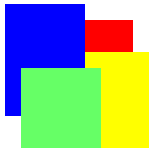


第4章 访问控制技术及应用

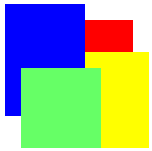
网络防火墙

董建阔

南京邮电大学

关键知识点*

- 网络防火墙本质上是一个网络访问控制系统。根据网络访问的两个特定功能层次，可以将网络防火墙分成网络层防火墙和应用层防火墙。
- 网络层防火墙通过对网络层分组的访问控制，实现对某个网络的访问控制。
- 应用层防火墙通过对应用层报文的访问控制，实现对某个网络应用的访问控制。



主要内容

- 网络防火墙基本概念
- 网络层防火墙
- 应用层防火墙
- 下一代防火墙

网络防火墙基本概念

- 网络防火墙定义
- 网络防火墙特征
- 网络防火墙部署结构
- 网络防火墙分类
- 网络防火墙自身安全性

网络防火墙定义

- 从理论上定义，防火墙是限制数据在网络之间自由传递的控制系统，它是网络系统中一种安全访问控制系统。
  - 网络层就是限定分组的传递，不涉及用户
  - 应用层就是限定报文的传递，可能涉及用户
- 在实际应用中，防火墙是限制数据在企业内部网络、企业外部网络以及公共互联网之间自由传递的安全控制系统。

网络防火墙特征

遵循托管监控器原理，防火墙具有以下特征：

（1）所有从外部网到内部网，或者从内部网到外部网的分组流或报文流必须经过防火墙；

- 完备性，不可翻墙！

（2）根据本地安全策略定义，只有被授权的分组流或报文流才能通过防火墙；

- 孤立性，本地处理

（3）防火墙具有抵御网络攻击的能力。

- 需要验证的能力，特别是机器验证能力！

托管监控器对防火墙的要求

- 为了保证托管监控器能够按照访问控制数据库的规则，实现访问控制策略，基于托管监控器的防火墙必须满足3点要求：
  - 完备性(任何访问操作无法绕过) → 必须经过防火墙
  - 孤立性(独立安全机制、不受其他系统干扰) → 本地安全策略
  - 可验证性(控制机制及其实现必须通过安全验证) → 抵御攻击

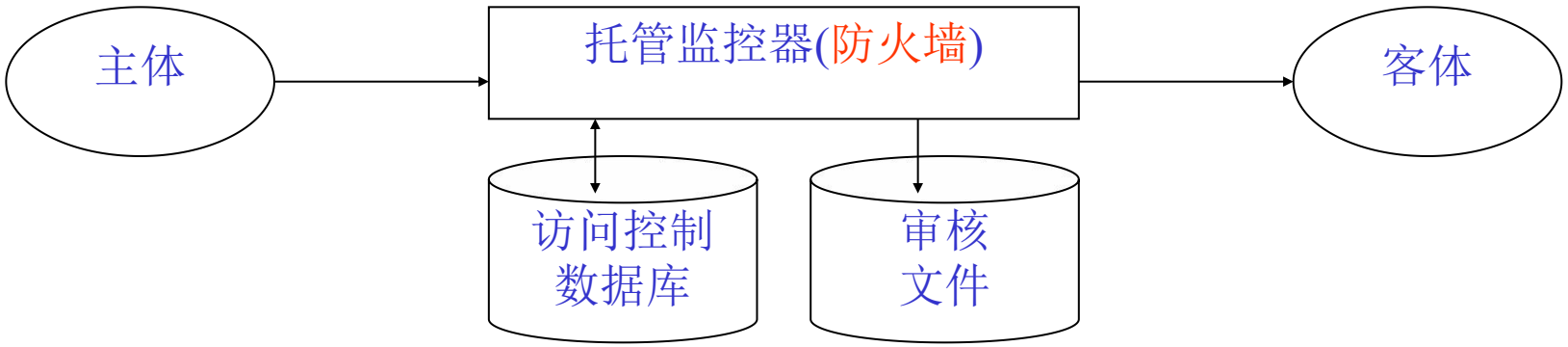
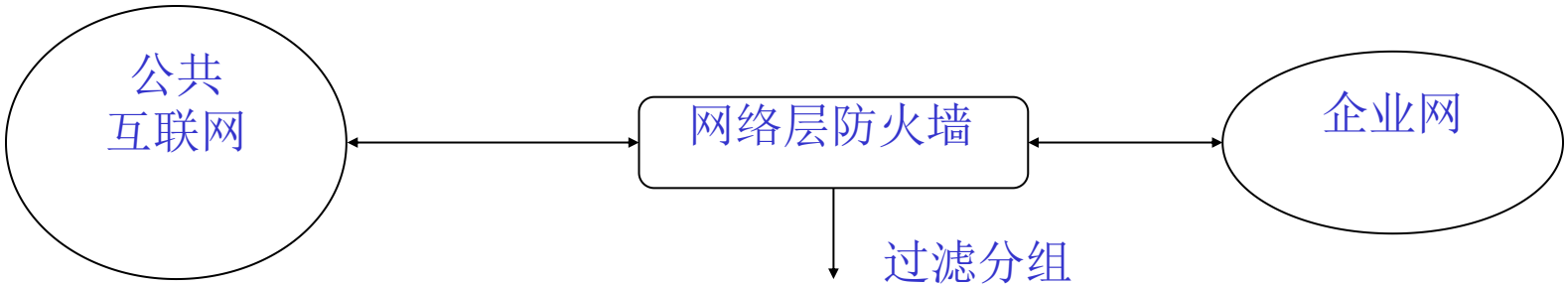


图4.1 托管监控器访问控制架构

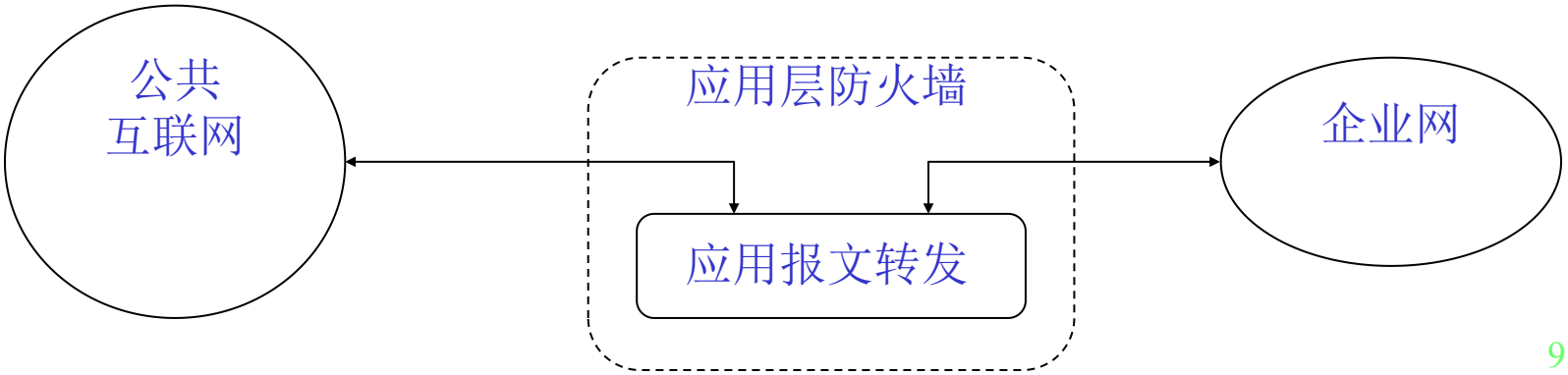
网络层防火墙

- 防火墙一般可以分成2种类型：网络层防火墙和应用层防火墙。
- 网络层防火墙也称为“分组过滤器”，它是通过网络路由交换设备对分组头的识别，过滤不符合安全策略的分组，实现对进入或者离开企业网的分组进行访问控制——路由交换设备的基本功能。



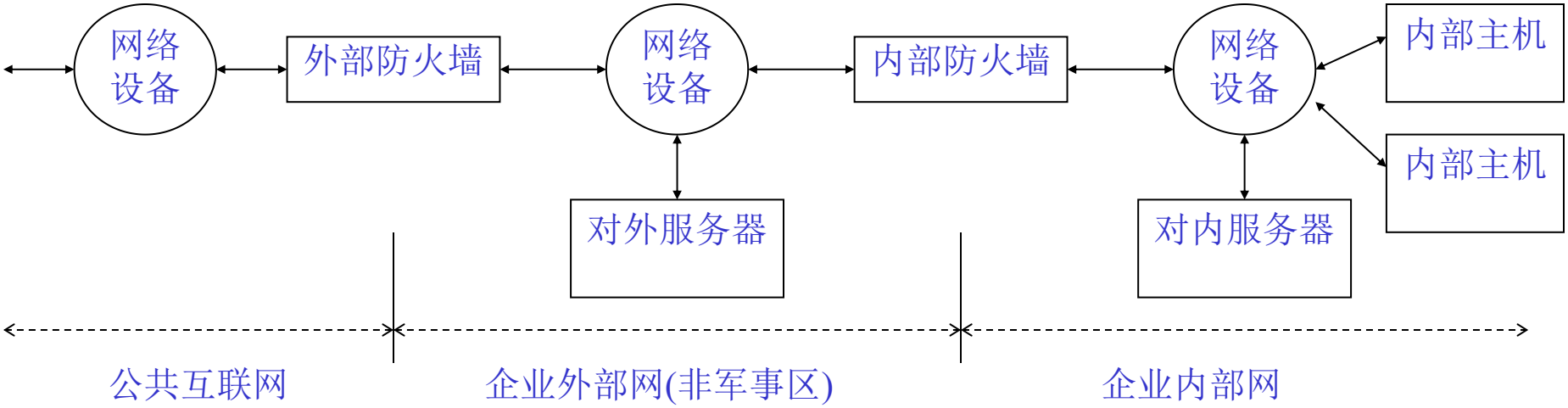
应用层防火墙

- 应用层防火墙也称为“报文转发器”或“应用网关”，它强制性在公共互联网与企业网之间中断应用连接，根据安全策略(访问控制表)检查应用连接，如果这些应用连接符合安全策略的要求，然后再转发应用连接。——代理服务器
  - 不是过滤报文，而是转换报文 → 网关的基本特征
  - 应用层防火墙会影响网络性能，需要权衡安全和性能



网络防火墙部署结构

- 在互联网环境下防火墙一般设置在公共互联网与企业网之间，而企业网中还可以进一步采用防火墙设置成企业外部网和企业内部网。

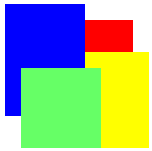


各类网络防火墙的功能定义

- 外部防火墙的功能：隔离公共互联网与外部网
  - 外部网：企业放置对外服务器（例如对外网站和邮件服务器）的网络区域。
- 外部防火墙通常是网络层防火墙
- 内部防火墙的功能：隔离外部网与内部网
  - 内部网：企业放置内部服务器和内部网络客户机的网络区域。
- 内部防火墙＝网络层防火墙＋应用层防火墙

网络防火墙自身安全性

- 防火墙的一个重要特征是自身具有很强的抵御网络攻击的能力。
- 从安全角度看，作为防火墙的路由交换设备或者网关都应该运行简单的、易于控制的、尽量少的程序，关闭不需要的服务。例如应该关闭路由交换设备或者网关上的远地登录服务。
- 应用层防火墙也称为“堡垒主机”。
  - 用户角度看的的应用层防火墙就是一台“主机”
  - 为了使得“堡垒主机”真正成为外部网络攻击无法攻破的“堡垒”，它所运行的操作系统、应用软件都是经过严格筛选和简化的系统和软件。



网络层防火墙

- 网络层防火墙原理
- 网络层防火墙功能
- 网络层防火墙配置
- 网络层防火墙优点
- 网络层防火墙缺点

网络层防火墙原理*

- 网络层防火墙通常称为“分组过滤器”，它能够在网络层转发分组过程中，根据安全策略对分组进行过滤。
- 这种防火墙主要在路由交换设备中实现。现在互联网上的路由交换设备通常提供一种基于访问控制列表(ACL)的访问控制功能，这种功能就是“分组过滤器”功能。
- 网络层防火墙既可以保护网络，也可以保护网络上的应用。

网络层防火墙功能*

- 通过禁止(允许)某类源IP地址或者某类目的IP地址，分组过滤器可以限制(允许)来自公共互联网的某些子网访问企业网，或者限制(允许)企业网内某些子网访问公共互联网；
- 通过禁止(允许)某类源端口号或者某类目的端口号，分组过滤器可以限制(允许)来自公共互联网的某类服务请求，或者限制(允许)企业网对公共互联网某些服务请求，限制网络应用。
- 需要注意：这里假定网络层防火墙采用ACL规则的从头顺序匹配、先匹配先执行的原则。

网络层防火墙配置*

- S. Bellovin和W. Cheswick建议采用以下三个步骤配置分组过滤器：
- 第一步需要了解被保护网络的安全策略，即需要知道什么应该被“允许”，什么应该被“禁止”，以及缺省情况。
- 第二步需要根据网络安全策略，寻找对应的可控制的分组(IP报文)控制字段，并且需要明确罗列具体的安全控制规则。
- 第三步按照分组过滤器中ACL要求的格式，配置具体罗列的安全控制规则。

网络层防火墙配置(续1)

举例：假定设置一个分组过滤器，作为公共互联网与企业外部网之间的网络层防火墙。其安全策略是：

(1) 只允许公共互联网访问企业外部网中的邮件服务器(210.10.10.36)；

(2) 不允许spam.com域名的子网(110.10.160.0)中的站点访问该邮件服务(端口号为25)。

要求设置相应的访问控制列表。

网络层防火墙配置(续2)

则该分组过滤器的访问控制列表应该如下设置：

动作	源IP地址	源端口号	目的IP地址	目的端口号	说明
禁止	110.10.160.0	*	*	*	禁止spam.com访问
允许	*	*	210.10.10.36	25	允许访问邮件服务器
禁止	*	*	*	*	缺省规则

网络层防火墙优点与缺点

- 网络层防火墙优点
  - 成本较低，容易在企业网的边界和内部大范围部署。
- 网络层防火墙缺点
  - 配置较为复杂，需要较为系统的网络知识。
  - 分组过滤器对网络服务的控制能力较弱，设计对网络服务的控制也比较复杂。
  - 缺乏严格的身份验证机制，网络攻击者可以假冒IP地址和端口号，攻破网络层防火墙。

应用层防火墙

- 应用层防火墙原理
- 应用层防火墙功能
- 应用层防火墙分类
- 应用层防火墙优点
- 应用层防火墙缺点

应用层防火墙原理

- 应用层防火墙是一种在两个同构网络之间为了安全控制而设置的一个用于报文转发的“网关”，用于实现不同安全域的某类具体网络应用协议的访问控制和转接。
- 应用层防火墙具有应用代理服务器的功能，即在符合访问控制规则前提下，代理一个安全域网络中的客户端请求另一个安全域网络中服务器的服务。

应用层防火墙原理图

- 典型的应用层防火墙处理示意图

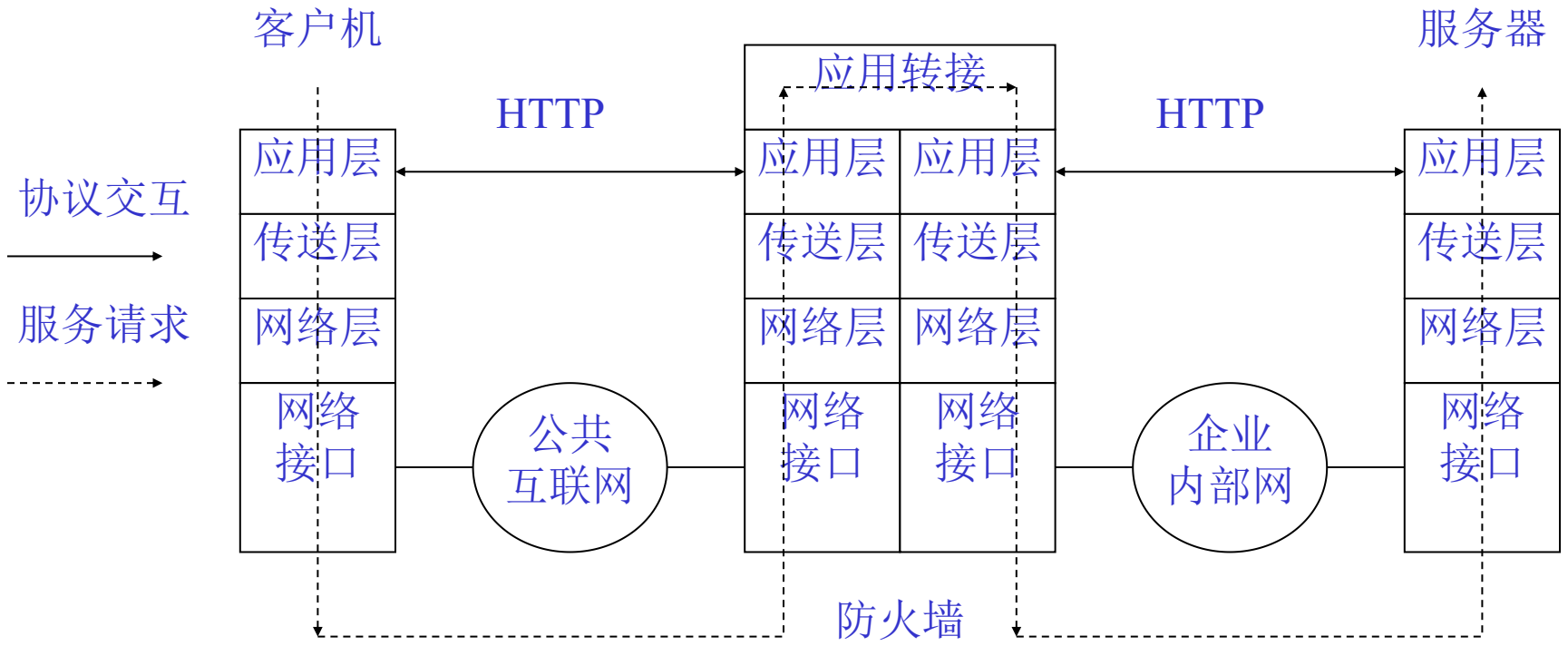


图4.7 应用层防火墙原理图

应用层防火墙功能

- 应用层防火墙可以根据应用协议类型进行访问控制，并且可以进一步根据网络用户身份进行访问控制。
- 对于安全控制机制较弱的防火墙，则仅仅识别HTTP/FTP等几个允许的应用协议，如果属于这些应用协议，则防火墙可以代理客户端向服务器发出服务请求。
- 对于安全控制机制较强的防火墙，则接收到客户端服务请求之后，还要求客户端输入用户名和登录口令(类似于网页登录)，在验证客户端真实身份之后，才能代理客户端向服务器发出请求(即代理服务器)。

应用层防火墙的部署分类

- 在应用层防火墙的工程化部署过程中，应用层防火墙通常根据它网络接口的数目，划分为
  - 单归宿防火墙(1个网络接口)；
  - 双归宿防火墙(2个网络接口)；以及
  - 三归宿防火墙(3个网络接口)。

双归宿防火墙实例

- 以下是双归宿防火墙实例：

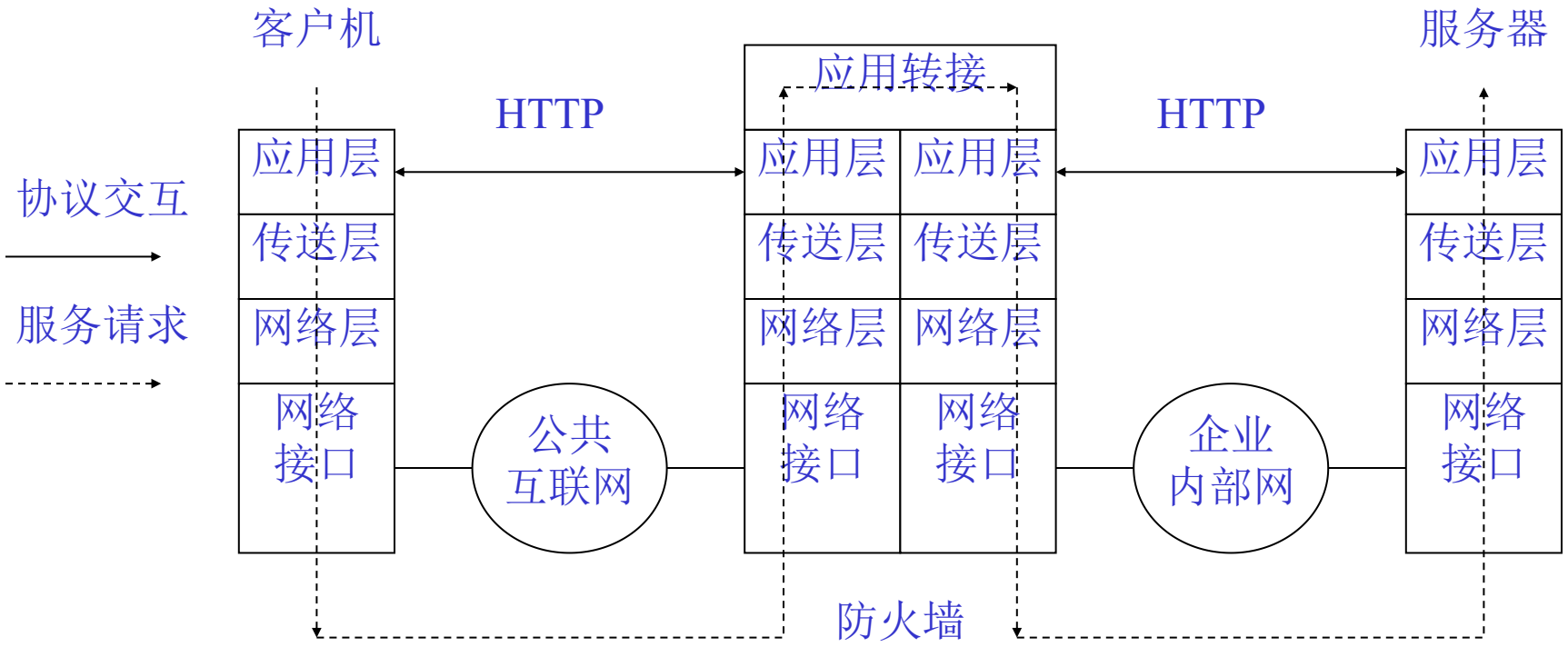


图4.7 应用层防火墙原理图

三归宿防火墙实例

- 以下是三归宿防火墙实例，是防火墙特有的网关形式，常用的防火窗产品结构。

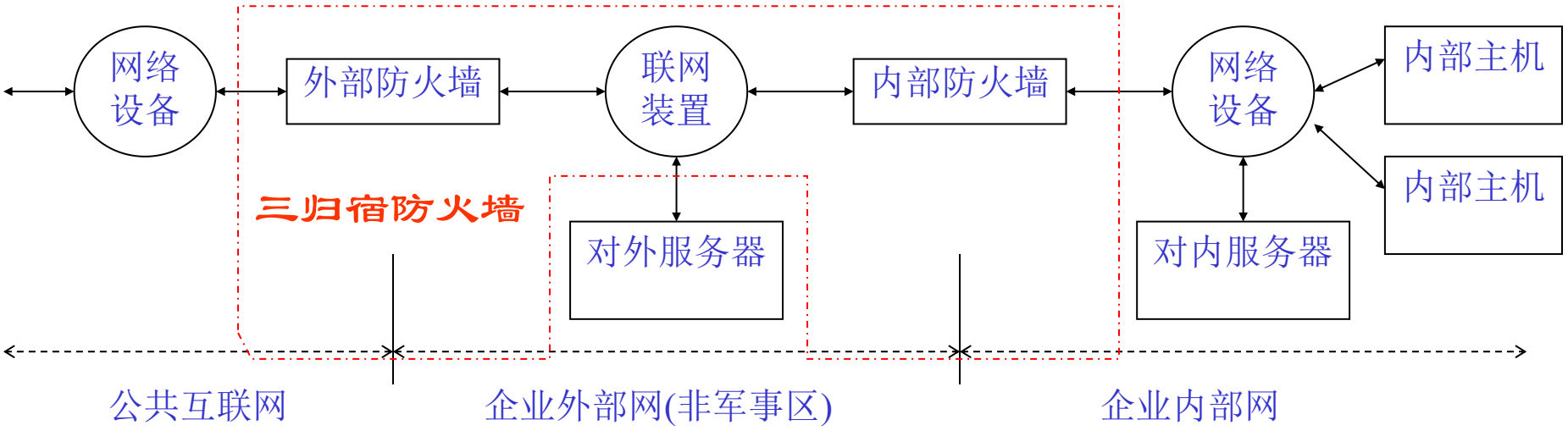
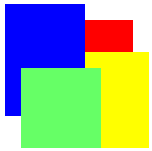


图4.5 防火墙应用的典型结构

应用层防火墙优点

- 具有配套的身份验证机制，针对具体的网络应用和网络服务进行安全控制，具有较强的访问控制能力。
- 具有较强的自身安全性。由于这种应用层防火墙软件采用专门设计的应用软件，仅仅设置了最基本的功能，软件漏洞较少。
- 具有较强的应用控制能力，可以在应用协议、用户身份、应用报文进行控制，可以在具体网络应用软件中增加特殊的过滤应用层服务请求的功能。



应用层防火墙缺点

- 需要为每种应用对应的应用协议设计专门的应用层防火墙软件。
- 对于新出现的网络应用可能造成了较大的障碍（如果缺省控制是“禁止”），有些新出现的网络应用就无法穿越应用层防火墙。

下一代网络防火墙的研发动因

- 网络应用的变化与发展：互联网中的85%以上的流量都是基于HTTP或HTTPS协议的Web应用，难以仅仅根据应用协议控制网络应用。互联网应用从Web 1.0的用户简单浏览功能发展到Web 2.0的用户可以编辑和发布内容等功能，防火墙已经不能仅仅提供企业外部网的浏览功能。
- 防火墙的自身不足：防火墙自身的配置和管理较为复杂，容易产生配置方面的漏洞。不同生产厂商的防火墙系统之间缺少可操作性，容易产生访问控制的不一致，难以满足系统性的访问控制需求。
- 现代网络攻击的更加精细化：现代网络攻击可以将自身伪装成为Web应用、可以攻破安全防护较弱的网络终端而窃取合法用户的访问账户和口令。

传统防火墙无法应对的威胁

Technology	How AET bypass?
Antivirus	Antivirus and antimalware work on endpoint devices. Threats bypass antivirus and antimalware by hiding activities in trusted systems and processes
Legacy Firewall	Advanced threats disguise activity as ordinary HTTP traffic or encrypt their data
Network Security Device	Advanced threats planted internally open holes through firewall and network security. Because of access to user accounts, hackers bypass internal network access controls.

下一代防火墙应对的方法

Technology	How NGFW works?
Antivirus	With application awareness, an NGFW analyze application traffic and report the potential threats by detecting malicious applications tunneling inside legitimate applications. Traditional firewall is limited to IP address and port.
Legacy Firewall	With the feature of application-specific content in NGFW, it can inspect encrypted traffic for malware by decrypting the packet stream.
Network Security Device	Most holes are created with command and control channel applications using well known ports, which can be detected by filtering application data. NGFW are capable of detecting outbound control and command protocols used by botnets

下一代网络防火墙的特征

Generation	Next Generation
Firewall Type	Deep Packet Inspection
OSI Layer	Application Layer
Main Functions	Looks deeps into packet and makes granular access control decisions based on packet header and payload. Excels in managing application and data driven threats. Incorporates intrusion detection and prevention technology features.

重点回顾

- 网络防火墙基本概念
  - 网络防火墙特征
  - 网络防火墙部署结构
- 网络层防火墙
  - 网络层防火墙功能
  - 网络层防火墙配置
- 应用层防火墙
  - 应用层防火墙原理
  - 应用层防火墙功能
- 下一代防火墙技术和特征

本章作业-1

应用题（1）假设某网络系统限定用户A1可以“读/写”访问目录D1、D2和D3中的文件，用户A2可以“读/写”访问目录D2和D3中的文件，用户A3可以“读/写”访问目录D3中的文件。问题：

1) 采用DAC策略实现以上访问控制，并说明实现过程。2) 采用MAC策略实现以上访问控制，并说明实现过程。3) 如果A3在A2中驻留了“特洛伊木马”软件，A3是否可以看到D2目录中的文件？为什么？

本章作业-2

应用题（2）如果需要设置一个分组过滤器，作为公共互联网与企业外部网之间的网络层防火墙。其安全策略1)只允许公共互联网访问企业外部网中的WWW服务器(210.110.10.1)和邮件服务器（210.110.10.3）；安全策略2)不允许attacker.com域名的子网(220.10.160.0)中的站点访问该WWW服务(端口号为80)，不允许spam.com域名的子网（230.101.130.0）访问该电子邮件服务(端口号为25)。需要解决一下问题：

1) 请设计该分组过滤器的访问控制列表，并说明各项含义。2) 如果发现公共互联网的一个网站（240.10.12.1)是一个恶意网站，如何更新网络层防火墙的配置，保护企业外部网的WWW服务器和邮件服务器？