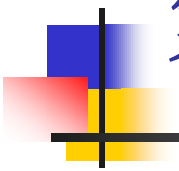


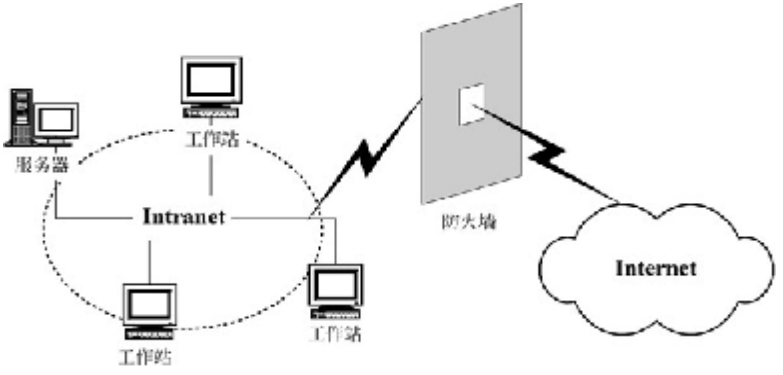
第5章　防火墙技术

5.1　防火墙基本概念
5.2　防火墙技术原理
5.3　防火墙的应用与维护
5.4　防火墙技术的发展趋势

5.1 防火墙基本概念

- 为了建筑安全，人们常在寓所之间砌起一道砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所。
- 防火墙（**Firewall**）是在两个网络之间执行访问控制策略的一个或一组系统，包括硬件和软件，目的是保护网络不被他人侵扰。本质上，它遵循的是一种允许或阻止业务来往的网络通信安全机制，也就是提供可控的过滤网络通信，只允许授权的通信。
- 通常，防火墙就是位于内部网或**Web**站点与因特网之间的一个路由器或一台计算机，又称为堡垒主机。其目的如同一个安全门，为门内的部门提供安全，控制那些可被允许出入该受保护环境的人或物。就像工作在前门的安全卫士，控制并检查站点的访问者。

5.1 防火墙基本概念



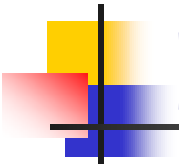
- 所有进入和离开的数据都必须经过防火墙检查，只有符合访问控制政策的数据才允许通过
- 从逻辑上讲，防火墙是分离器、限制器和分析器。从物理角度看，各站点防火墙物理实现的方式有所不同。通常防火墙是一组硬件设备，即路由器、主计算机或者是路由器、计算机和配有适当软件的网络的多种组合。

Firewall Characteristics

- 防火墙可以在网络边界实施访问控制政策
  - **Only authorized traffic (defined by the local security police) will be allowed to pass**
- 防火墙可以记录所有的访问
- 防火墙可以隐藏内部网络
  - **The firewall itself is immune to penetration (use of trusted system with a secure operating system)**

防火墙不可以做什么

- 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防病毒



防火墙弊端

- 防火墙破坏了Internet端到端的特性，阻碍了新的应用的发展
- 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

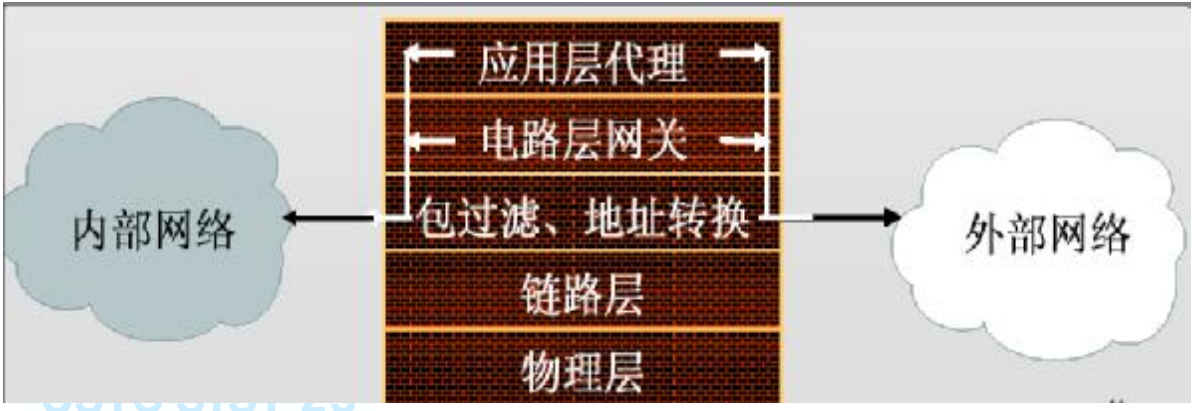
5.2 防火墙技术原理

Four general techniques:

- **Service control**
  - **Determines the types of Internet services that can be accessed, inbound or outbound**
- **Direction control**
  - **Determines the direction in which particular service requests are allowed to flow**
- **User control**
  - **Controls access to a service according to which user is attempting to access it**
- **Behavior control**
  - **Controls how particular services are used (e.g. filter e-mail)**

防火墙的分类

- 包过滤技术(Packet filtering/screening)
- 电路层网关(Socks)
- 应用层代理(Proxy)
- 地址转换（NAT）



数据包过滤

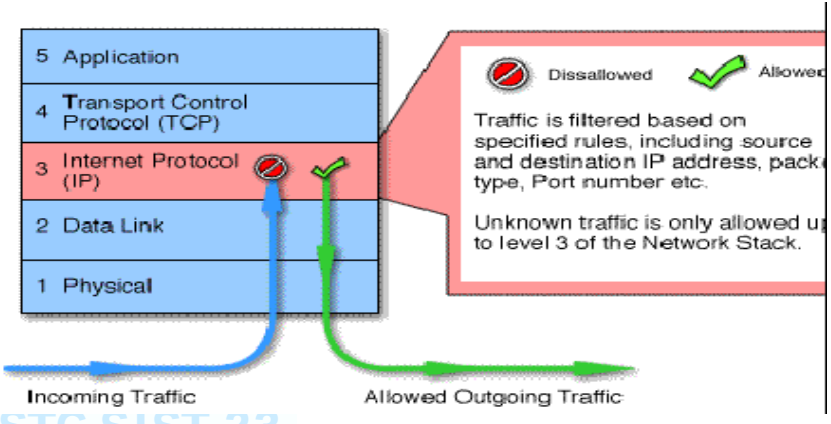
- 防火墙通常是一个具备包过滤功能的简单路由器，支持因特网安全。这是使因特网联接更加安全的一种简单方法，因为包过滤是路由器的固有属性。
- 包是网络上信息流动的单位。在网上传输的文件一般在发出端被划分成一串数据包，经过网上的中间站点，最终传到目的地，然后这些包中的数据又重新组成原来的文件。
- 每个包有两个部分：数据部分和包头。包头中含有源地址和目标地址等信息。
- 包过滤一直是一种简单而有效的方法。通过拦截数据包，读出并拒绝那些不符合标准的包头，过滤掉不应入站的信息。

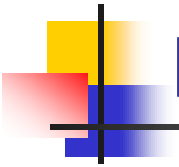
数据包过滤

- 基本的思想
  - 在网络层对数据包进行选择
  - 对于每个进来的包，适用一组规则，然后决定转发或者丢弃该包
- 判断依据有(只考虑IP包)：
  - 数据包协议类型：TCP、UDP、ICMP、IGMP等
  - 源、目的IP地址
  - 源、目的端口：FTP、HTTP、DNS等
  - IP选项：源路由、记录路由等
  - TCP选项：SYN、ACK、FIN、RST等
  - 其它协议选项：ICMP ECHO、ICMP ECHO REPLY等
  - 数据包流向：in或out
  - 数据包流经网络接口：eth0、eth1

常见包过滤设备/软件

- 路由器访问控制表ACL
- 硬件包过滤设备
- 软件：ipchains / netfilter

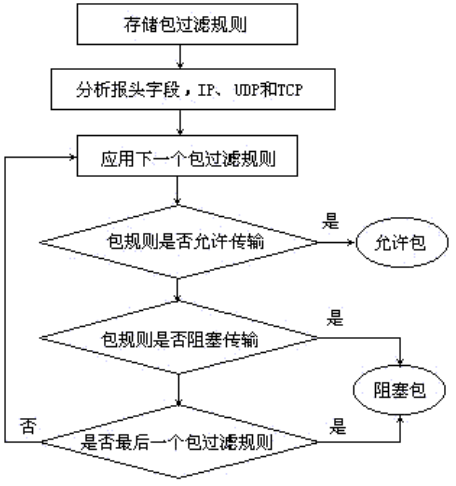




Packet-filtering Router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)

过滤器规则设计例



- 假设网络策略安全规则确定：从外部主机发来的因特网邮件在某一特定网关被接收，并且想拒绝从不信任的**CREE-PHOST**的主机发来的数据流。
- **SMTP**使用的网络安全策略必须翻译成包过滤规则：
  - **[过滤器规则1]**：我们不相信从**CREE-PHOST**来的连接。
  - **[过滤器规则2]**：我们允许与我们的邮件网关的连接。

过滤器规则设计例

- 这些规则可以编成表。其中星号（*）表明它可以匹配该列的任何值。
- 对于过滤器规则**1**：阻塞任何从（*）**CREE-PHOST**端口来的到我们任意（*）主机的任意（*）端口的连接。
- 对于过滤器规则**2**：允许任意（*）外部主机从其任意（*）端口到我们的**Mail-GW**主机端口的连接。

过滤器规则设计例

序	动作	内部主机	内	外部主机	外	说明
1	阻塞	*	*	Cree-phost	*	阻塞来自CREEPHOST流量
2	允许	Mail-GW	25	*	*	允许我们的邮件网关的连接
3	允许	*	*	*	25	允许输出SMTP至远程邮件网关

- 对于过滤器规则3 ：表示了一个内部主机发送SMTP邮件到外部主机端口25。如果外部站点对SMTP不使用端口25，那么SMTP发送者便发送邮件。
- 这些规则应用的顺序与它们在表中的顺序相同。如果一个包不与任何规则匹配，它就会遭到拒绝。表中规定：它允许任何外部机器从端口25产生一个请求。端口25应该保留SMTP。

依据地址进行过滤

- 在包过滤系统中，最简单的方法是依据地址进行过滤。用地址进行过滤可以不管使用什么协议，仅根据源地址/目的地址对流动的包进行过滤。我们可用这种方法只让某些被指定的外部主机与某些被指定的内部主机进行交互。

依据服务进行过滤

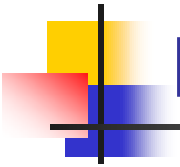
1．往外的Telnet服务

在往外的Telnet服务中，一个本地用户与一个远程服务器交互。我们必须对往外与往内的包都加以处理。

2．往内的Telnet服务 ACK位，端口

3．依据源端口来过滤

依据源端口来过滤必须有个前提，提供端口号的机器必须是真实的。如若入侵者已经通过root完全控制了这台机器，那他就可随意在这台机器上，也就等于在我们包过滤规则的端口上运行任意的客户程序或服务器程序。有时我们就根本不能相信由对方机器提供的机器源地址，因为有可能那台机器就是入侵者伪装的。



Packet-filtering Router

- **Advantages:**
  - **Simplicity**
  - **Transparency to users**
  - **High speed**
- **Disadvantages:**
  - **Difficulty of setting up packet filter rules**
  - **Lack of Authentication**

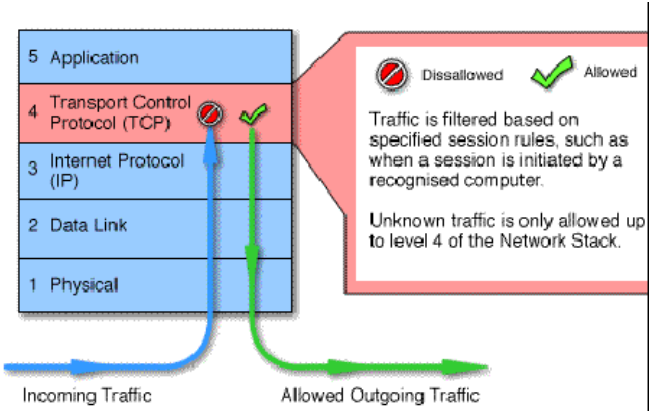
Packet-filtering Router

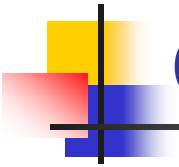
- **Possible attacks and appropriate countermeasures**
  - **IP address spoofing**
    - 利用IP地址并不是出厂的时候与MAC固定在一起的，攻击者通过自封包和修改网络节点的IP地址，冒充某个可信节点的IP地址，进行攻击。
  - **Source routing attacks**
    - 利用IP数据包中的一个选项-IP Source Routing来指定路由，利用可信用户对服务器进行攻击，特别是基于UDP协议的由于其是面向非连接的，更容易被利用来攻击
  - **Tiny fragment attacks**

电路层网关（Circuit Gateway）

- 工作在传输层/会话层
  - 根据数据包的标志位建立一个连接状态表
  - 对于收到的某个IP包，检查它是否属于某一个会话？
  - 跟踪一段时间内一个会话中经过包的总数
- 常见设备/软件
  - 商业防火墙硬件/软件
  - 免费软件：Socksd
- 相关标准
  - rfc1928.txt

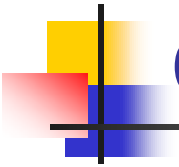
Circuit-level Gateway





Circuit-level Gateway

- Stand-alone system or
- Specialized function performed by an Application-level Gateway
- Sets up two TCP connections
- The gateway typically relays TCP segments from one connection to the other without examining the contents



Circuit-level Gateway

- The security function consists of determining which connections will be allowed
- Typically use is a situation in which the system administrator trusts the internal users
- An example is the SOCKS package
  - E.g. SocksCap32

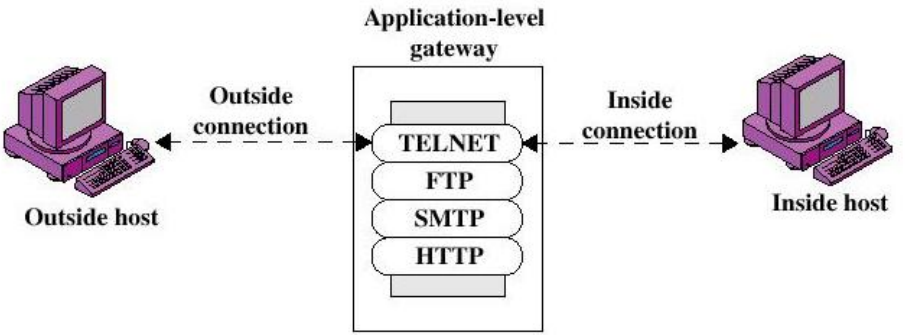
Circuit-level Gateway

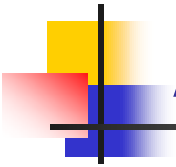
- 优点
  - 支持所有**TCP**应用
  - 保持状态，可以检测、防范**SYN Flood**类型的攻击
  - 隐藏内部网络
- 缺点
  - 对应用不透明，应用软件必须经过**socksified**才能使用防火墙
  - 保持状态，可能造成网络中断
  - 性能的开销较大
  - 防火墙本身易受**DOS**攻击

应用层代理（Proxy Server）

- 工作在应用层(Application Layer)
- 应用/协议相关(Protocol specific),比如telnet , http , smtp ,pop , ftp proxy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, Netscape, MS ISA 2000等

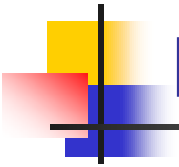
Application-level Gateway





Application-level Gateway

- **Advantages:**
  - **Higher security than packet filters**
  - **Only need to scrutinize a few allowable applications**
  - **Easy to log and audit all incoming traffic**
  - 用户认证、细粒度的访问控制
  - 对于**Web**应用，提供内容缓存功能（**cache** ）
- **Disadvantages:**
  - **Additional processing overhead on each connection (gateway as splice point)**
  - 协议相关的，需要对每一种应用协议编写**Proxy**程序



Bastion Host

- A system identified by the firewall administrator as a critical strong point in the network´s security
- The bastion host serves as a platform for an application-level or circuit-level gateway

地址转换（NAT）

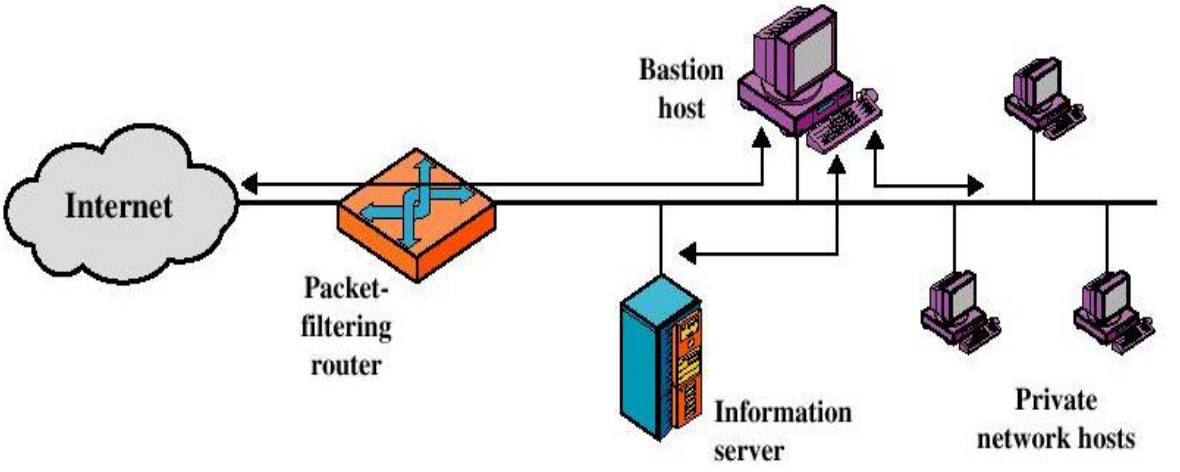
- 类似路由器，工作在网络层。除了转发以外，完成地址转换
- 不能提供额外的安全性，但是可以隐蔽内部网络，节省地址空间
- 转换方式
  - 静态地址转换
  - 动态地址转换
  - 静态地址转换＋端口映射（Port Mapping）
  - 动态地址转换＋端口映射

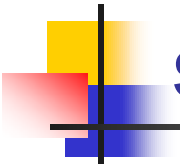
5.3 防火墙的应用与维护

- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- Three common configurations

Firewall Configurations

- **Screened host firewall system (single-homed bastion host)**



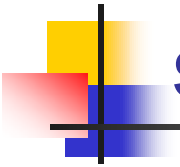


single-homed bastion host

- Screened host firewall, single-homed bastion configuration
- Firewall consists of two systems:
  - A packet-filtering router
  - A bastion host

single-homed bastion host

- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router
- The bastion host performs authentication and proxy functions

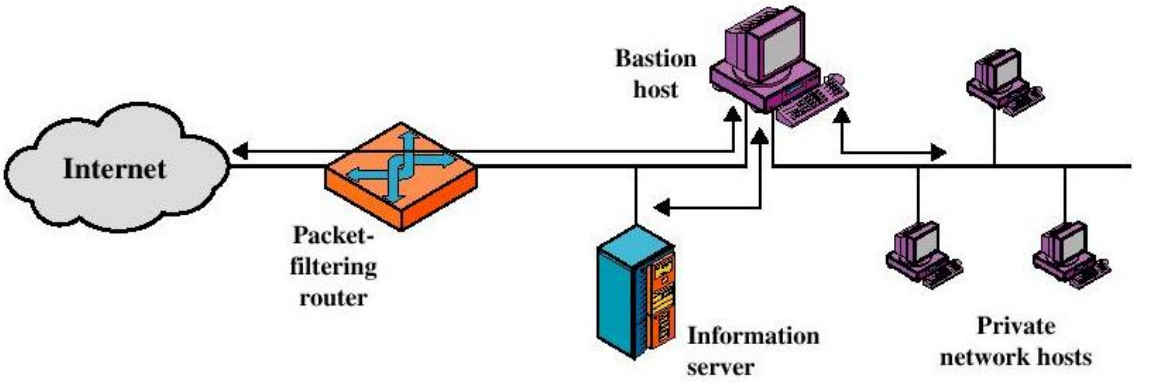


single-homed bastion host

- Greater security than single configurations because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
  - An intruder must generally penetrate two separate systems
- This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)

Screened host firewall system (dual-homed bastion host)

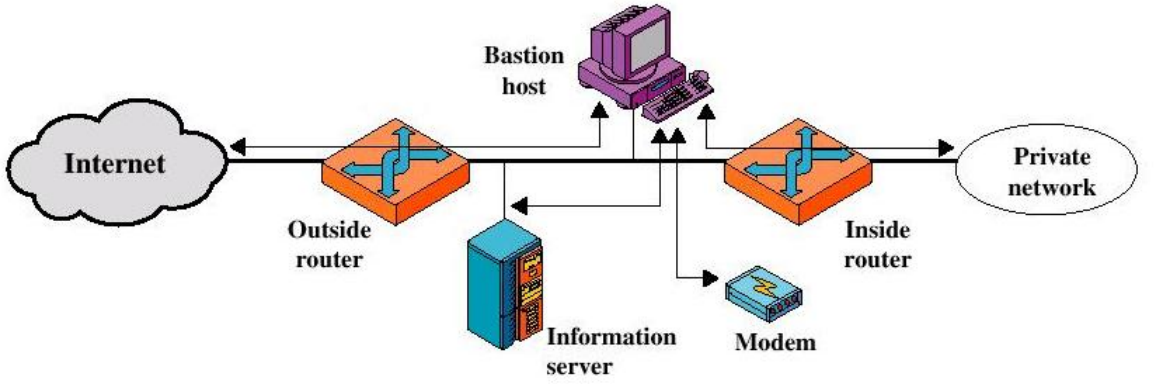
双重宿主主机，双网卡



Screened host firewall system (dual-homed bastion host)

- **Screened host firewall, dual-homed bastion configuration**
  - **The packet-filtering router is not completely compromised**
  - **Traffic between the Internet and other hosts on the private network has to flow through the bastion host**

Screened-subnet firewall system屏蔽子网



- Most secure configuration of the three
- Two packet-filtering routers are used
- Creation of an isolated sub-network

Screened-subnet firewall system屏蔽子网

- 外部路由器
  - 只允许对DMZ的访问
  - 拒绝所有以内部网络地址为源地址的包进入内部网络
  - 拒绝所有不以内部网络地址为原地址的包离开网络
- DMZ(Demilitarized zone), 不设防区
  - 通常放置DNS, Web , Email, FTP，Proxy Server等
- 内部路由器
  - 保护内部网络，防止来自Internet或DMZ的访问
  - 内部网络一般不对外部提供服务，所以拒绝外部发起的一切连接，只允许内部对外的访问

Screened-subnet firewall system屏蔽子网

- **Advantages:**
  - **Three levels of defense to thwart intruders**
  - **The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)**
  - **The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet)**

防火墙的设计与选择

- 你需要防火墙做什么？
  - 你的安全政策是什么：你要保护什么？哪些行为是允许的？哪些行为是禁止的？
- 缺省允许原则与缺省拒绝原则
  - 你的用户需要访问哪些服务？你的网络提供哪些服务？你的网络规模有多大，带宽是多少，实际流量有多大，将来的扩展性怎样？
- 你需要多高的安全性？怎样的可靠性？

防火墙的设计与选择

- 功能
  - 防火墙类型（包过滤/电路层网关/应用代理）
  - 支持的网络接口类型（10M/100M/1000M）
  - 支持的协议（对于代理服务器）
  - 是否支持地址翻译(NAT)，虚拟专网(VPN)
  - 如何扩展，怎样实现负载平衡(Load Balancing)
  - 用户身份验证方式：口令，RADIUS/Kerberos
  - 实时监控、审计、报警能力
  - 管理与维护的能力

防火墙的设计与选择

- 性能：
  - 对不同大小的包的转发能力
  - 并发会话数目（对于状态包过滤、代理服务器）
  - 最大允许的规则数目
  - 是否具有自动加固宿主机功能
  - 可靠性，稳定性，是否提供双机热备份功能
- 从防火墙实时检测主防火墙的工作状态，一旦发现主防火墙死机、系统崩溃，从防火墙将立即取代主防火墙进行工作，同时从防火墙会及时向管理员发送报警信息，通知管理员对发现故障的防火墙及时进行维修。

防火墙的设计与选择

- 价格 http://zdc.zol.com.cn/507/5073905.html
- 典型的防火墙产品
  - 华为**USG**系列
  - **Cisco**思科公司的**ASA5505**、**5520**
  - **Checkpoint**公司的**FireWall-1**
  - **Netscreen**公司的**Netscreen**系列
  - **Axent**公司的**Raptor**
  - **NAI**公司的**Gaunlet**

个人防火墙

- 个人防火墙**(Personal Firewall)**顾名思义是一种个人行为的防范措施，这种防火墙不需要特定的网络设备，只要在用户所使用的**PC** 上安装软件即可。 由于网络管理者可以远距离地进行设置和管理，终端用户在使用时不必特别在意防火墙的存在，极为适合小企业等和个人等的使用。
- 常见的个人防火墙有：
  - **360**防火墙、天网防火墙、瑞星防火墙、费尔个人防火墙、江民防火墙和金山网镖等。
  - **Symantec**公司的诺顿系列、**Comodo**防火墙、**Network Ice**公司的**BlackIce Defender** 、**Zone Labs**的**ZoneAlarm** 及***Windows****自带的****Firewall/Security Center***等

    修改**Win7**旗舰版远程桌面端口
- 移动平台的防火墙 一般不提供对外服务
  - 手机防火墙 - 智能手机软件 拒接黑名单中的电话和短信
  - 流量控制 - 每个应用是否可以通过移动数据网络和**wifi**访问互联网

防火墙的测试与维护

1. 测试

   a. IP欺骗 b. 端口监控 c. 检查规则数据库

   d. 验证连接正常 e.了解OS f. 端口扫描

2. 探测工具 telnet netcat(瑞士军刀)
   Send IP　　伪造TCP/UDP会话

3. 防火墙日志 拦截和警告

   第三方日志

防火墙测试的标准RFC2979

5.4 防火墙技术的发展趋势

- 防火墙技术作为目前用来实现网络安全的一种手段，主要是用来拒绝未经授权的用户访问网络、存取敏感数据，同时允许合法用户不受妨碍地访问网络，充分地共享网络资源。如果使用得当，可以在很大程度上提高网络的安全性能，但是并不能百分之百地解决网络上的信息安全问题。
- 防火墙虽然能对外部网络的攻击进行有效的防护，但对来自内部网络的攻击却无能为力。事实上，据统计，60％以上的网络安全问题来自内部网络，而且在网络程序和网络管理系统中也可能存在缺陷。

5.4 防火墙技术的发展趋势

- 网络安全单靠防火墙是不够的，还需要考虑其他技术和非技术的因素，如信息加密技术、制订法规、提高网络管理使用人员的安全意识等。
- 现在网络防火墙技术在不断地发展，值得研究的课题
  - 如何对一个防火墙产品进行危险评估，标准化；
  - 如何对网络中传输的敏感数据进行加密，数据应在网络哪一层加密，采用传统密码体制还是公钥密码体制；
  - 如何在网络协议中增加鉴别机制对通信双方的身份进行鉴别，
  - 防火墙算法设计，知识工程和专家系统在防火墙安全策略研究中的应用；
  - 如何减少对网络性能的影响，设计开放的与硬件平台和软件平台无关的防火墙产品等等。

5.4 防火墙技术的发展趋势

高性能、智能化、多功能（防病毒、内容过滤）

- 防火墙将从目前对子网或内部网管理方式向远程上网集中管理方式发展，分布式防火墙，可视化。

  主机防火墙对于分布式防火墙来讲是一个必要的组成部分，因为在局域网中的每一台主机上我们都会安装一个主机防火墙，它要负责执行安全策略，这个安全策略就是由管理中心进行制定和分发的，这时主机防火墙就成为了分布式防火墙的一个策略执行节点。
- 过滤深度不断加强，从目前的地址、服务过滤，发展到**URL(**页面**)**过滤，关键字过滤和对**Active X**、**Java Script**等的过滤，并逐渐有木马过滤病毒扫除功能。
- 利用防火墙建立专用网**(VPN**将在较长一段时间内，仍然是用户使用的主流**)**。**IP**加密需求越来越强，安全协议的开发是一大热点。
- 单向防火墙**(**又叫网络二极管**)**将作为一种产品门类而出现。
- 对网络攻击的检测和各地告警将成为防火墙的重要功能。
- 安全管理工具不断完善，特别是可疑活动的日志分析工具等将成为防火墙产品中的一部分。

习题与思考题

1. 简述防火墙工作原理。
2. 防火墙的体系结构有哪些？
3. 一个好的防火墙应具备哪些功能？
4. 简述包过滤的基本特点及其工作原理。
5. 简述代理服务器的作用，常用代理服务的软件有哪些？