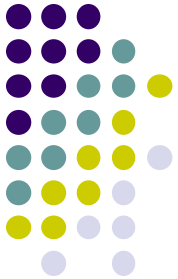
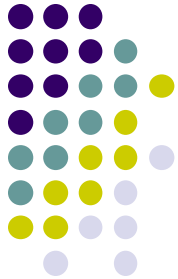


第7章
网络边防

第7章 内容概要

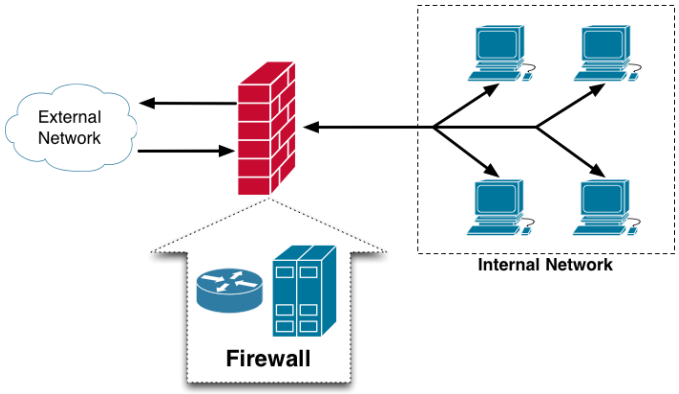
- 7.1 一般框架
- 7.2 分组过滤
- 7.3 电路网关
- 7.4 应用网关
- 7.5 可信系统和堡垒主机
- 7.6 防火墙配置
- 7.7 网络地址转换
- 7.8 配置防火墙

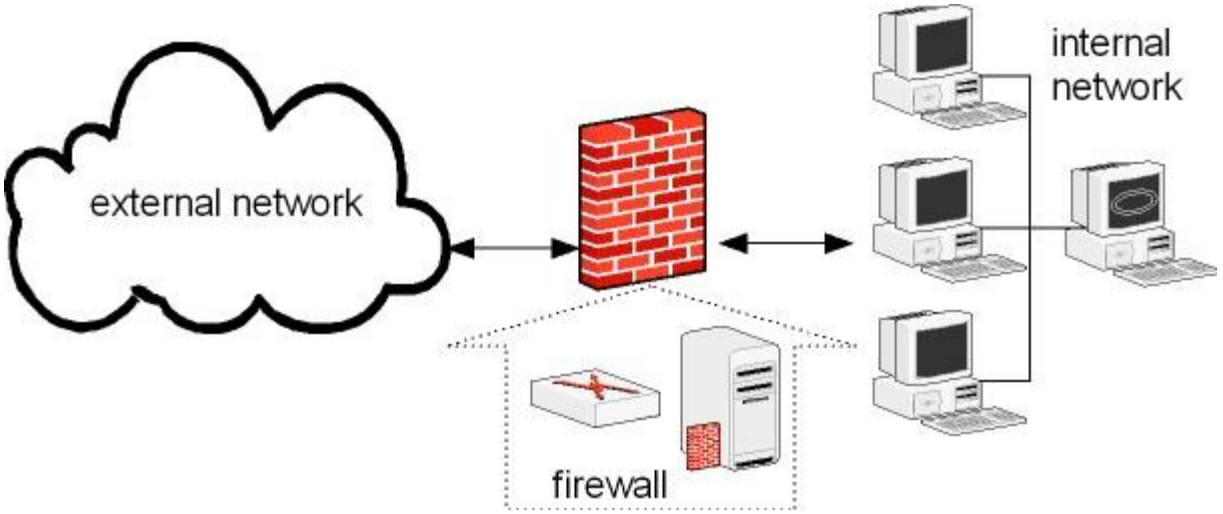
概述



- LANs, WANs, WLANs 都属于网络边界
  - 可能属于企业或家庭网络
  - 需要收到保护，以免被入侵
- 为什么要用防火墙?
  - 加密不行吗?
    - 不能组织恶意分组进入网络边界
  - 验证呢?
    - 可以确定收到的一个分组是否来自于可信的用户
    - 然而，不是所有主机都有资源运行验证算法
  - 管理主机的不同用户技术水平参差不齐

一般框架

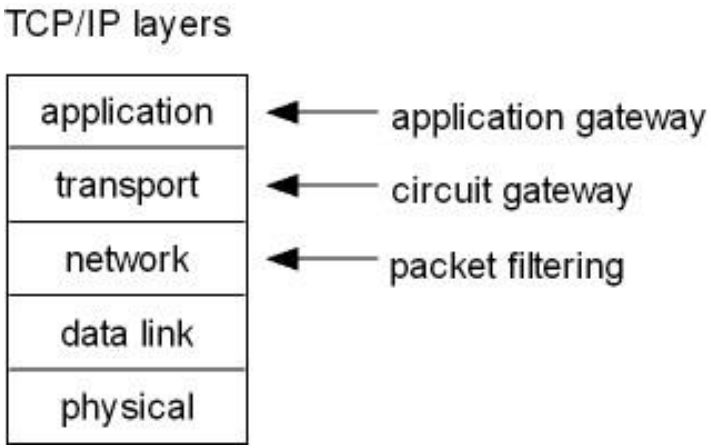




《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

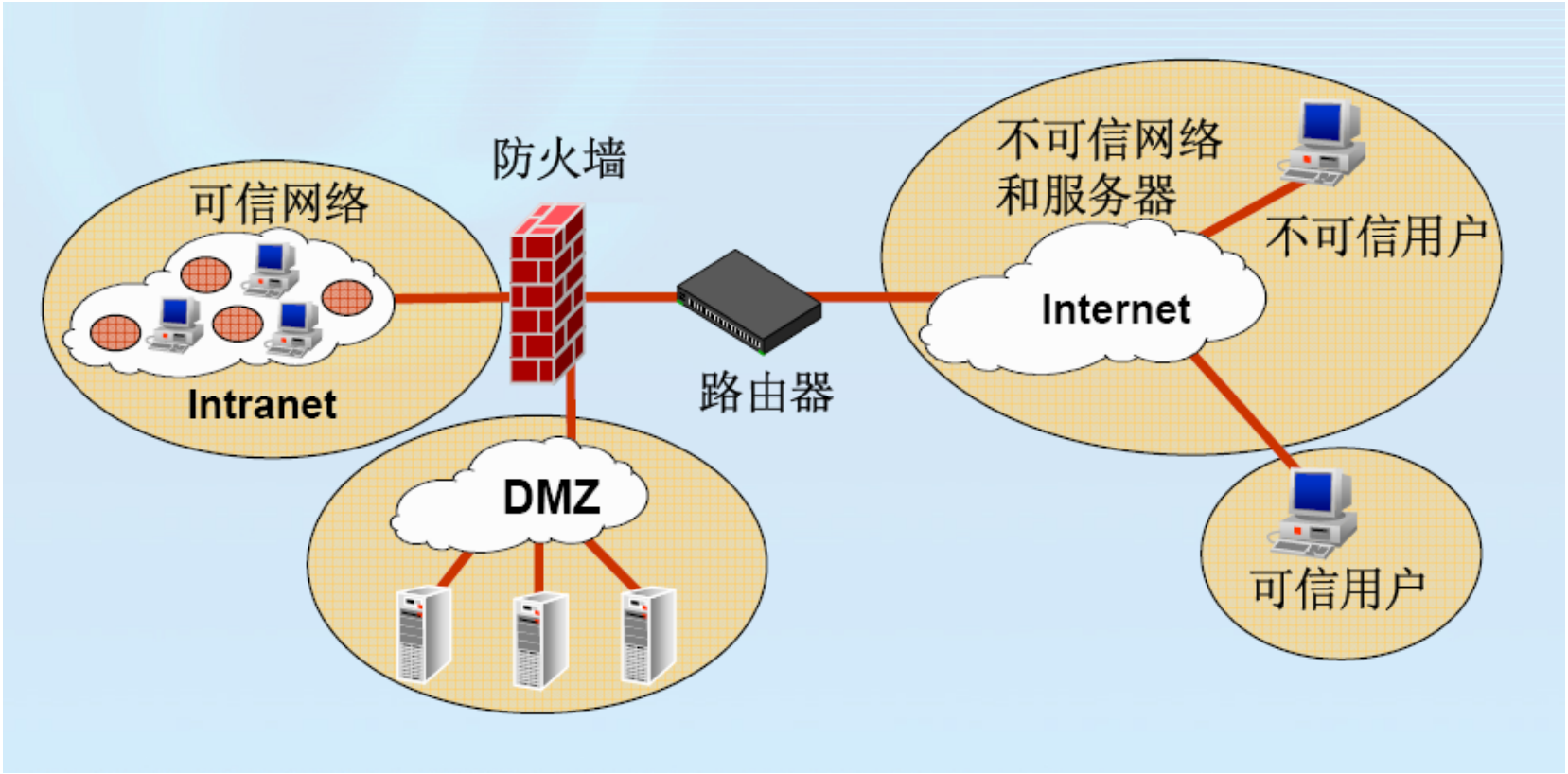
一般框架

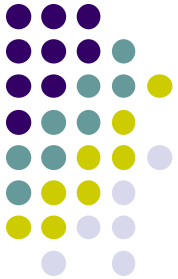
- 防火墙是什么?
  - 一个硬件设备, 一种软件,或者两者结合
  - 是Internet和网络边缘的一个界线(内部网络)
  - 一种过滤流入和外发分组的机制.
  - 可能是硬件和(或)软件
    - 硬件快但是升级不方便
    - 软件慢但便于升级



防火墙安置

- 什么是防火墙





什么是防火墙

定义:

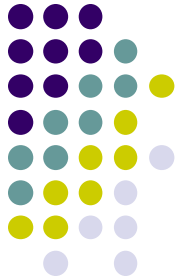
防火墙（Firewall）是一种用来加强网络之间访问控制的特殊网络互连设备，是一种非常有效的网络安全模型。

核心思想:

在不安全的网际网环境中构造一个相对安全的子网环境。

目的:

都是为了在被保护的内部网与不安全的非信任网络之间设立唯一的通道，以按照事先制定的策略控制信息的流入和流出，监督和控制使用者的操作。



什么是防火墙:

防火墙可在链路层、网络层和应用层上实现；

其功能的本质特征是隔离内外网络和对进出信息流实施访问控制。隔离方法可以是基于物理的，也可以是基于逻辑的；

从网络防御体系上看，防火墙是一种被动防御的保护装置。

防火墙的功能：

① 防火墙是网络安全的屏障；

② 防火墙可以强化网络安全策略；

③ 对网络存取和访问进行见空审计；

④ 防止内部信息的外泄；

防火墙仍不能完成的任务：

① 防火墙不能防御不通过防火墙的攻击

② 防火墙没有透视功能

特洛伊木马和病毒仍可以通过

不能检测隧道中的话务

不能检测加密话务

③ 防火墙的有效性很大程度上以来于安全策略

没有规则的防火墙只能简单地传输话务

防火墙的分类

1.个人防火墙

是在操作系统上运行的软件，可为个人计算机提供简单的防火墙功能；

大家常用的个人防火墙有：Norton Personal Firewall、天网个人防火墙、瑞星个人防火墙等；

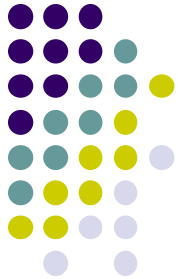
安装在个人PC上，而不是放置在网络边界，因此，个人防火墙关心的不是一个网络到另外一个网络的安全，而是单个主机和与之相连接的主机或网络之间的安全。

防火墙的分类

2. 软件防火墙

个人防火墙也是一种纯软件防火墙，但其应用范围较小，且只支持Windows系统，功能相对来说要弱很多，并且安全性和并发连接处理能力较差；

作为网络防火墙的软件防火墙具有比个人防火墙更强的控制功能和更高的性能。不仅支持 Windows 系统，并且多数都支持 Unix 或Linux系统。如十分著名的Check Point FireWall-1，Microsoft ISA Server 2000等。



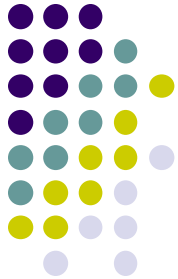
防火墙的分类

3. 一般硬件防火墙

不等同于采用专用芯片的纯硬件防火墙，但和纯软件防火墙有很大差异；

一般由小型的防火墙厂商开发，或者是大型厂商开发的中低端产品，应用于中小型企业，功能比较全，但性能一般；

一般都采用PC架构（就是一台嵌入式主机），但使用的各个配件都量身定制。



防火墙的分类

3.一般硬件防火墙

其操作系统一般都采用经过精简和修改过内核的Linux或Unix，安全性比使用通用操作系统的纯软件防火墙要好很多，并且不会在上面运行不必要的服务，这样的操作系统基本就没有什么漏洞。但是，这种防火墙使用的操作系统内核一般是固定的、不可升级的，因此新发现的漏洞对防火墙来说可能是致命的。

国内自主开发的防火墙大部分都属于这种类型。

防火墙的分类

4.纯硬件防火墙

采用专用芯片（非X86芯片）来处理防火墙核心策略的一种硬件防火墙，也称为芯片级防火墙。（专用集成电路（ASIC）芯片或者网络处理器（NP）芯片）；

最大的亮点：高性能，非常高的并发连接数和吞吐量；

采用ASIC芯片的方法在国外比较流行，技术也比较成熟，如美国NetScreen公司的高端防火墙产品；国内芯片级防火墙大多还处于开发发展的阶段，采用的是NP技术。

防火墙的分类

5.分布式防火墙

前面的几种防火墙都属于边界防火墙（Perimeter Firewall），它无法对内部网络实现有效地保护；

随着人们对网络安全防护要求的提高，产生了一种新型的防火墙体系结构——分布式防火墙。近几年，分布式防火墙技术已逐渐兴起，并在国外一些大的网络设备开发商中得到实现，由于其优越的安全防护体系，符合未来的发展趋势，这一技术一出现就得到了许多用户的认可和接受。

第7章 内容概要

- 7.1 一般框架
- 7.2 分组过滤
- 7.3 电路网关
- 7.4 应用网关
- 7.5 可信系统和堡垒主机
- 7.6 防火墙配置
- 7.7 网络地址转换
- 7.8 配置防火墙

数据包过滤

- 包过滤防火墙对所接收的每个数据包做允许拒绝的决定。防火墙审查每个数据报以便确定其是否与某一条包过滤规则匹配。过滤规则基于可以提供给IP转发过程的包头信息。
- 包头信息中包括IP源地址、IP目标端地址、类型（TCP、UDP、ICMP、或IPTunnel）、TCP/UDP目标端口、ICMP消息类型、TCP包头中的ACK位置。

数据包过滤

- 包过滤防火墙使得防火墙能够根据特定的服务允许或拒绝流动的数据，因为多数的服务侦听都在已知的端口上。例如，Telnet服务器在TCP的23号端口上监听远地连接，而SMTP服务器在TCP的25号端口上监听人连接。为了阻塞所有进入的Telnet连接，防火墙只需简单的丢弃所有TCP端口号等于23的数据包。为了将进来的Telnet连接限制到内部的数台机器上，防火墙必须拒绝所有TCP端口号等于23并且目标IP地址不等于允许主机的IP地址的数据包。

数据包过滤

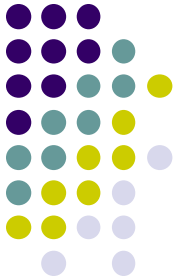
优点：

逻辑简单，价格便宜，易于安装和使用，网络性能和透明性好。

主要缺点：

① 安全控制只限于源地址、目的地址和端口号等，不能保存与传输或与应用相关的状态信息，因而只能进行较为初步的安全控制，安全性较低；

② 数据包的源地址、目的地址以及端口号等都在数据包的头部，很有可能被窃听或假冒。



数据包过滤

注意：

① 创建规则比较困难；

② 规则过于复杂并难以测试，必须要用手工或用仪器才能彻底检测规则的正确性；

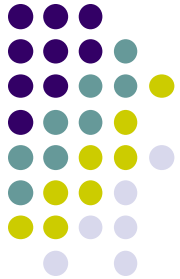
③ 对特定协议包的过滤：

FTP协议：使用两个端口，因此要作特殊的考虑；

UDP协议：要对UDP数据包进行过滤，防火墙应有动态数据包过滤的特点；

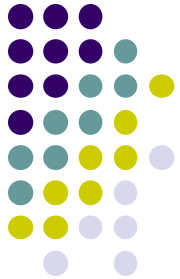
ICMP协议：应根据ICMP的类型进行过滤。

分组过滤



- 执行分组进入和外出的过滤
- 仅监视IP和TCP/UDP的头部, 不考虑负载
- 既可以执行无状态的也可以执行有状态的过滤
  - 无状态的过滤: 容易实现但非常简单
  - 有状态的过滤: 较难实现但功能强大

无状态的过滤



- 执行“哑的”过滤
  - 应用静态规则集来监视每个分组
  - 不保留之前分组的结果
- 所用规则集称为访问控制列表 (ACL)
  - 自顶向下的匹配规则，应用匹配到的第一个规则
  - 如果没有匹配的规则,则按照缺省规则过滤

ACL 实例

Sample ACL rules for ingress filtering

int addr	int port	ext addr	ext port	action	Comment
*	*	129.63.8.52	*	block	Block all packets from this IP
192.63.8.254	110	*	*	allow	Open internal POP3 port

Sample ACL rules for egress filtering

int addr	int port	ext addr	ext port	action	Comment
*	*	129.63.8.52	*	block	Block all packets to this IP
*	*	*	25	allow	Allow packets to external SMTP
*	*	*	>1023	allow	Allow packets to non-privileged ports

- 阻止来自于特定IP地址或者端口的外发和流入的分组
- 监控一个由内部地址作为源IP的流入分组以过滤可能经过精心设计的（恶意）分组
- 鉴别那些通过指定特定路由器试图绕开防火墙的分组
- 监视那些净载荷很小可能是分片攻击的分组
- 阻止控制分组外发

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

有状态的过滤

- 比无状态的过滤智能
  - 保持对内部和外部主机连接的跟踪
  - 仅接受/拒绝基于连接状态的分组
  - 通常和无状态的过滤组合使用
- 必须关注内存和CPU的时间需求; 连接跟踪是非常耗费资源的!

client addr	*client port*	*server addr*	*server port*	*connection state*	*protocol*
219.22.101.32	1030	129.63.24.84	25	established	*TCP*
219.22.101.54	1034	129.63.24.84	161	established	*UDP*
210.99.201.14	2001	129.63.24.87	80	established	*TCP*
24.102.129.21	3389	129.63.24.87	110	established	*TCP*

连接状态表实例

《计算机网络安全的理论与实践（第2版）》. 【美】王杰, 高等教育出版社, 2011年.

状态检测

状态检测防火墙是在动态包过滤的基础上，增加了状态检测机制而形成的；

动态包过滤与普通包过滤相比，需要多做一项工作：对外出数据包的“身份”做一个标记，允许相同连接的进入数据包通过。

状态检测

利用状态表跟踪每一个网络会话的状态，对每一个数据包的检查不仅根据规则表，更考虑了数据包是否符合会话所处的状态；

状态检测防火墙采用了一个在网关上执行网络安全策略的软件引擎，称之为检测模块。检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各层实施监测，并动态地保存起来作为以后制定安全决策的参考。

状态检测

状态检测 既能够提供代理服务的控制灵活性，又能够提供包过滤的高效性，是二者的结合；

工作过程：

对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接；请求数据包通过，并记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表，就可以通过。

状态检测

主要优点：

① 高安全性（工作在数据链路层和网络层之间；“状态感知”能力）

② 高效性（对连接的后续数据包直接进行状态检查）

③ 应用范围广（支持基于无连接协议的应用）

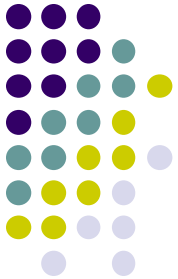
主要缺点：

状态检测防火墙在阻止DDoS攻击、病毒传播问题以及高级应用入侵问题（如实现应用层内容过滤）等方面显得力不从心。

第7章 内容概要

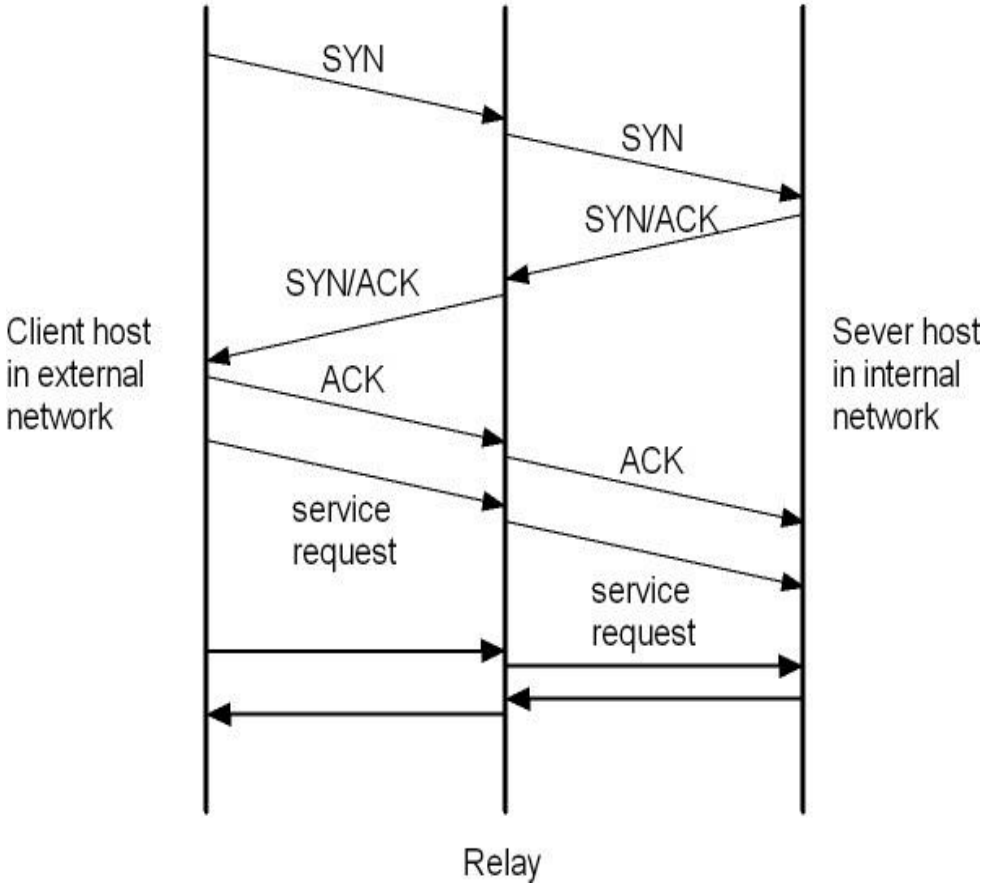
- 7.1 一般框架
- 7.2 分组过滤
- 7.3 电路网关
- 7.4 应用网关
- 7.5 可信系统和堡垒主机
- 7.6 防火墙配置
- 7.7 网络地址转换
- 7.8 配置防火墙

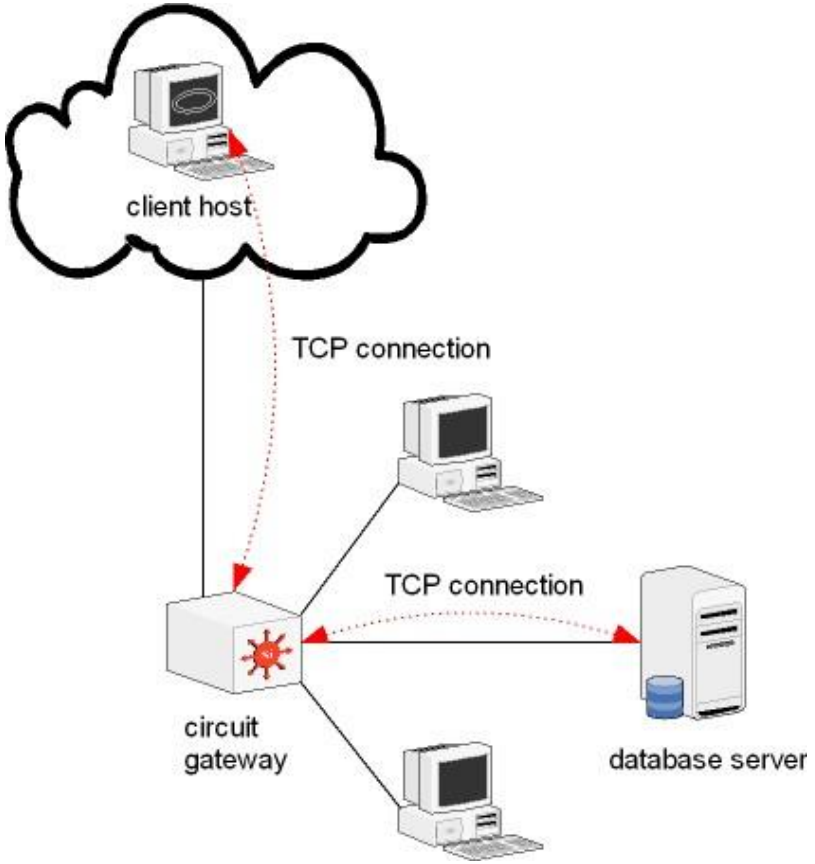
电路网关



- 运行在传输层
- 审查TCP/UDP段的IP地址信息和端口号信息来确定该连接是否合法
- 在应用中，通常将分组过滤和电路网关结合起来
- 基本结构:
  - 在一个内部主机和外部主机形成一个TCP中继连接
  - 不允许内外部网络直接连接
  - 对有效连接维护一个表并且检查不符合列表规则的流入分组

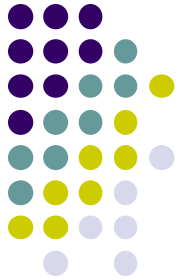
实例





《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

SOCKS协议

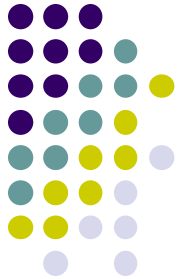


- 一个为了实现电路网关的网络协议
- 由三部分组成:
  - SOCKS 服务器
    - 在1080端口上运行一个分组过滤防火墙
  - SOCKS 客户端
    - 运行在外部网络的客户端
  - SOCKS 客户端库
    - 运行在内部客户端
  - 目的在于为鉴别和建立连接而验证信息
  - 为远程网络提供了一个验证过的中继

第7章 内容概要

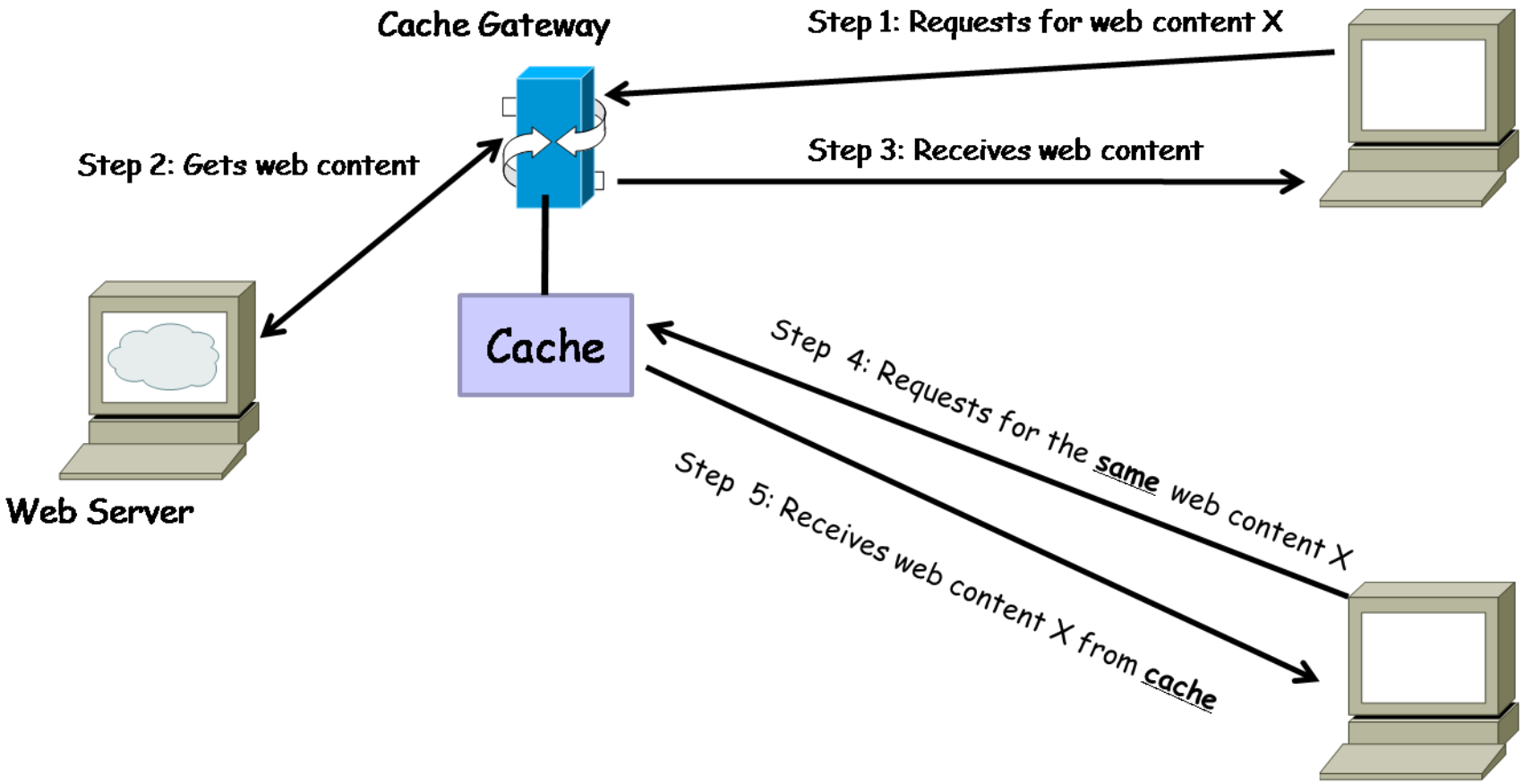
- 7.1 一般框架
- 7.2 分组过滤
- 7.3 电路网关
- 7.4 应用网关
- 7.5 可信系统和堡垒主机
- 7.6 防火墙配置
- 7.7 网络地址转换
- 7.8 配置防火墙

应用网关



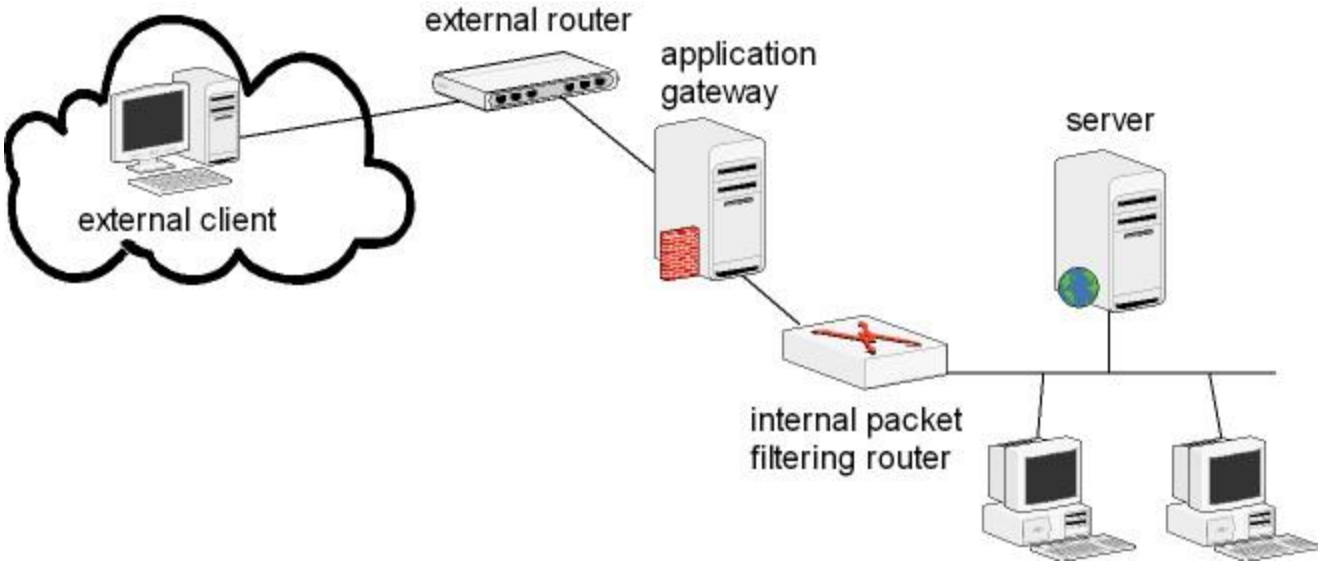
- 也叫做应用级网关或代理服务器
- 扮演内部主机的代理角色, 处理来自外部客户端的服务请求
- 对所有分组执行深度检查
  - 检查应用程序格式
  - 基于负载应用规则
  - 具有检测恶意和可疑分组的能力
- 对资源需求极为敏感

缓存网关



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

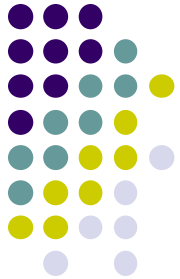
应用网关



在网关后安置一个路由器用于保护网关和内部主机之间的连接

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

有状态的分组监视



- 有状态的分组过滤在应用级的扩展
  - 支持扫描分组负载
  - 若分组不匹配协议期望的连接或数据类型，则丢弃该分组

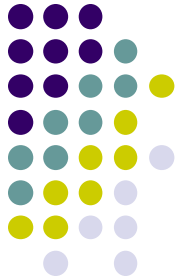
第7章 内容概要

- 7.1 一般框架
- 7.2 分组过滤
- 7.3 电路网关
- 7.4 应用网关
- 7.5 可信系统和堡垒主机
- 7.6 防火墙配置
- 7.7 网络地址转换
- 7.8 配置防火墙

可信系统和堡垒主机

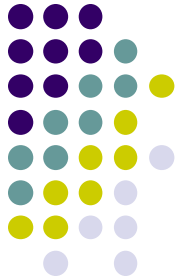
- 应用网关被部署在内部网络和外部网络之间
  - 暴露在外部网络的攻击下
- 需要强大的安全保护
  - 可信操作系统
  - 堡垒主机

可信操作系统



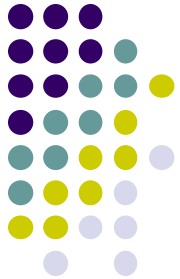
- 一个满足一套特定安全需求的操作系统
  - 系统设计不包含缺陷
  - 系统软件不包含漏洞
  - 系统正确配置
  - 系统管理恰当
- 可能包含多个具有不同安全许可的用户
- 必须服从关于许可权的严格的规则

访问权限



- 不往上读
  - 具有低级别许可的用户不能执行具有高级别密级的程序
  - 具有低级别密级的程序不能读具有高级别密级的文件
- 不往下写
  - 具有高级别许可的用户不能用低级别密级的程序相一个文件写数据
  - 具有高级别密级的程序不能向低级别密级的文件里写数据

堡垒主机



- 具有强防御机制的系统
- 服务于主机从而实现：
  - 网关
  - 电路网关
  - 其它类型的防火墙
- 运行在一个可信的操作系统上
  - 必须不能包含不必要的功能
- 保持系统的简单以减少出错的概率

需求

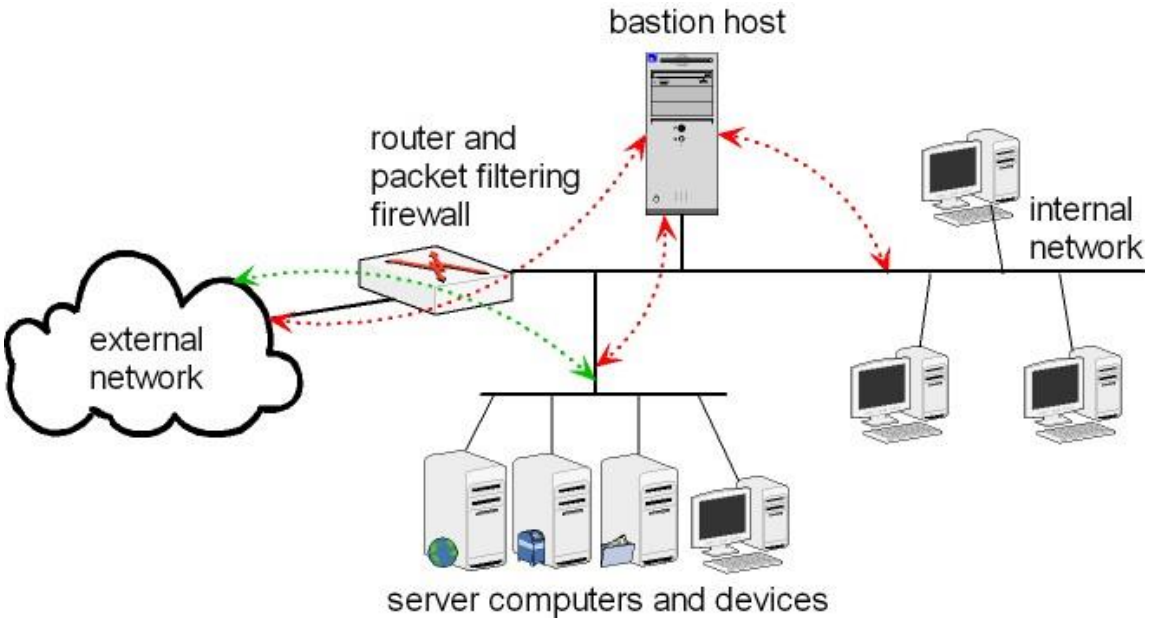
- 网关软件应该仅用小的模块实现
- 可能在网络层提供用户的验证
- 应该被连接到尽可能少的内部主机上
- 系统内多有事务的大规模的日志都应该保留
- 如果多个网关运行在单一主机上，他们必须相互独立的运行
- 主机应该避免写数据到他们的硬盘上
- 运行在堡垒主机上的网关不应该被赋予管理权限

第7章 内容概要

- 7.1 一般框架
- 7.2 分组过滤
- 7.3 电路网关
- 7.4 应用网关
- 7.5 可信系统和堡垒主机
- 7.6 防火墙配置
- 7.7 网络地址转换
- 7.8 配置防火墙

单界面堡垒系统

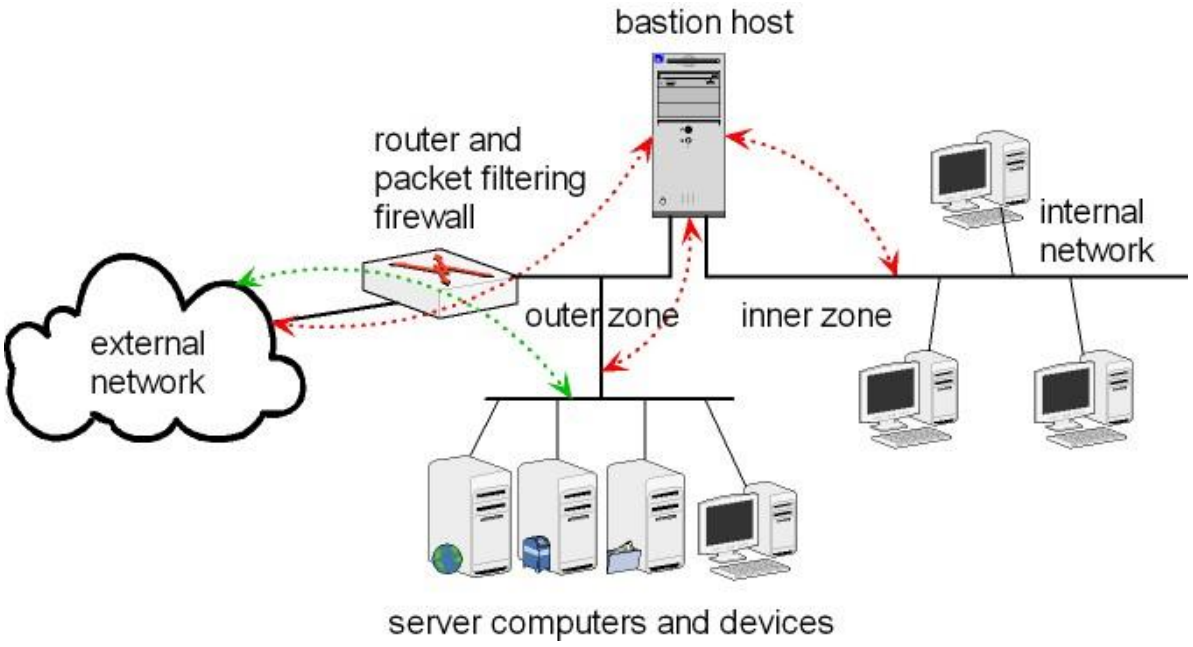
- 由一个分组过滤路由器和一个堡垒主机组成
  - 路由器用于连接内部和外部网络
  - 堡垒主机在内部网络
- 分组过滤防火墙（PF firewall）检查每个外发分组，如果其源地址不是堡垒主机的IP地址，则将其阻挡
- 如果分组过滤路由器受到损害，攻击者可能修改ACL并绕过堡垒主机



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

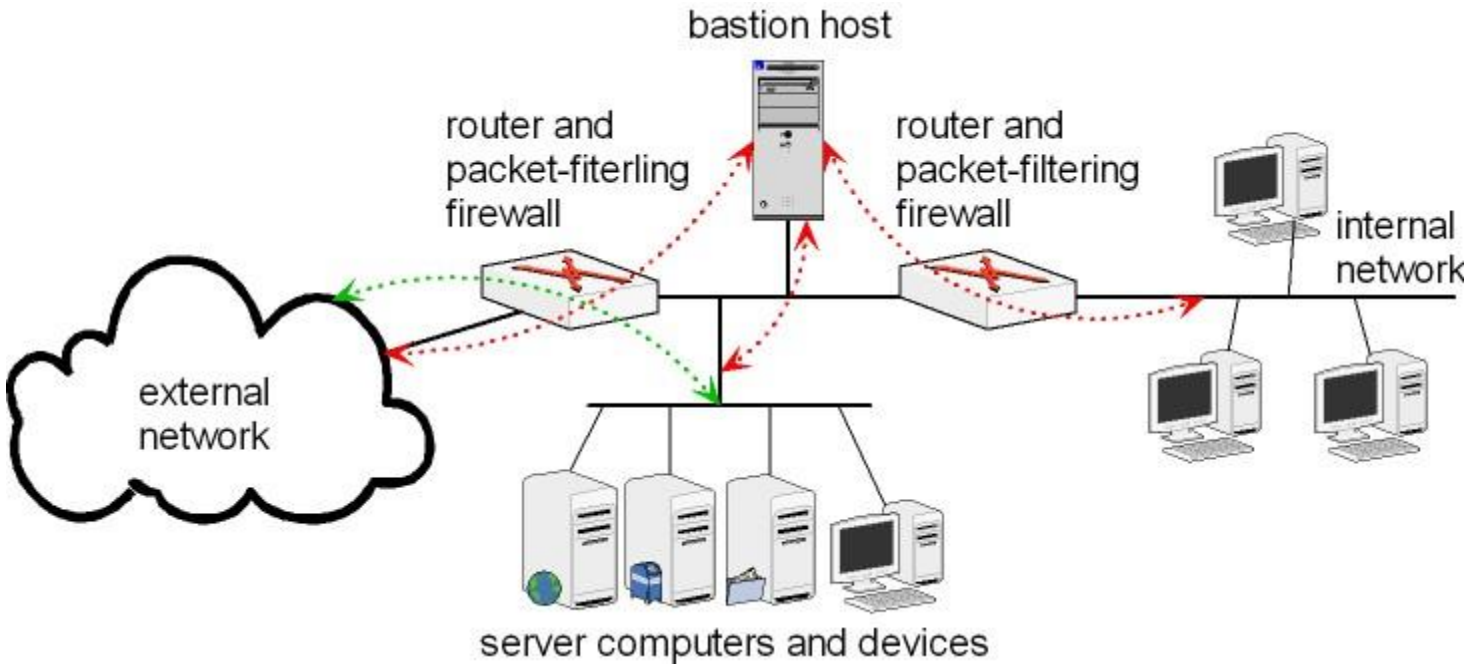
双界面堡垒系统

- 在内部网络中有两个区域:
  - 内区: 从外部不可访问
  - 外区: 来自Internet的主机可以访问
- 内区的主机受到堡垒主机和分组过滤路由器的双重保护
- 外区的服务器分组过滤路由器保护
- 即使分组过滤路由器受损也能阻止外部对内部网络的访问



《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

子网监控防火墙系统

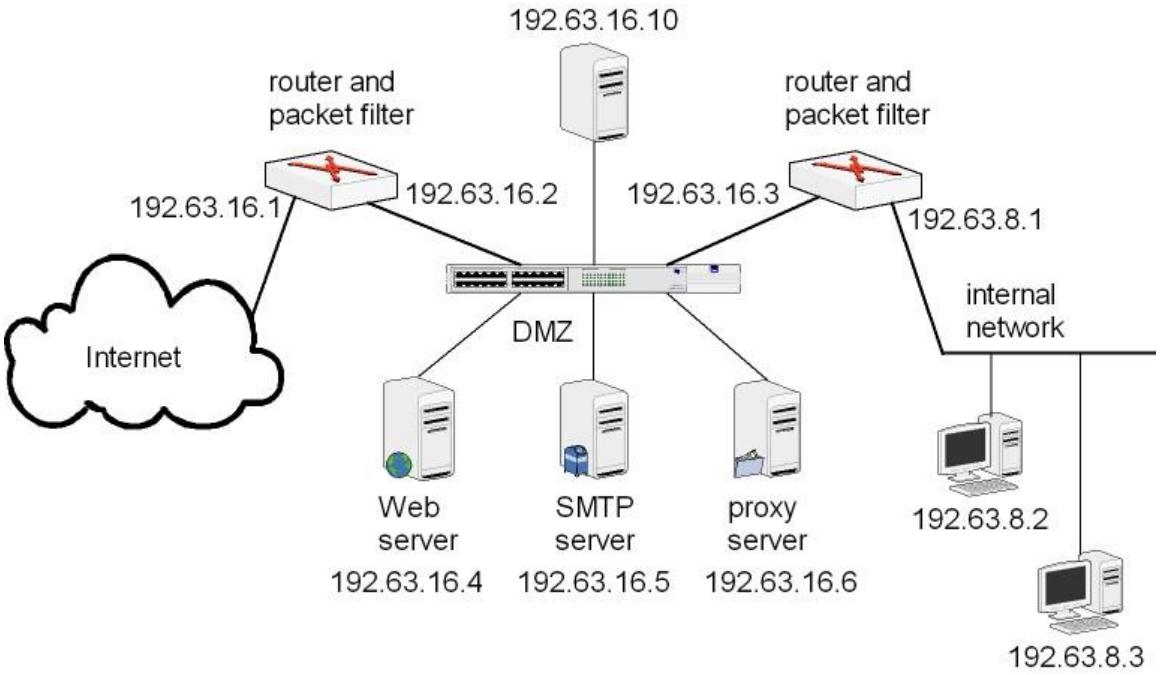


- 一个单界面堡垒系统网络为内部网络配备一个二级分组过滤路由器
- 两个分组过滤路由器之间的区域被称一个监控子网
- 将内部网络结构隐藏起来

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

非军事区 (DMZ)

- 在一个内部网络中两个防火墙之间的一个子网
  - 外部防火墙将DMZ和外部威胁隔离开来
  - 内部防火墙将内部网络和DMZ隔离开来

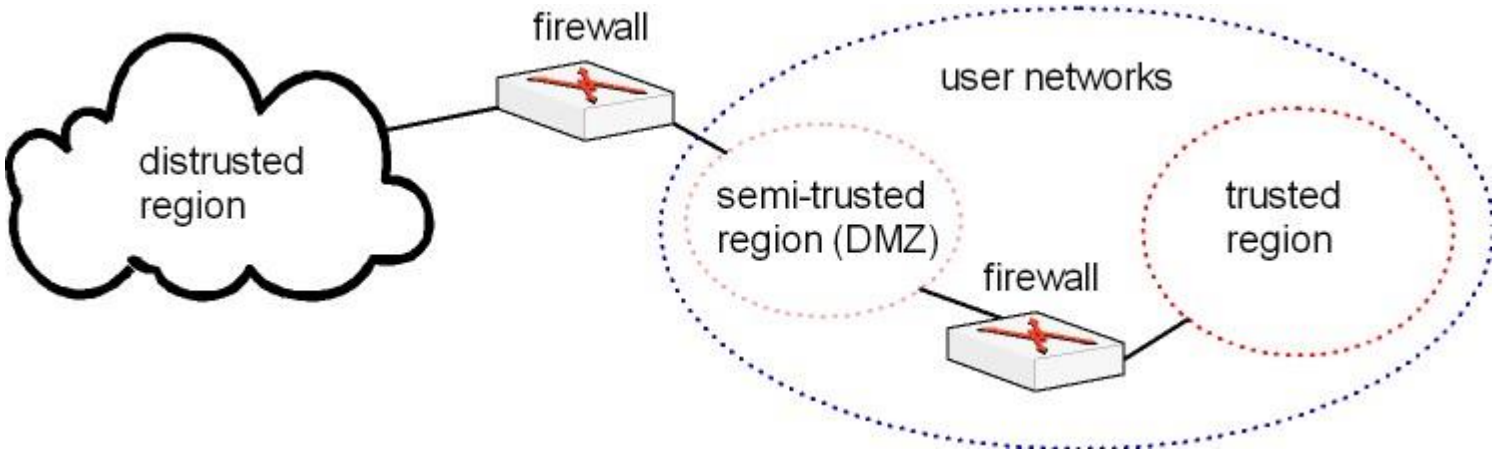


- DMZs 可以以一种层次结构来实现

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

网络安全技术

- 防火墙将网络分为三个区域:
  - 非信任区域
  - 半信任区域
  - 可信区域



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

第7章 内容概要

- 7.1 一般框架
- 7.2 分组过滤
- 7.3 电路网关
- 7.4 应用网关
- 7.5 可信系统和堡垒主机
- 7.6 防火墙配置
- 7.7 网络地址转换
- 7.8 配置防火墙

网络地址转换(NAT)

- 将IP地址分为公有和私有（不可路由）两个组
  - 互联网地址编码分配机构指定了三个IP块作为私有地址
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
- 许多私有地址可通过一个或几个公有IP地址接入Internet
  - 在IPv4里，克服了地址匮乏问题（2^{32}）

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

网络地址转换

（1）客户机将数据包发给运行NAT的计算机。

（2）NAT将数据包中的端口号和专用的IP地址换成它自己的端口号和公用的IP地址，然后将数据包发给外部网络的目的主机，同时记录一个跟踪信息在映像表中，以便向客户机发送回答信息。

（3）外部网络发送回答信息给NAT。

（4）NAT将所收到的数据包的端口号和公用IP地址转换为客户机的端口号和内部网络使用的专用IP地址并转发给客户机。

网络地址转换

NAT的主要作用：

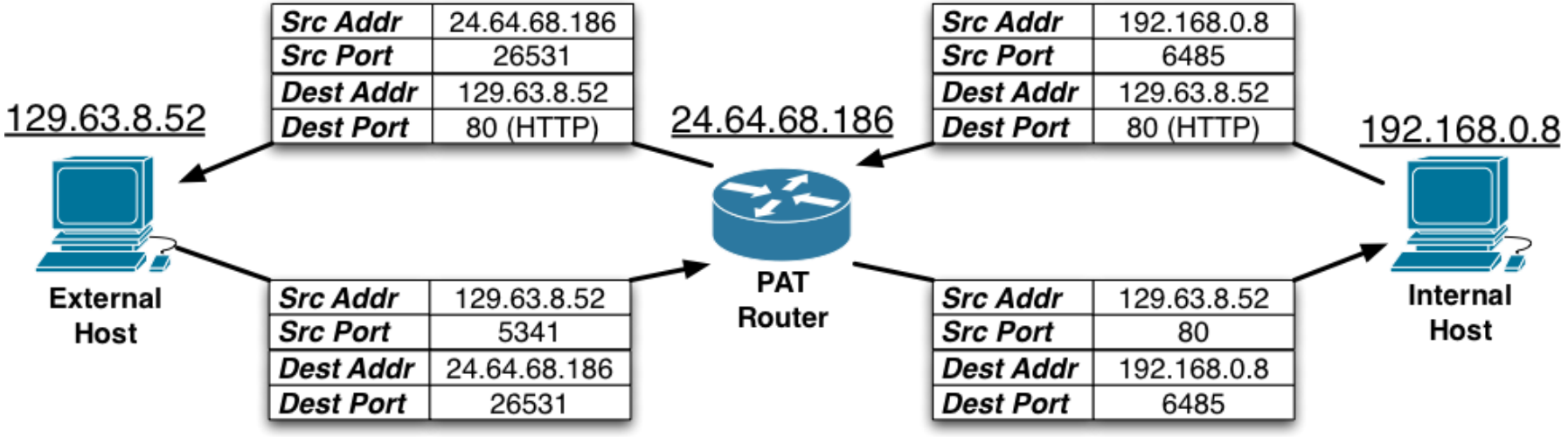
① 隐藏内部网络的IP地址；

② 解决地址紧缺问题。

注意：NAT本身并不是一种有安全保证的方案，它仅仅在包的最外层改变IP地址。所以通常要把NAT集成在防火墙系统中。

动态NAT

- 动态地指定少数几个共有IP地址给私有地址
- 端口地址转换 (PAT), 是NAT的一个变种
  - 允许一个或更多的私有网络共享一个单一的IP
  - 通常由家庭或小企业网络使用
  - 通过重新映射分组的源和目的地址和端口号来工作



《计算机网络安全的理论与实践（第2版）》. 【美】王杰, 高等教育出版社, 2011年.

网络地址转换

静态网络地址转换:

内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。

动态网络地址转换:

可用的合法IP地址是一个范围，而内部网络地址的范围大于合法IP的范围，在做地址转换时，如果合法IP都被占用，此时从内部网络的新的请求会由于没有合法地址可以分配而失败。

网络地址转换

端口地址转换:

把内部地址映射到外部网络的一个单独的IP地址上，同时在该地址上加上一个由NAT 设备选定的 TCP 端口号，这样所有不同的信息流看起来好象来源于同一个IP地址。

网络地址转换

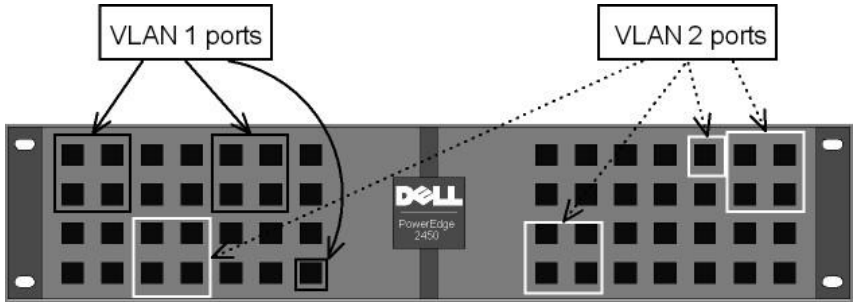
比较：

静态地址翻译：不需要维护地址转换状态表，功能简单，性能较好；

动态转换和端口转换：必须维护一个转换表，以保证能够对返回的数据包进行正确的反向转换，功能强大，但是需要的资源较多。

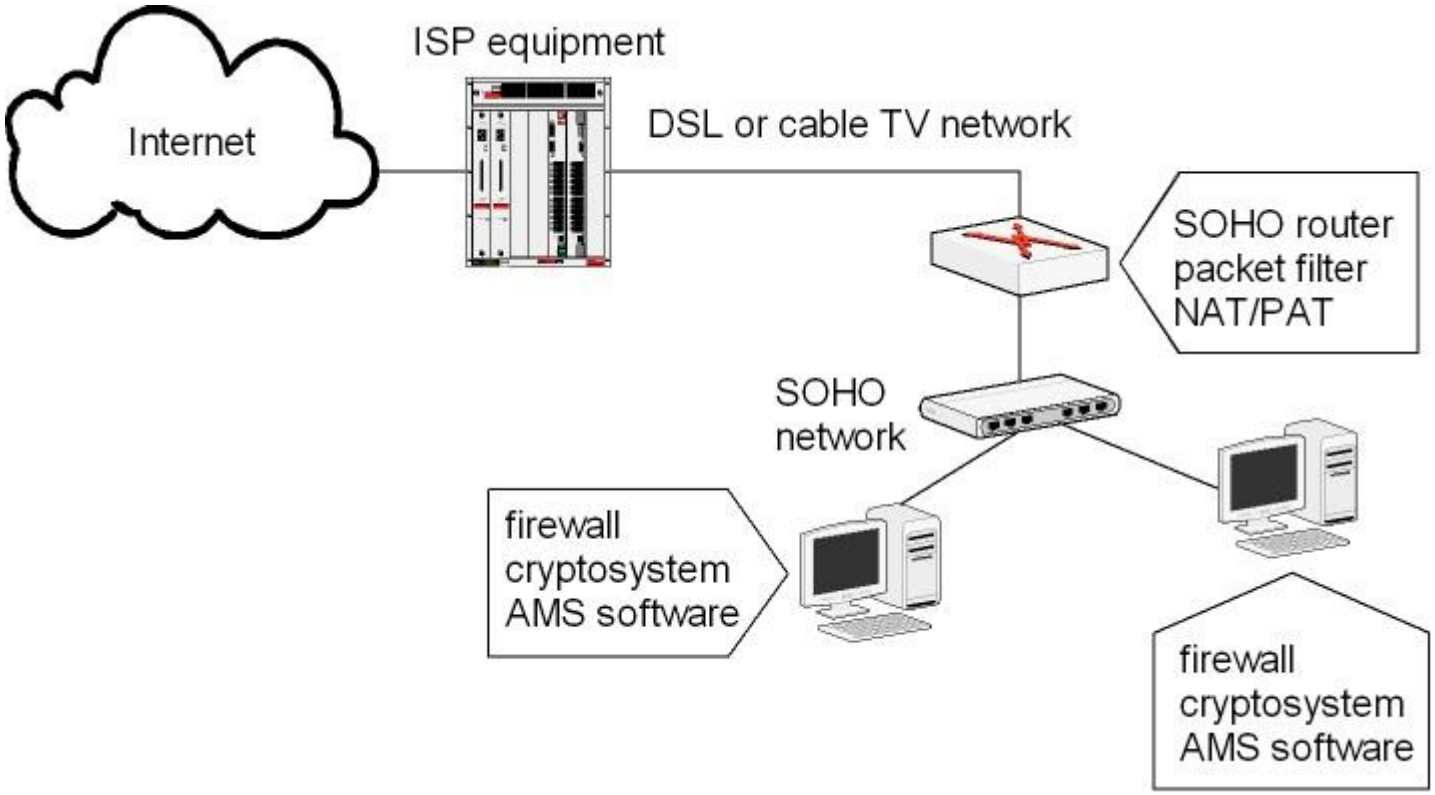
虚拟局域网 (VLAN)

- 一种在同一个物理网络中构建多个独立的逻辑局域网的技术
- VLANs 可由软件来创建
- VLAN 交换机: 一个VLAN交换机可以配置成多个逻辑的交换端口组，从而实现独立的VLAN



《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

小型办公和家庭网络防火墙(SOHO)

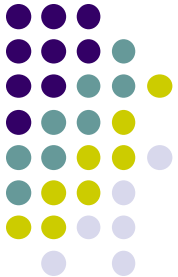


《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

第7章 内容概要

- 7.1 一般框架
- 7.2 分组过滤
- 7.3 电路网关
- 7.4 应用网关
- 7.5 可信系统和堡垒主机
- 7.6 防火墙配置
- 7.7 网络地址转换
- 7.8 配置防火墙

配置防火墙



- Windows 系统:
  - 控制面板中内置防火墙
- Linux
  - *使用iptables*:

    iptables <option> <chain> <matching criteria> <target>

    实例:

    iptables –A INPUT –p TCP –s 129.63.8.109 –j ACCEPT

    iptables –A INPUT –p TCP ! –syn –d 129.63.8.109 –j ACCEPT

    iptables –A INPUT –p TCP –d 129.63.8.109 telnet –j DROP
- FreeBSD UNIX
  - 使用 *ipf*