168.0.0/24
内部网

高级应用—双机热备


外部网
Internet
218.23.156.2
218.23.156.2
192.168.0.252
192.168.0.252
内部网
192.168.0.0/24

防火墙策略分析-最安全的防火墙架构



THANK YOU

做真实的自己，用良心做教育