第5章 防火墙技术

中国科学技术大学

曾凡平 billzeng@ustc.edu.cn

主要内容

5.1 防火墙概述

5.2 防火墙的功能和分类

- 5.2.1 防火墙的功能　5.2.2 防火墙的分类

5.3 包过滤防火墙

- 5.3.1 静态包过滤防火墙　　5.3.2 动态包过滤防火墙

5.5 防火墙的典型部署

5.6 Linux防火墙的配置

5.7 防火墙的发展趋势

5.8 防火墙的设计

5.9 防火墙的指标与选择

5.1 防火墙概述

- **防火墙的定义：**防火墙是位于两个(或多个)网络之间执行访问控制的软件和硬件系统，它根据访问控制规则对进出网络的数据流进行过滤。

- 防火墙的概念起源于中世纪的城堡防卫系统，那时人们为了保护城堡的安全，在城堡的周围挖一条护城河，每一个进入城堡的人都要经过吊桥，并且还要接受城门守卫的检查。人们借鉴了这种防护思想，设计了一种网络安全防护系统，这种系统被称为**防火墙(FireWall)**。

Internet的普及和发展
促使了防火墙技术的出现和发展

- 在Internet并不流行的1980年代，企业网络大多是封闭的局域网，与外部网络在物理上是隔开的，网络上的计算机均由内部员工使用，内部网络被认为是安全的和可信的。
- 到了Internet逐步普及的时候，为了提高资源共享的效率和更好地获取信息，企业网络就通过路由器连接到了Internet。

- Internet中存在各种各样的恶意用户（比如黑客），是不可信的、不安全的。

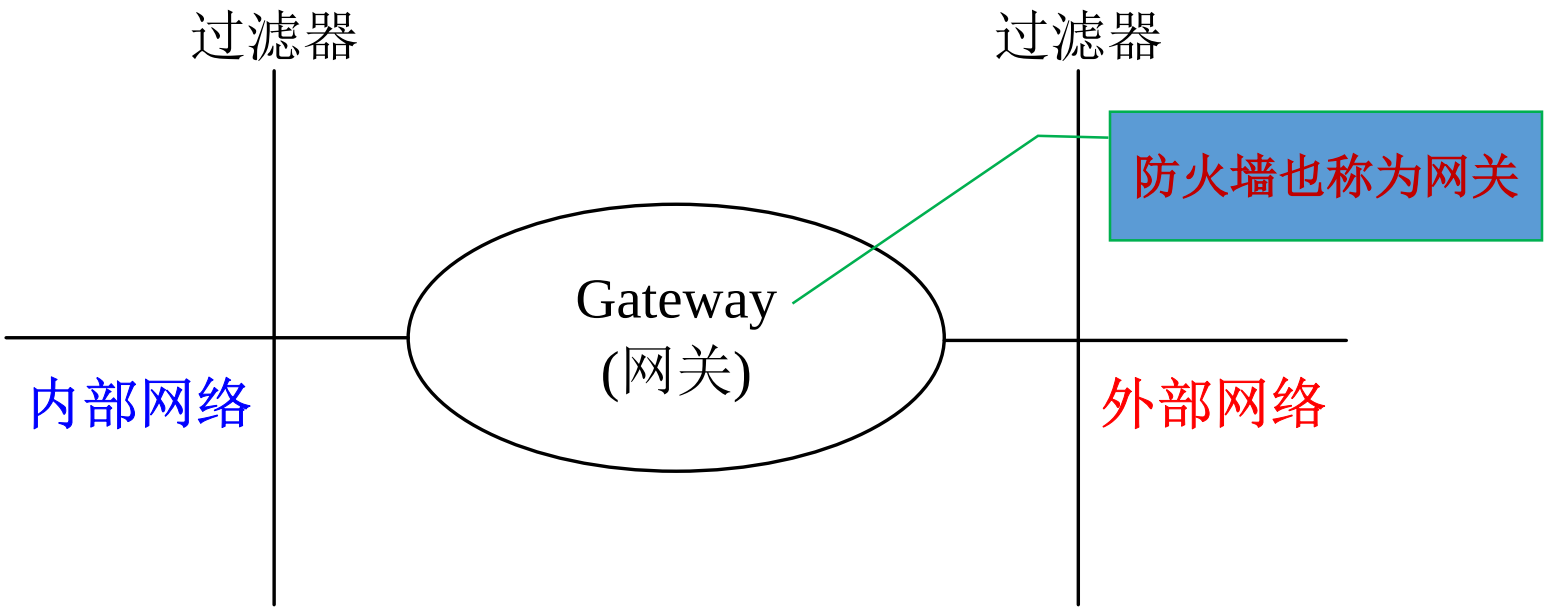
防火墙：过滤和监视内外网络之间的数据流

- 如果不限制Internet上的用户对企业内部网络的访问，将带来巨大的安全风险；同时，内部网络中的用户如果不受限制地访问外部网络（比如恶意网站），也可能会引入木马、病毒等安全风险。

- 为了抵挡内部和外部网络的各种风险，可以在内部网络与外部网络之间设置一道屏障，用于**过滤和监视内外网络之间的数据流**，这种屏障就是防火墙。

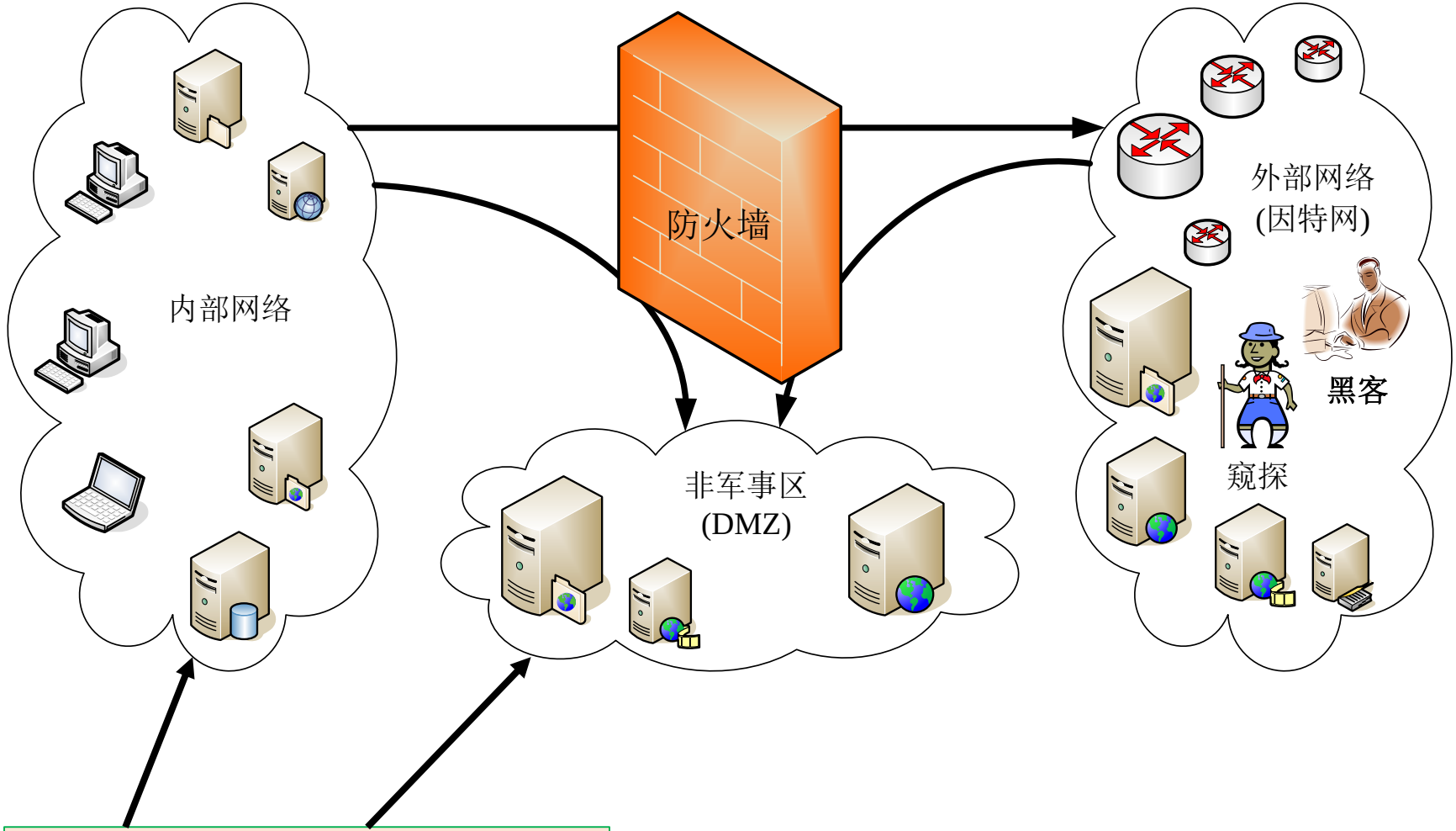
所有数据流都要经过防火墙

- 防火墙位于不同网络或网络安全域之间，从一个网络到另一个网络的所有数据流都要经过防火墙。如果我们根据企业的安全策略设置合适的访问控制规则，就可以**允许**、**拒绝或丢弃**数据流，从而可以在一定程度上保护内部网络的安全。



对数据流的处理方式：允许、拒绝和丢弃

- 根据安全策略，防火墙对数据流的处理方式有三种：
  - ①允许数据流通过；
  - ②拒绝数据流通过：通知发送方
  - ③将这些数据流丢弃：不通知发送方
- 当数据流被**拒绝**时，防火墙要向发送者回复一条消息，提示发送者该数据流已被拒绝。
- 当数据流被**丢弃**时，防火墙不会对这些数据包进行任何处理，也不会向发送者发送任何提示信息。丢弃数据包的做法加长了网络扫描所花费的时间，发送者只能等待回应直至通信超时。



企业网络包括**内部网络**和DMZ（**非军事区**）

图5-1 防火墙示意图

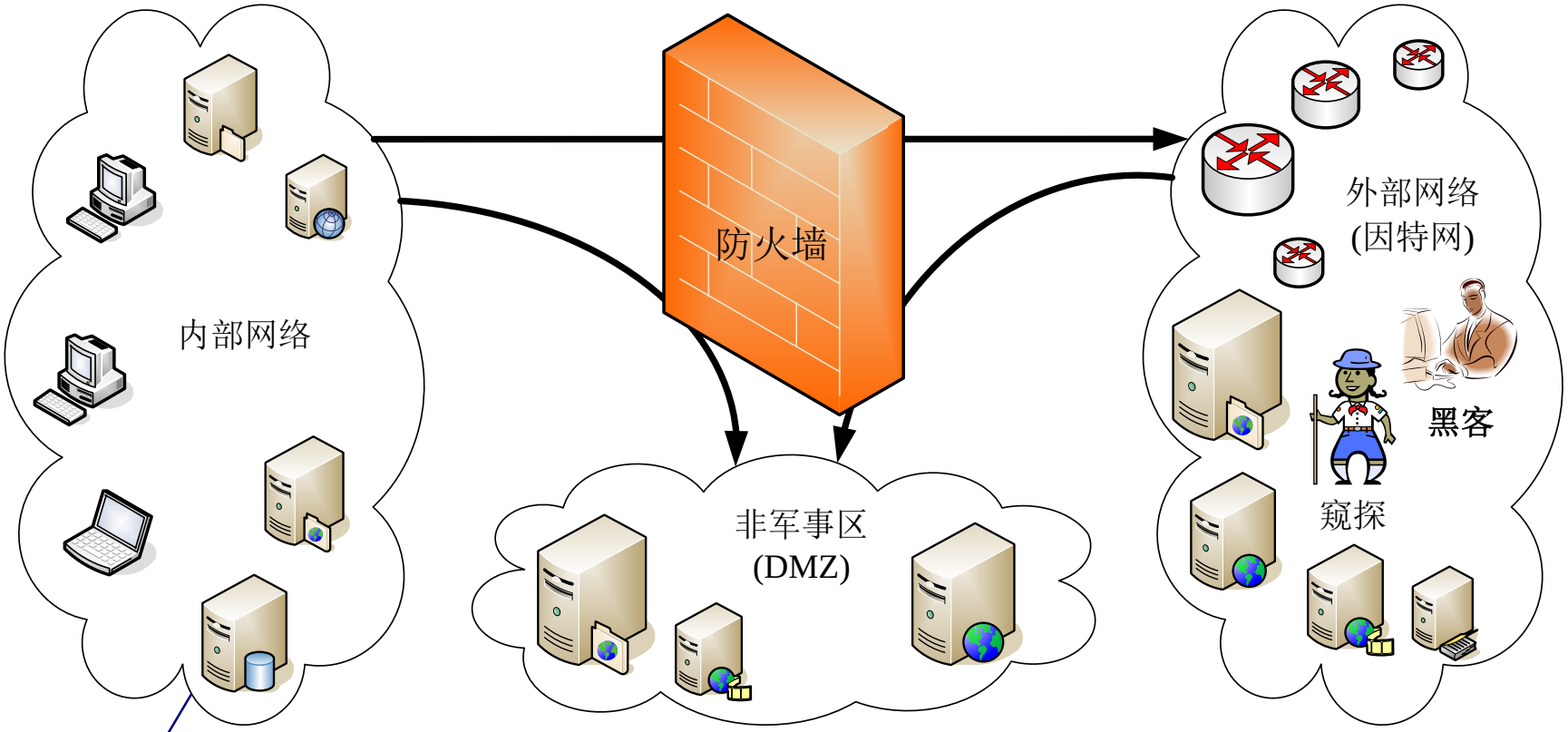
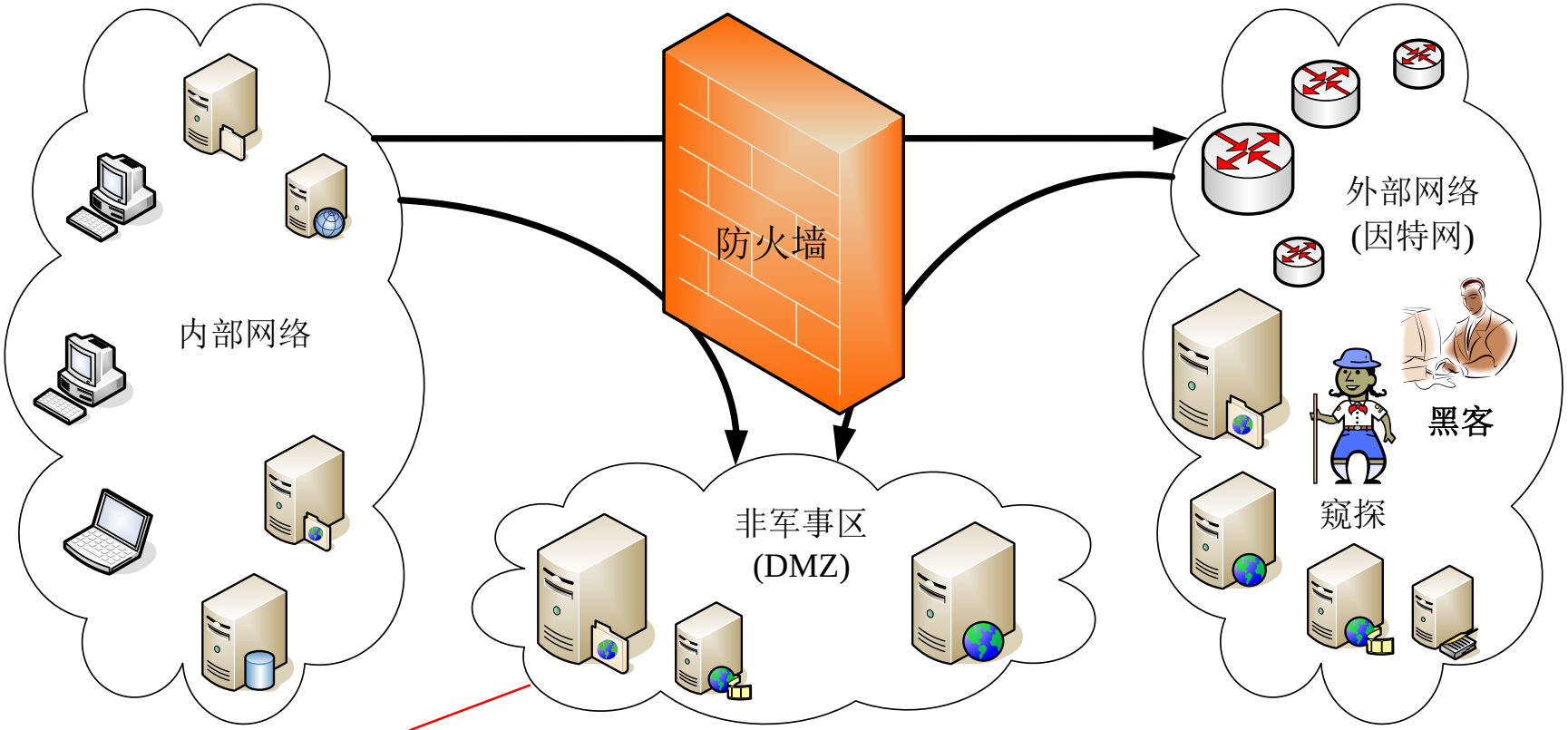


图5-1 防火墙示意图

内部网络一般是企业内部的局域网，其安全性是致关重要的，必须禁止外部网络的访问，同时只开放有限的对外部网络的访问权。



为了配置和管理方便，通常将内部网中需要向外部提供服务的服务器设置在单独的网段，这个网段被称为非军事区(DMZ)。DMZ是防火墙的重要概念，在实际应用中经常用到。DMZ是周边网络，位于内部网之外，使用与内部网不同的网络号连接到防火墙，其中部署了Web服务器、ftp服务器、通信服务器等对外提供公共服务。DMZ隔离内外网络，并为内外网之间的通信起到缓冲作用。

- DMZ通过防火墙对内部网络和外部网络开放不同的访问权，以保证企业网络安全可靠地运行。
- 防火墙本质上就是一种能够限制网络访问的设备或软件。它可以是一个硬件的“盒子”，也可以是计算机和网络设备中的一个“软件”模块。许多网络设备均含有简单的防火墙功能，如路由器、调制解调器、无线基站、IP交换机等。

- 现代操作系统中也含有软件防火墙：Windows系统和Linux系统均自带了软件防火墙，可以通过策略(或规则)定制相关的功能。

防火墙技术已经非常成熟

- 防火墙是最早出现的Internet安全防护产品，其技术已经非常成熟，有众多的厂商生产和销售专业的防火墙。目前，市场上销售的防火墙的质量都非常高，其区别主要在于防火墙的吞吐量以及售后服务的保障。对个人用户而言，一般用操作系统自带的防护墙或启用杀毒软件中的防火墙（如金山毒霸、腾讯电脑管家、360安全软件等均提供了个人防火墙功能）。
- 对于企业用户而言，购买专业的防火墙是比较好的选择。购买专业防火墙会有很多好处：第一，防火墙厂商提供的接口会更多、更全；第二，过滤深度可以定制，甚至可以达到应用级的深度过滤；第三，可以获得厂商提供的技术支持服务。

5.2.1 防火墙的功能

- 防火墙是执行访问控制策略的系统，它通过监测和控制网络之间的信息交换和访问行为来实现对网络安全的有效管理。
- 防火墙遵循的是一种允许或禁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。因此，对数据和访问的控制、对网络活动的记录，是防火墙的基本功能。
- 具体地说，防火墙具有以下几个方面的功能：

(1) 访问控制功能

- 这是防火墙最基本和最重要的功能，通过禁止或允许特定用户访问特定资源，保护内部网络的资源和数据。

- 防火墙配置在企业网络与Internet的连接处，是任何信息进出网络的必经之处，它保护的是整个企业网络，因此可以集中执行强制性的信息安全策略，可以根据安全策略的要求对网络数据进行不同深度的监测，允许或禁止数据的出入。这种**集中的强制访问控制简化了管理，提高了效率**。

(2) 内容控制功能

- 防火墙可以防止非法用户进入内部网络，也能禁止内网用户访问外网的不安全服务（比如恶意网站），这样就能有效地防止邮件炸弹、蠕虫病毒、宏病毒等攻击。
- 如果发现某个服务存在安全漏洞，则可以用防火墙关闭相应的服务端口号，从而禁用了不安全的服务。
- 如果在应用层进行过滤，还可以过滤不良信息传入内网，比如，过滤色情暴力信息的传播。

(3) 日志功能

- 记录通过防火墙的信息内容和活动。
- 防火墙系统能够对所有的访问进行日志记录。日志是对一些可能的攻击进行分析和防范的十分重要的信息。另外，防火墙系统也能够对正常的网络使用情况做出统计。通过对统计结果的分析，可以使网络资源得到更好的使用。

告警和集中管理功能

(4) 对网络攻击的检测和告警

- 当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。

(5) 集中管理功能

- 针对不同的网络情况和安全需要，指定不同的安全策略，在防火墙上集中实施，使用中还可能根据情况改变安全策略。防火墙应该是易于集中管理的，便于管理员方便地实施安全策略。

其他功能

- 此外，防火墙还可能具有流量控制、网络地址转换(NAT)、虚拟专用网(VPN)等功能。

- 防火墙正在成为控制对网络系统访问的非常流行的方法。事实上，在Internet上的Web网站中，超过1／3的Web网站都是由某种形式的防火墙加以保护，这是对黑客防范最严，安全性较强的一种方式，任何关键性的服务器，都建议放在防火墙之后。

5.2.2 防火墙的分类

(1) 按防火墙的使用范围分类

- 可分为**个人防火墙**和**网络防火墙**。

- 个人防火墙保护一台计算机，一般提供简单的包过滤功能，通常内置在操作系统或随杀毒软件提供。
- 网络防火墙保护一个网络中的所有主机，布置在内网与外网的连接处。

(2) 根据防火墙在网络协议栈中的过滤层次分类

- 这是主流的分类方法。根据防火墙在网络协议栈中的过滤层次不同，可以把防火墙分为三类：
  - 包过滤防火墙
  - 电路级网关防火墙
  - 应用级网关防火墙(代理防火墙)

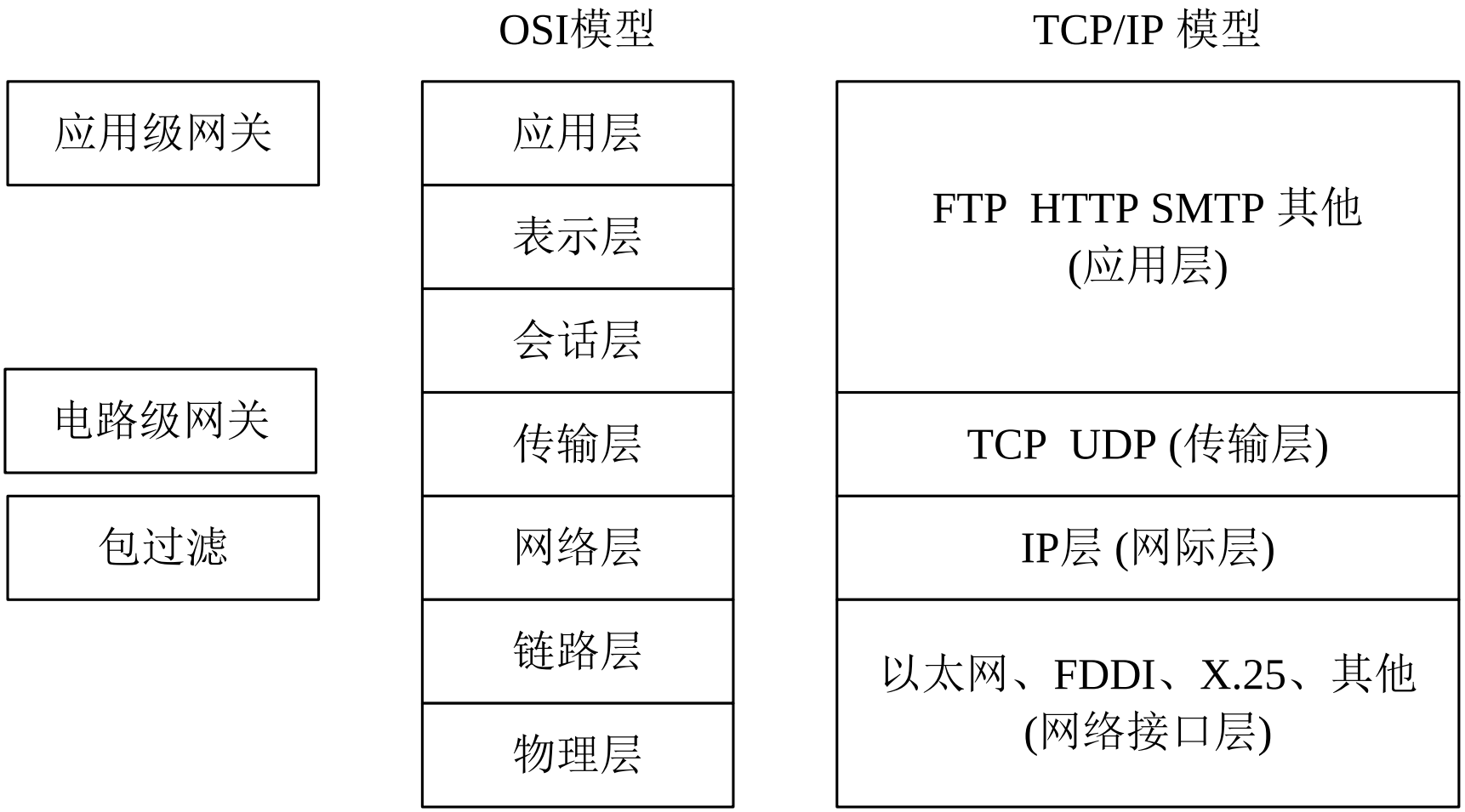

OSI模型
TCP/IP 模型
应用级网关
电路级网关
包过滤
应用层
表示层
会话层
传输层
网络层
链路层
物理层
FTP HTTP SMTP 其他
(应用层)
TCP UDP (传输层)
IP层 (网际层)
以太网、FDDI、X.25、其他
(网络接口层)

图5 - 2 防火墙示意图

- **包过滤防火墙**主要根据网络层的信息进行控制，**电路级网关防火墙**主要根据传输层的协议信息进行过滤，**应用级网关防火墙**主要根据应用层协议的信息进行过滤。
- 一般而言，防火墙的工作层次越高，则其能获得的信息就越丰富，提供的安全保护等级也就越高，但是由于其需要分析更多的内容，其速度也就越慢。
- 由于电路级网关防火墙很少单独存在，一般作为代理防火墙的一个模块存在，因此我们只介绍包过滤防火墙和代理防火墙。

(3) 按防火墙的发展沿革(历史)分类

- 第一代防火墙
- 第二代防火墙
- 第三代防火墙
- 第四代防火墙
- 第五代防火墙

第一、二代防火墙

- **第一代防火墙始于1985年前后**，它几乎与路由器同时出现，由Cisco的IOS软件公司研制。这一代防火墙称为**包过滤防火墙**。直到1988年，DEC公司的Jeff Mogul根据自己的研究，才发表了第一篇描述有关包过滤防火墙过滤过程的文章。

- **在1989—1990年前后**，AT&T贝尔实验室的Dave Presotto和Howard Tfickey率先提出了**基于电路中继的第二代防火墙**结构，此类防火墙被称为电路级网关防火墙。但是，他们既没有发表描述这一结构的任何文章，也没有发布基于这一结构的任何产品。

第三代防火墙

- **第三代防火墙结构是在20世纪80年代末和20世纪90年代初**由Purdue University的Gene Spafford，AT&T贝尔实验室的Bill Cheswick和Marcus Ranum分别研究和开发。这一代防火墙被称为**应用级网关防火墙**。

- 在1991年，Ranum的文章引起了人们的广泛关注。此类防火墙采用了在堡垒主机运行代理服务的结构。根据这一研究成果，DEC公司推出了第一个商用产品SEAL。

第四代防火墙

- 大约在1991年，Bill Cheswick和Steve Bellovin开始了对**动态包过滤防火墙**的研究。

- 1992年，在USC信息科学学院工作的Bob Braden和Annette DeSchon开始研究用于“Visas”系统的动态包过滤防火墙，后来它演变为目前的**状态检测防火墙**。

- **1994年**，以色列的Check Point Software公司推出了基于**第四代结构**的第一个商用产品。

第五代防火墙

- 关于第五代防火墙，目前尚未有统一的说法，关键在于目前还没有出现获得广泛认可的新技术。

① 一种观点认为，在1996年由Global Internet Software Group公司的首席科学家Scott Wiegel开始启动的**内核代理结构**(Kernel Proxy Architecture)研究计划**属于第五代防火墙**；

② 还有一种观点认为，在1998年由NAI公司推出的**自适应代理**(Adaptive Proxy)技术给代理类型的防火墙赋予了全新的意义，可以称之为**第五代防火墙**。

5.3 包过滤防火墙

- 包过滤防火墙也称为分组过滤防火墙，是最早出现的防火墙，几乎与路由器同时出现，最初是作为路由器的一个过滤模块来实现的。目前的路由器均集成了简单的包过滤功能。由于可以直接使用路由器软件的过滤功能，无须购买专门的设备，因此可以减少投资。

- **包过滤工作在IP层（网络层）**，也用到了传输层的协议端口号等信息。根据访问控制策略的实现机制的不同，又可以分为**静态包过滤**和**动态包过滤**。

- 网络管理员首先根据企业的**安全策略**定义一组**访问控制规则**，然后防火墙在内存中建立一张与访问控制规则对应的**访问控制列表**。对于每个数据包，如果在访问控制列表中有对应的项，则防火墙按规则的要求允许或拒绝数据包的通过，否则应用**“默认规则”**。
- **“默认规则”**有两种，即**“默认丢弃”**或**“默然允许”**。“默认丢弃”是指如果没有对应的规则，则丢弃数据包；“默认允许”是指如果没有对应的规则，则允许数据包通过。显然，“默认丢弃”更有利于企业网的安全防护。

5.3.1 静态包过滤防火墙

- 静态包过滤防火墙的访问控制列表在运行过程中是不会动态变化的，其过滤规则只利用了IP与TCP/UDP报头中的几个字段，只适合一些对安全要求不高的场合，其访问控制规则的配置比较复杂，对于某些需要打开动态端口的应用，很难定义合适的规则。

静态包过滤防火墙对数据包的处理过程如下：

- (1)接收每个到达的数据包。
- (2)对数据包按序匹配过滤规则，对数据包的IP头和传输字段内容进行检查。如果数据包的头信息与一组规则匹配，则根据该规则确定是转发还是丢弃该数据包。
- (3)如果没有规则与数据包头信息匹配，则对数据包施加默认规则。
- 静态包过滤防火墙仅检查当前的数据包，是否允许通过的**判决仅依赖于当前数据包**的内容，检查的内容包括如下几部分：**①源IP地址；②目的IP地址；③应用或协议号；④源端口号；⑤目的端口号**。因此，对数据包的检测是**孤立的、无状态**的。

静态包过滤防火墙的优点

- **(1)对网络性能的影响较小：**由于包过滤防火墙只是简单地根据地址、协议和端口进行访问控制，因此对网络性能的影响比较小。只有当访问控制规则比较多时，才会感觉到性能的下降。
- **(2)成本较低：**路由器通常集成了简单包过滤的功能，基本上不再需要单独的防火墙设备实现静态包过滤功能，因此从成本方面考虑，包过滤的成本非常低。
- **(3)对用户透明：**数据包过滤是在IP层实现的，它工作在网络层和传输层，与应用层无关；Internet用户根本感觉不到它的存在，不用改动客户机和主机上的任何应用程序；包过滤不要求任何自定义软件或者客户机配置；它也不要求用户经过任何特殊的训练或者操作，使用起来很方便。

静态包过滤防火墙的缺点

- **(1) 安全性较低。**由于包过滤防火墙仅工作于网络层，其自身的结构设计决定了它不能对数据包进行更高层的分析和过滤。因此，包过滤防火墙仅提供较低水平的安全性。
- **(2) 缺少状态感知能力。**一些需要动态分配端口的服务需要防火墙打开许多端口，这就增大了网络的安全风险，从而导致网络整体安全性不高。
- **(3) 容易遭受IP欺骗攻击。**由于简单的包过滤功能没有对协议的细节进行分析，因此有可能遭受IP欺骗攻击。
- **(4) 创建访问控制规则比较困难。**要创建严密有效的访问控制规则，管理员需要认真地分析和研究一个组织机构的安全策略，同时必须严格区分访问控制规则的先后次序，这对于新手而言是一个比较困难的问题。

5.3.2 动态包过滤防火墙

- 由于静态包过滤防火墙的访问控制表是固定的，这就很难应用于需要打开动态端口的一些网络服务，比如ftp协议。由于事先无法知道需要打开哪些端口，这种情况下如果必须采用原始的静态包过滤技术的话就要将所有可能用到的端口都打开，即只能过滤IP地址，无法限制端口，这就带来了风险。

- 解决这一问题的方法是使用动态包过滤技术，它可以根据网络当前的状态检查数据包，即根据当前所交换的信息动态调整过滤规则表。

- 动态包过滤技术能够通过检查**应用程序信息**以及连接信息，来判断某个端口是否需要临时打开。当传输结束时，端口又可以马上恢复为关闭状态。这样的话就可以保证主机的端口没有一个是永远打开的，那么外界也就无从连接主机。
- 只有在主机主动地跟外界连接时，其他的机器才可以跟它连接。

动态包过滤防火墙的工作原理

1. 首先检测每一个有效连接的状态，并根据这些信息决定网络的数据包是否能够通过防火墙。
2. 然后通过从协议栈低层截取数据包，并将当前数据包及其状态信息和其前一时刻的数据包及其状态信息进行比较，从而得到该数据包的控制信息。
3. 接下来，**动态包过滤**模块就开始截获、分析并处理所有试图通过防火墙的数据包，以保证网络的高度安全和数据完整。由于网络和各种应用的通信状态可以被动态存储到动态状态表中，结合预定义好的规则，动态包过滤模块就可以识别出不同应用的服务类型，同时还可以通过以前的通信及其他应用程序分析出目前这个连接的状态信息。

4. 再接下来检验IP 地址、端口以及其他需要的信息以便决定该通信包是否满足安全策略。
5. 最后它还把会相关的状态和状态之间的关联信息存储到动态连接表中以随时更新其中的数据。通过这些数据，动态包过滤模块就可以观测到后继的通信信息。

- 由于动态包过滤技术对应用程序透明，不需要针对每个服务设置单独的代理，从而使其具有更高的安全性和更好的伸缩性及扩展性。

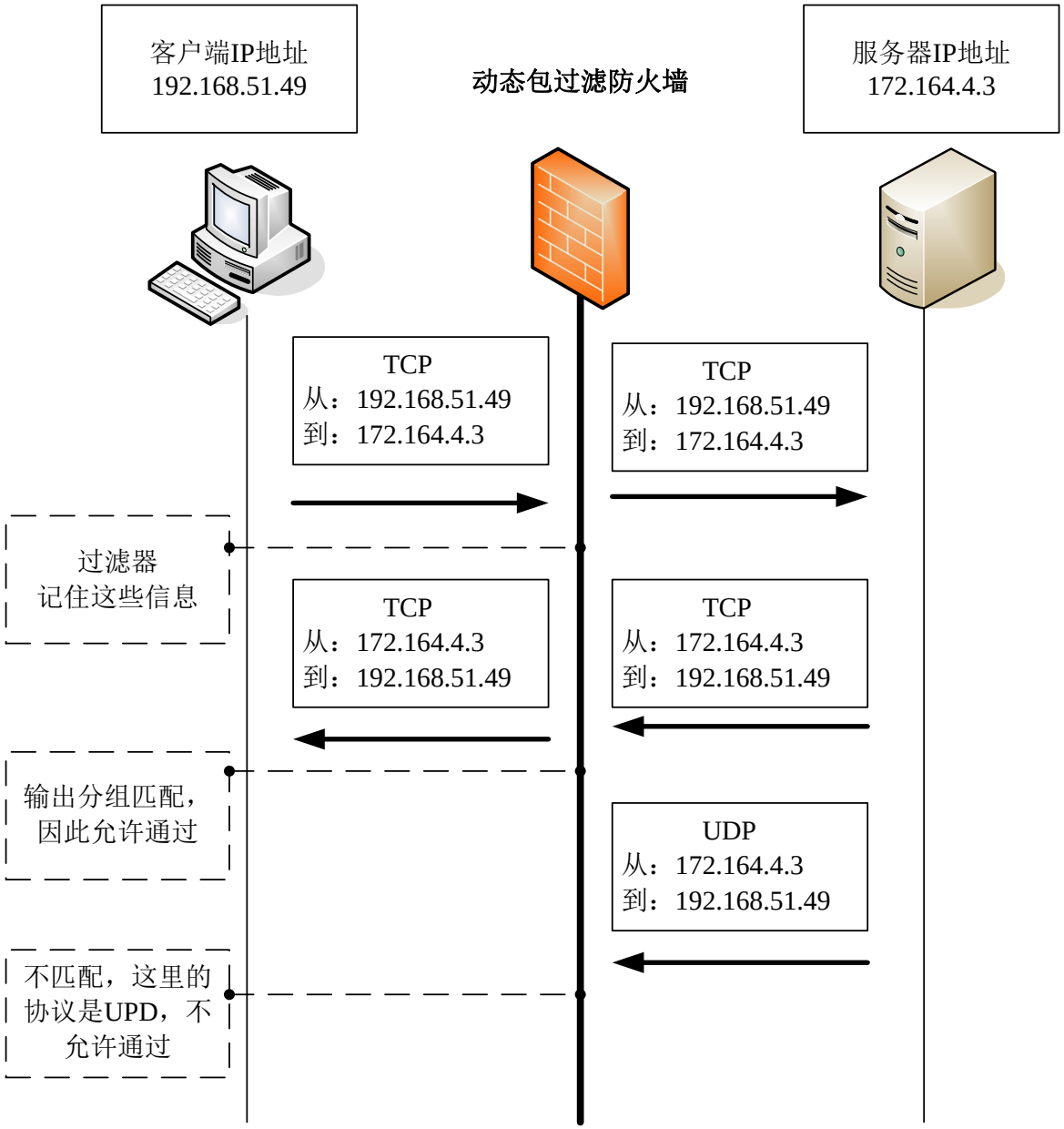


图5 - 4 动态包过滤的工作过程

动态包过滤防火墙的优点

(1) 高安全性

- 动态包过滤防火墙的安全性优于静态包过滤防火墙。由于具有“状态感知”能力，所以防火墙可以区分连接的发起方与接收方，也可以通过检查数据包的状态阻断一些攻击行为。与此同时，对于不确定端口的协议数据包，防火墙也可以通过分析打开相应的端口。防火墙所具备的这些能力使其安全性有了很大的提升。

(2) 高性能

- 动态包过滤防火墙的“状态感知”能力也使其性能得到了显著提高。由于防火墙在连接建立后保存了连接状态，当后续数据包通过防火墙时，不再需要烦琐的规则匹配过程，这就减少了访问控制规则数量增加对防火墙性能造成的影响，因此其性能比静态包过滤防火墙好很多。

(3) 伸缩性和易扩展性

- 动态包过滤防火墙不像代理防火墙那样，每一个应用对应一个服务程序，这样所能提供的服务是有限的，而且当增加一个新的服务时，必须为新的服务开发相应的服务程序，这样系统的可伸缩性和可扩展性降低。
- 动态包过滤防火墙不区分每个具体的应用，只是根据从数据包中提取的信息、对应的安全策略及过滤规则处理数据包，当有一个新的应用时，它能动态产生新的应用的规则，而不用另外写代码，因此，具有很好的伸缩性和扩展性。

(4) 针对性

- 它能对特定类型的数据包中的数据进行检测。
- 由于在常用协议中存在着大量众所周知的漏洞，其中一部分漏洞来源于一些可知的命令和请求等，因而利用状态包检查防火墙的检测特性使得它能够通过检测数据包中的数据来判断是否是非法访问命令。

(5) 应用范围广

- 动态包过滤防火墙不仅支持基于TCP的应用，而且支持基于无连接协议的应用，如RPC和基于UDP的应用（DNS、WAIS和NFS等）。对于无连接的协议，**静态包过滤**防火墙和**应用代理**对此类应用要么不支持，要么开放一个大范围的UDP端口，这样暴露了内部网，降低了安全性。
- 动态包过滤防火墙对基于UDP应用安全的实现是通过在UDP通信之上保持一个虚拟连接来实现的。防火墙保存通过网关的每一个连接的状态信息，允许穿过防火墙的UDP请求包被记录，当UDP包在相反方向上通过时，依据连接状态表确定该UDP包是否是被授权的，若已被授权，则通过，否则拒绝。如果在指定的一段时间响应数据包没有到达，则连接超时，该连接被阻塞，这样所有的攻击都被阻塞，UDP应用安全实现了。**动态包过滤防火墙也支持RPC**，因为对于RPC服务来说，其端口号是不固定的，因此，简单的跟踪端口号是不能实现该种服务的安全的，动态包过滤防火墙通过动态端口映射图记录端口号，为验证该连接还保存连接状态与程序号等，通过动态端口映射图来实现此类应用的安全。

动态包过滤防火墙的缺点

(1) 由于没有对数据包的净荷部分进行过滤，因此仍然只具有较低的安全性。

(2) 容易遭受IP地址欺骗攻击。

(3) 难于创建规则，管理员创建规则时必须要考虑规则的先后次序。

(4) 如果动态包过滤防火墙在连接建立时没有遵循RFC建议的三步握手协议，就会引入额外的风险。

- 如果防火墙在连接建立时仅使用两次握手，很可能导致防火墙在DoS/DDoS攻击时因耗尽所有资源而停止响应。

5.4 应用级网关防火墙

- 应用级网关防火墙也称为代理防火墙，是实现内容过滤的主要技术之一。应用级网关防火墙针对每一种应用软件，均由对应的代理软件对其网络载荷进行分析和过滤。因此，代理是特定于应用的。

- 目前常用的有http代理、ftp代理、email代理等。

- 应用代理包括客户代理和服务器代理，如图5-5所示。

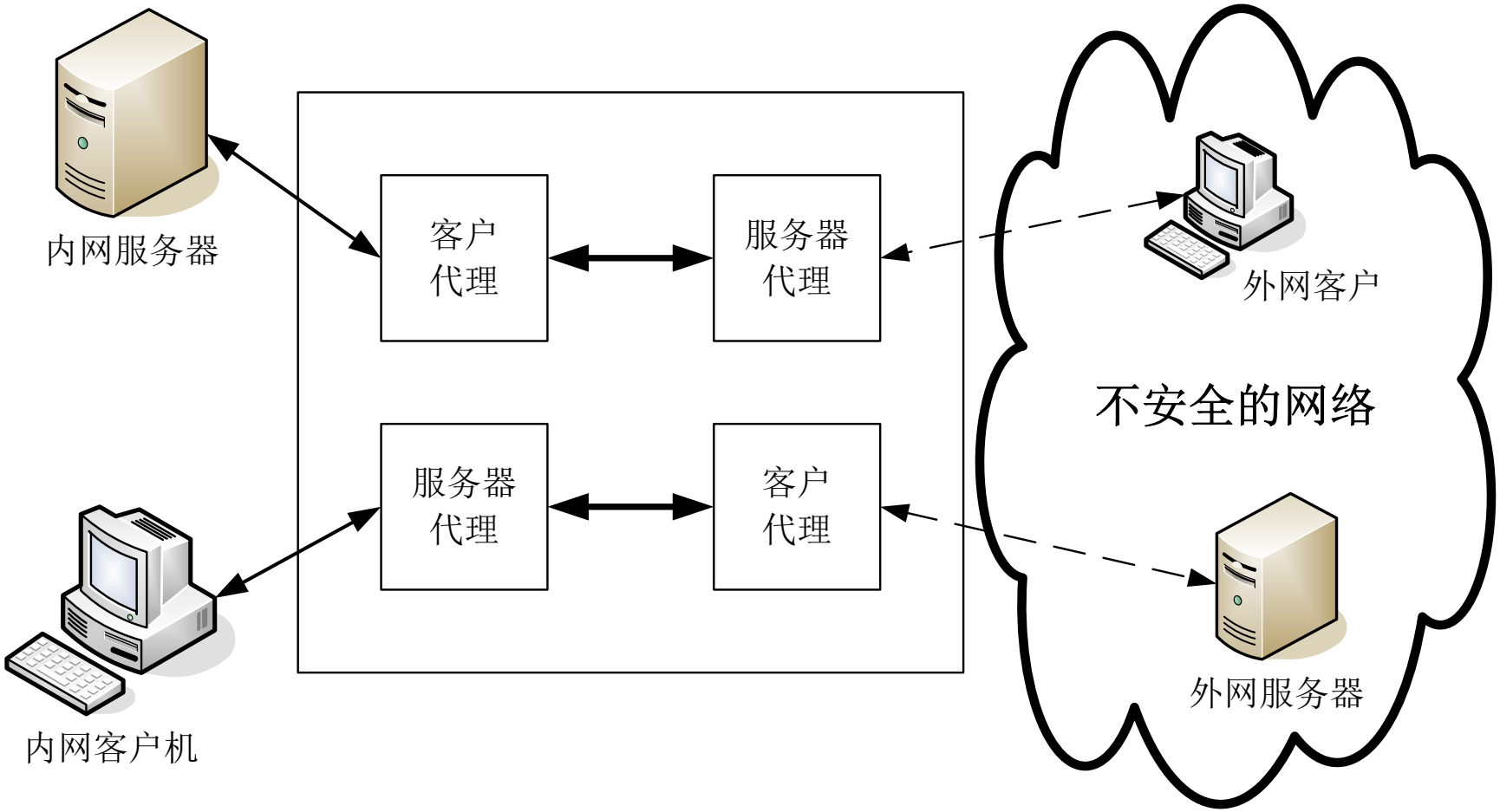


图5 - 5 代理防火墙的逻辑结构

- 应用级网关截获进出网络的数据包，对数据包的内容进行检查，如果符合所制定的安全规则，则允许数据通过；否则根据安全策略的要求进行处理。比如：可以直接丢弃数据包，也可以删除数据包的不良内容，将改变的数据包传递到通信的另一端。
- **由于应用代理避免了服务器和客户机之间的直接连接，其安全性是最高的。**虽然应用级网关防火墙具有很高的安全性，但是它有一个固有的缺点，那就是**缺乏透明性，即你所看到的未必是原来的信息**。此外，缺乏对新应用、新协议的支持也成了制约应用级网关发展的主要障碍。由于各种应用软件的升级很快，应用代理要跟上应用软件的升级速度是很难的，这就制约了代理防火墙的广泛使用。

应用级网关的主要优点

(1) 在已有的安全模型中安全性较高。由于工作于应用层，因此应用级网关防火墙的安全性取决于厂商的设计方案。应用级网关防火墙完全可以对服务(如HTTP、FTP等)的命令字过滤，也可以实现内容过滤，甚至可以进行病毒的过滤。

(2) 具有强大的认证功能。由于应用级网关在应用层实现认证，因此它可以实现的认证方式比电路级网关要丰富得多。

(3) 具有超强的日志功能。包过滤防火墙的日志仅能记录时间、地址、协议、端口，而应用级网关的日志要明确得多。例如，应用级网关可以记录用户通过HTTP访问了哪些网站页面、通过FTP上传或下载了什么文件、通过SMTP给谁发送了邮件，甚至邮件的主题、附件等信息，都可以作为日志的内容。

(4) 应用级网关防火墙的规则配置比较简单。由于应用代理必须针对不同的协议实现过滤，所以管理员在配置应用级网关时关注的重点就是应用服务，而不必像配置包过滤防火墙一样还要考虑规则顺序的问题。

应用级网关的主要缺点

(1) 灵活性很差，对每一种应用都需要设置一个代理。由此导致的问题很明显，每当出现一种新的应用时，必须编写新的代理程序。

- 由于目前的网络应用呈多样化趋势，这显然是一个致命的缺陷。
- 在实际工作中，应用级网关防火墙中集成了电路级网关或包过滤防火墙，以满足人们对灵活性的需求。

(2) 配置烦琐，增加了管理员的工作量。由于各种应用代理的设置方法不同，因此对于不是很精通计算机网络的用户而言，难度可想而知。对于网络管理员来说，当网络规模达到一定程度的时候，其工作量很大。

(3) 性能不高，有可能成为网络的瓶颈。虽然目前的CPU处理速度还是保持以摩尔定律的速度增长，但是周边系统的处理性能(如磁盘访问性能等)远远落后于运算能力的提高，很多时候系统的瓶颈根本不在于处理器的性能。目前，应用级网关的性能依然远远无法满足大型网络的需求，一旦超负荷，就有可能发生停机，从而导致整个网络中断。

5.5 防火墙的典型部署

- 防火墙有三种典型的部署模式：屏蔽主机模式、双宿/多宿主机模式和屏蔽子网模式。在这些部署中，堡垒主机都承担了重要的作用。

- **堡垒主机(Bastion Host)**是一种配置了较为全面的安全防范措施的网络上的计算机，它为网络间的通信提供了一个阻塞点。通常堡垒主机可以用作应用级和电路级网关的平台，是一个组织机构网络安全的中心主机。其特征如下：

- (1)堡垒主机硬件平台运行较为安全的操作系统，成为可信任的系统。
- (2)只有网络管理员认为必要的服务才会安装在堡垒主机上。这些服务包含了代理服务，如Telnet，DNS，FTP，SMTP以及用户认证等。
- (3)当允许一个用户访问代理服务时，堡垒主机可能会要求进行额外认证。另外，每一个代理服务都可能需要相应的鉴别机制(Authentication)。
- (4)每一个代理都只能支持标准应用服务命令集中的一个子集。
- (5)每一个代理只允许访问指定主机的通信。这意味着每一个代理通过对所用的网络流量、每一个连接及其持续时间记录日志，保留了详细的审计信息。审计日志对检测和终止入侵者极为重要。

- (6)每一个代理模块都是一个为网络安全设计的一个很小的软件包。
- (7)代理之间相互独立。
- (8)代理通常无需进行磁盘访问，不需要读取初始配置文件。这使得入侵者很难在主机上安装Trojan horse、sniffers或其他危险的文件。
- (9)堡垒主机是一个组织机构网络安全的中心主机。
- 因为堡垒主机对网络安全至关重要，对它必须进行完善的防御。这就是说，堡垒主机是由网络管理员严密监视的。堡垒主机软件和系统的安全情况应该定期地进行审查。对访问记录应进行查看，以防潜在的安全漏洞和对堡垒主机的试探性攻击。

5.5.1 屏蔽主机模式防火墙

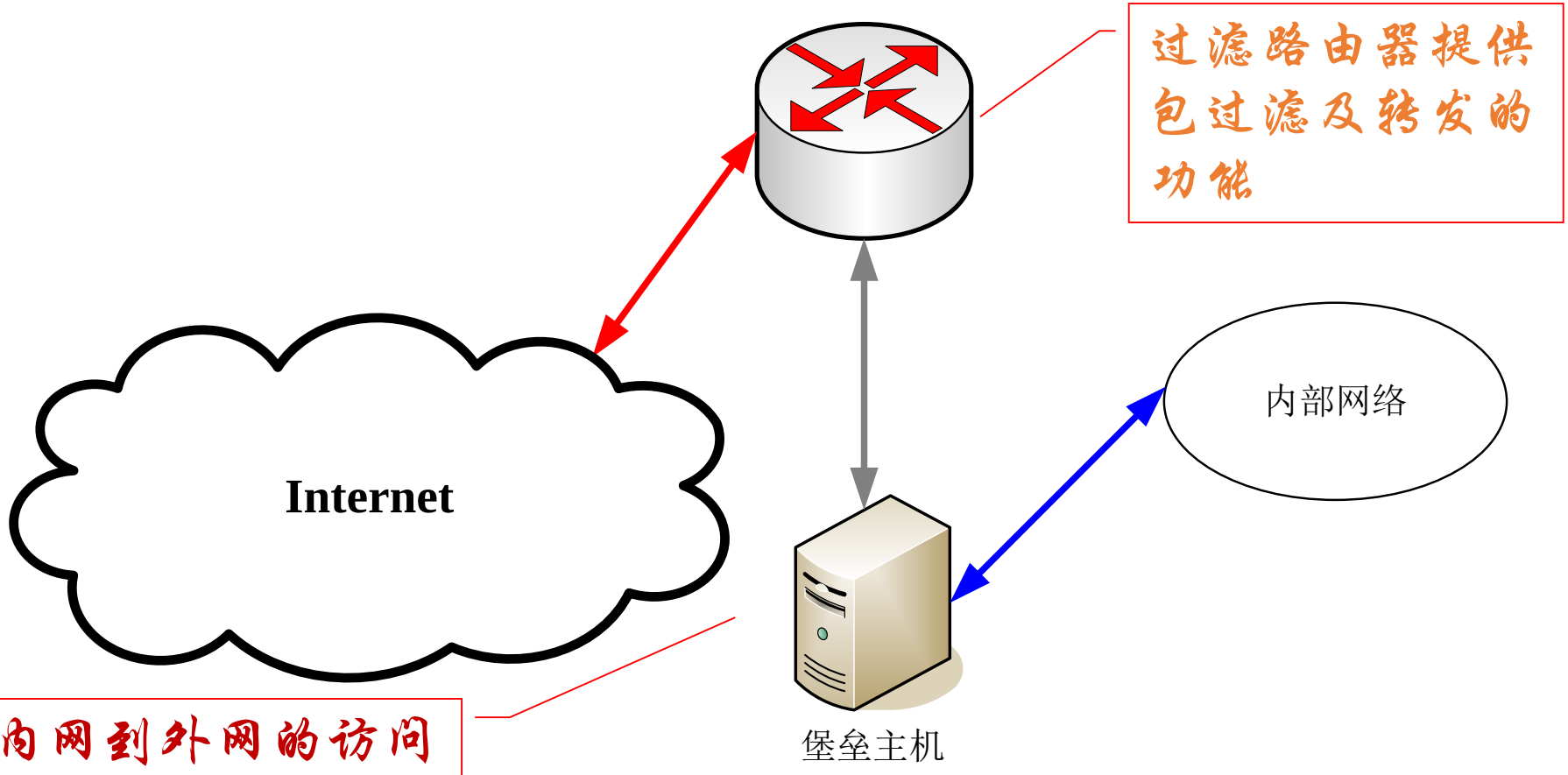


图5－6 屏蔽主机模式防火墙

- 屏蔽主机模式防火墙的实质就是包过滤和代理服务功能的结合。**堡垒主机**担任了身份鉴别和代理服务的功能。这样的配置比单独使用包过滤防火墙或应用层防火墙更加安全。
- 首先，这种配置能够实现数据包级过滤和应用级过滤，在定义安全策略时有相当的灵活性。其次，在入侵者威胁到内部网络的安全以前，必须能够“穿透”两个独立的系统（包过滤路由器和堡垒主机）。同时，这种配置在对Internet进行直接访问时，有更大的灵活性。例如，内部网络中有一个公共信息服务器，如Web服务器（在高级别的安全中是不需要的），这时，可以配置路由器允许网络流量在信息服务器和Internet之间传输。然而，单宿主机模式存在一个缺陷：一旦过滤路由器遭到破坏，堡垒主机就可能被越过，使得内部网络完全暴露。

5.5.2 双宿/多宿主机模式防火墙

- 双宿/多宿主机模式防火墙(Dual-homed/Multi-Homed Firewall)，又称为双宿/多宿网关防火墙。它是一种拥有两个或多个连接到不同网络上的网络接口的防火墙。通常用一台装有两块或多块网卡的**堡垒主机**作为防火墙，每块网卡各自与受保护网络和外部网连接。
- 其体系结构如图5-7所示。

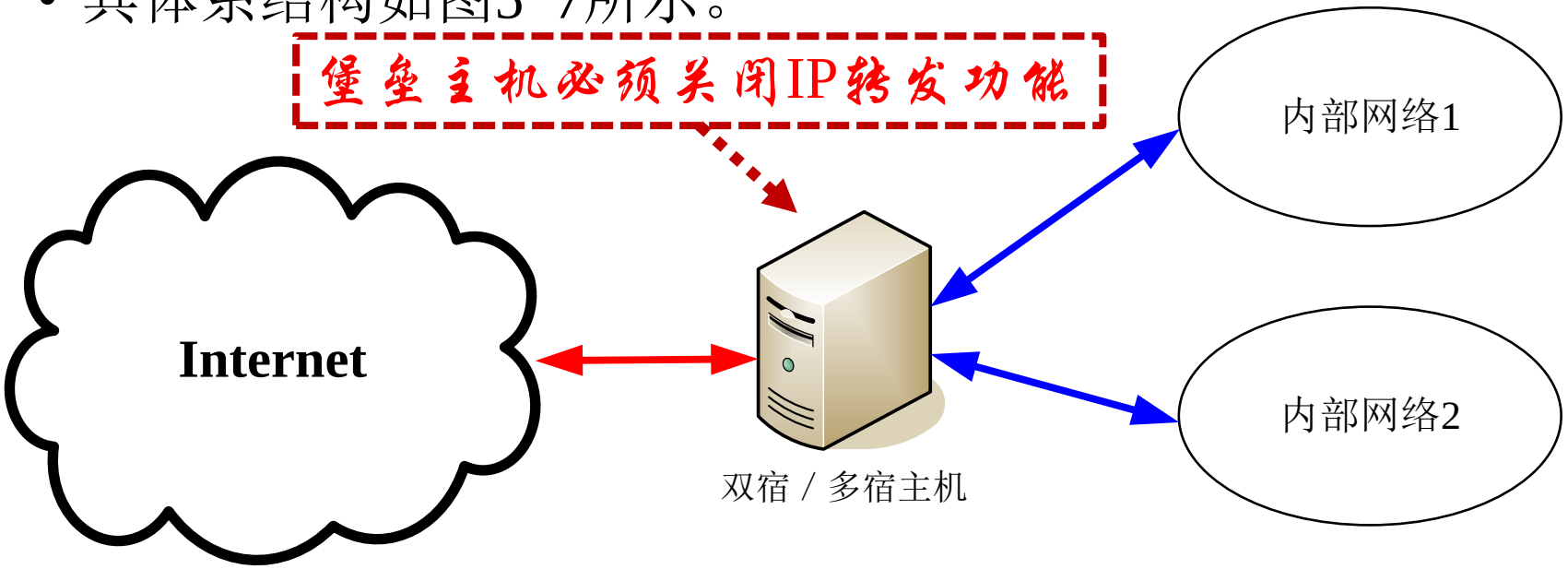


图5 - 7 双宿/多宿主机模式防火墙

- 该模式下，**堡垒主机必须关闭了IP转发功能**，其网关功能是通过提供代理服务而不是通过IP转发来实现的。显然只有特定类型的协议请求才能被代理服务处理。于是，网关采用了“缺省拒绝”策略以得到很高的安全性。
- 这种体系结构的防火墙简单明了，易于实现，成本低，能够为内外网提供检测、认证、日志等功能。
- 但是这种结构也存在弱点，一旦黑客侵入堡垒主机并打开其IP转发功能，则任何网上用户均可随意访问内部网络。因此，双宿/多宿网关防火墙对不可信任的外部主机的访问必须进行严格的身份验证。

5.5.3 屏蔽子网模式防火墙

- 与前面几种配置模式相比，屏蔽子网模式防火墙(Screened Subnet Mode Firewall)是最为安全的一种配置模式。
- 它采用了两个包过滤路由器：一个位于堡垒主机和外部网络(Internet)之间；另一个位于堡垒主机和内部网络之间。该配置模式在内部网与外部网络之间建立了一个被隔离的子网，其体系结构如图5-8所示。

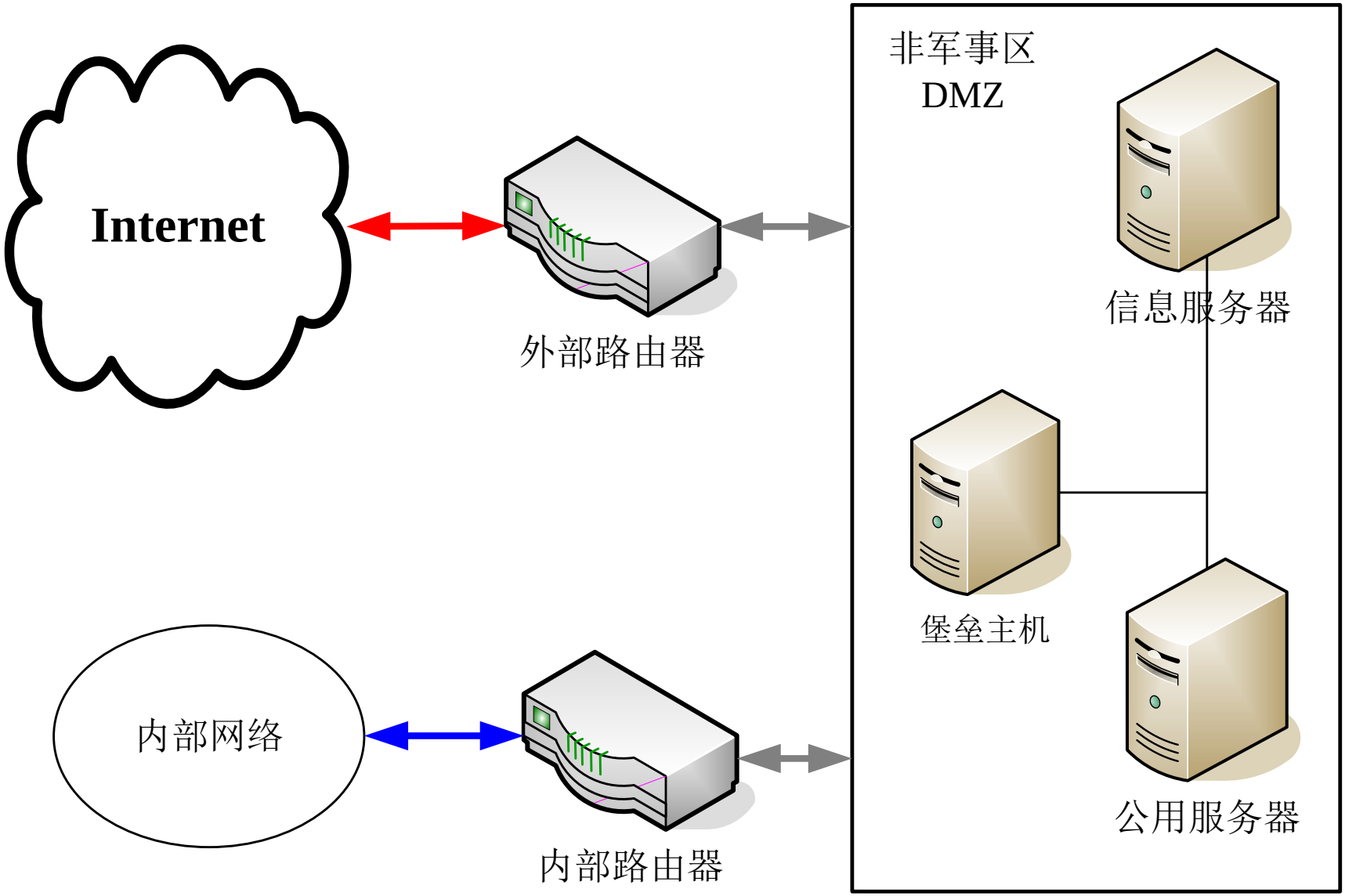


图5 - 8 屏蔽子网模式防火墙

- 周边防御网络是位于内部网络与外部网络之间的一个安全子网，分别和内外两个路由器相连。这个子网被定义为**“非军事区”(demilitarized zone)**网络，这一网络所受到的威胁不会影响到内部网络，网络管理员可以将堡垒主机、Web服务器、E-mail服务器等公用服务器放在非军事区网络中，将重要的数据放在内部网服务器上。内部网络和外部网络均可访问屏蔽予网，但禁止它们穿过屏蔽子网通信。在这一配置中，内网增加了一台内部包过滤路由器，该路由器与外部路由器的过滤规则完全不同，它只允许源于堡垒主机的数据包进入。
- 这种防火墙安全性好，但成本高。即使外部路由器和堡垒主机被入侵者控制，内部网络仍受到内部包过滤路由器的保护。

5.6 Linux防火墙的配置

- Linux系统免费且源代码开源，在构建企业级的信息系统中得到了极为广泛的应用，尤其是服务器大多使用Linux系统。
- Linux系统下的防火墙最初用iptables进行配置，比较复杂，对管理员的要求较高。为了提高防火墙的易用性，使之适合普通用户，近年来Linux系统的各个发行版均提供了优秀的配置工具，以简化防火墙的配置。
- 本节以Fedora linux和Ubuntu linux为例进行简要说明。

Fedora Linux系统提供了图形界面下的配置软件。
在终端下输入**firewall-config**则将打开配置界面。对于要开放的端口或服务标记“√”，如图5-9所示：

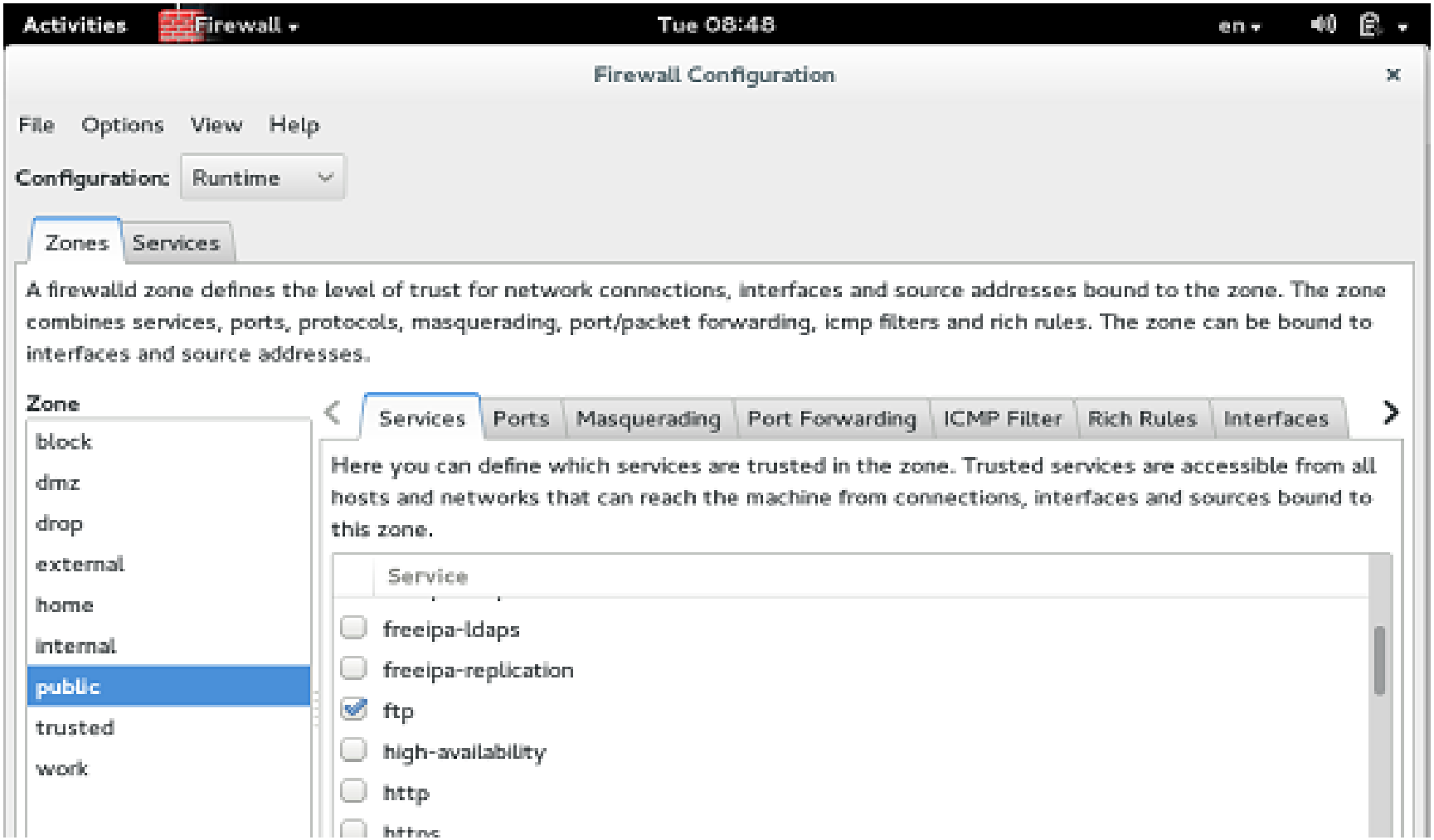


图5 - 9 Fedora Linux防火墙配置工具

Ubuntu linux系统的防火墙

- Ubuntu系统用ufw命令配置防火墙
  - 查看帮助：ufw -?
  - 启动|关闭防火墙：ufw enable | disable
  - 开放(关闭)某个端口： ufw allow (deny) port
  - 开放(关闭)某个端口： ufw allow (deny) 50050
  - 开放(关闭)某服务： ufw allow (deny) service
  - 开放(关闭)某个端口： ufw allow (deny) ssh

5.7 防火墙发展动态和趋势

- 尽管防火墙有许多防护功能，但由于互连网的开放性，它也有一些力不能及的地方，表现在：
  - **防火墙不能防范不经由防火墙的攻击。**例如，如果允许从受保护网内部不受限制的向外拨号，一些用户可以形成与Internet的直接的SLIP或PPP连接。从而绕过防火墙，造成一个潜在的后门攻击渠道。
  - **防火墙目前还不能防止感染了病毒的软件或文件的传输。**这只能在每台主机上装反病毒软件。

- **防火墙不能防止数据驱动式攻击。**当有些表面看来无害的数据被邮寄或复制到Internet主机上并被执行而发起攻击时，就会发生数据驱动攻击。例如，一种数据驱动的攻击可以使一台主机修改与安全有关的文件，从而使入侵者下一次更容易入侵该系统。
- 另外，**防火墙还存在着安装、管理、配置复杂的缺点**，在高流量的网络中，防火墙还容易成为网络的瓶颈。

- 针对存在的问题，防火墙产品正向以下趋势发展:

(1) 优良的性能

- 新一代防火墙系统不仅应该能更好地保护防火墙后面内部网络的安全，而且应该具有更为优良的整体性能。传统的代理型防火墙虽然可以提供较高级别的安全保护，但是同时它也成为限制网络带宽的瓶颈，这极大地制约了在网络中的实际应用。数据通过率是表示防火墙性能的参数，由于不同防火墙的不同功能具有不同的工作量和系统资源要求，因此数据在通过防火墙时会产生延时。自然，数据通过率越高，防火墙性能越好。现在大多数的防火墙产品都支持NAT功能，它可以让受防火墙保护的一边的IP地址不至于暴露在没有保护的另一边，但启用NAT后，势必会对防火墙系统性能有所影响，目前如何尽量减少这种影响也成为防火墙产品的卖点之一。另外防火墙系统中集成的VPN解决方案必须是真正的线速运行，否则将成为网络通信的瓶颈。
- 特别是采用复杂的加密算法时，防火墙性能尤为重要。总之，未来的防火墙系统将会把**高速的性能和最大限度的安全性**有机结合在一起，有效地消除制约传统防火墙的性能瓶颈。

(2) 可扩展的结构和功能

- 对于一个好的防火墙系统而言，它的**规模和功能应该能适应内部网络的规模和安全策略的变化**。选择哪种防火墙，除了应考虑它基本性能外，毫无疑问，还应考虑用户的实际需求与未来网络的升级。
- 因此，防火墙除了具有保护网络安全的基本功能外，还提供对VPN的支持，同时还应该具有可扩展的内驻应用层代理。除了支持常见的网络服务以外，还应该能够按照用户的需求提供相应的代理服务，例如，如果用户需要NNTP（网络消息传输协议）、X-Window、HTTP和Gopher等服务，防火墙就应该包含相应的代理服务程序。
- 未来的防火墙系统应是一个可随意伸缩的模块化解决方案，从最为基本的包过滤器到带加密功能的VPN型包过滤器，直至一个独立的应用网关，使用户有充分的余地构建自己所需要的防火墙体系。

(3) 简化的安装与管理

- 防火墙的确可以帮助管理员加强内部网的安全性。**一个不具体实施任何安全策略的防火墙无异于高级摆设。**防火墙产品配置和管理的难易程度是防火墙能否达到目的的主要考虑因素之一。实践证明，许多防火墙产品并未起到预期作用的一个不容忽视的原因在于配置和实现上的错误。同时，若防火墙的管理过于困难，则可能会造成设置上的错误，反而不能达到其功能。
- 因此**未来的防火墙将具有非常易于进行配置的图形用户界面**，NT防火墙市场的发展证明了这种趋势。Windows NT提供了一种易于安装和易于管理的基础。尽管基于NT的防火墙通常落后于基于Unix的防火墙，但NT平台的简单性以及它方便的可用性大大推动了基于NT的防火墙的销售。 同时，像DNS这类一直难于与防火墙恰当使用的关键应用程序正引起有意简化操作的厂商越来越多的关注。

(4) 主动过滤

- Internet数据流的简化和优化使网络管理员将注意力集中在这一点上：在Web数据流进入他们的网络之前需要在数据流上完成更多的事务。
- 防火墙开发商通过建立功能更强大的Web代理对这种需要做出了回应。例如，许多防火墙具有内置病毒和内容扫描功能或允许用户将病毒与内容扫描程序进行集成。今天，许多防火墙都包括对过滤产品的支持，并可以与第三方过滤服务连接，这些服务提供了不受欢迎的Internet站点的分类清单。防火墙还在它们的Web代理中包括时间限制功能，允许非工作时间的冲浪和登录，并提供冲浪活动的报告。

(5) 防病毒与防黑客

- 尽管防火墙在防止**不良分子**进入上发挥了很好的作用，但TCP／IP 协议套件中存在的脆弱性使Internet对拒绝服务攻击敞开了大门。在拒绝服务攻击中，攻击者试图使企业Internet服务器饱和或使与它连接的系统崩溃，使Internet无法供企业使用。
- 防火墙市场已经对此做出了反应。 虽然没有防火墙可以防止所有的拒绝服务攻击，但防火墙厂商一直在尽其可能阻止拒绝服务攻击。像对付序列号预测和IP欺骗这类简单攻击，这些年来已经成为了防火墙工具箱的一部分。像“SYN泛滥”这类更复杂的拒绝服务攻击需要厂商部署更先进的检测和避免方案来对付。

(6) 发展联动技术

- **联动即通过一种组合的方式，将不同的技术与防火墙技术进行整合**，在提高防火墙自身功能和性能的同时，由其他技术完成防火墙所缺乏的功能，以适应网络安全整体化、立体化的要求。
- 防火墙与防病毒产品联动，可以在网关处查杀病毒，将病毒的发作限制在最小的可能。
- 防火墙与认证系统联动，可以在制定安全策略时使用强度更大、安全性更高的认证体系。
- 防火墙与入侵检测系统联动，可以对网络进行动静结合的保护 。
- 防火墙与日志分析系统联动。

发展趋势总结

- 综上所述，未来防火墙技术会全面考虑网络的安全、操作系统的安全、应用程序的安全、用户的安全、数据的安全，五者综合应用。

- 此外，网络的防火墙产品还将把网络前沿技术，如Web页面超高速缓存、虚拟网络和带宽管理、与其它安全技术联动等与其自身结合起来。

5.8 防火墙的设计

- 现代的操作系统已经集成了基本的防火墙架构，用户只要在相关的架构上加入自定义的软件模块，就可以实现高强度的防火墙功能。

- Windows环境下要学习设备驱动程序的设计，对网络协议要有所了解。

- Linux环境下要学习内核可加载模块LKM的设计，要了解netfilter/iptables架构。

(1) 防火墙设计--Windows

OSI 7层模型	Windows 结构	开发环境
应用层(Application Layer)	应用程序(EXE)	...
表示层(Presentation Layer)	Winsock API (DLL)	winsock
会话层(Session Layer)	SPI (DLL) 用户级	winsock SPI
传输层(Transport Layer)	TDI (vxd, sys) 内核级	DDK、 WDK
网络层(Network Layer)	NDIS (vxd, sys)	
数据链路层(Data Link Layer)	网卡驱动程序(vxd, sys)	...
物理层(Physical Layer)	网卡	...

Windows 防火墙设计

- 用户级
  - SPI接口，Windows2000包过滤接口
- 内核级
  - TDI过滤驱动程序，NDIS中间层过滤驱动程序，NDIS过滤钩子驱动程序。
- 参考安全焦点上的三篇参考文章
  - http://www.xfocus.net/articles/200706/922.html
  - http://www.xfocus.net/articles/200304/518.html
  - http://www.xfocus.net/articles/200307/568.html

(2) Linux 防火墙设计

- Linux kernel 集成了过滤系统
  - 2.0 ipfwadm
  - 2.2 ipchains
  - 2.4以上内核：netfilter/iptables
- 目前大多数Linux下的防火墙都是在这些过滤系统之上开发设计的。**通过LKM注册钩子函数，实现对数据的检测，从而实现自定义的防火墙。**
- 商用防火墙大多在netfilter/iptables上开发。

5.9 防火墙的指标与选择
5.9.1 防火墙的功能指标

防火墙主要功能类指标项

防火墙功能指标项	功能描述
网络接口	防火墙所能够能保护的网络类型，如以太网、快速以太网、千兆以太网ATM、令牌环网、FDDI等
协议支持	支持的非IP协议：除IP协议外，又支持AppleTalk、DECNnetIPX及NETBEUT等协议 建立VPN通道的协议：IPSec、PPTP、专用协议等
加密支持	防火墙所能够支持的加密算法，如DES、RC4、IDEA、AES以及国内专用的加密算法
认证支持	防火墙所能够支持的认证类型，如Radius、Kerberos、TACACS/TACACS+口令方式，数字证书等
访问控制	防火墙所能够支持的访问控制方式，如包过滤、时间、代理等
安全功能	防火墙能够支持的安全方式，如病毒扫描、内容过滤等
管理功能	防火墙所能够支持的管理方式，如基于SNMP管理、管理的通信协议、带宽管理、负载平衡管理、失效管理、用户权限管理、远程管理和本地管理
审计和报表	防火墙所能够支持的设计方式和分析处理审计数据表达形式，如远程审计、本地审计，

5.7.2 防火墙的性能指标

- 许多用户仅仅通过并发连接数等指标考察产品性能，这其实是一个很大的误区。吞吐且、丢包率和延迟等才是衡量一个防火墙的性能的重要指标参数。一个千兆防火墙系统要达到千兆线速，必须在全速处理最小的数据封包(64B)转发时可达到100%吞吐率。
- 然而根据赛迪评测对国内外千兆防火墙的评测数据可以看到，还没有一款千兆防火墙在64B帧长时可以达到100%的吞吐率（最好的测试数据仅为72.58%）。
- 用户在考察防火墙设备的性能指标时，必须从吞吐量、延迟、丢包率等数据确定产品的性能。换句话说，无论防火墙是采用何种方式实现的，上述指标仍然是判断防火墙性能的主要依据。

(1) 吞吐量

- 吞吐量是防火墙的第一个重要指标，该参数体现了防火墙转发数据包的能力。它决定了每秒钟可以通过防火墙的最大数据流量，**通常用防火墙在不丢包的条件下每秒转发包的最大数目来表示。**该参数以位每秒(bit/s)或包每秒(p/s)为单位。以位每秒为单位时，数值从几十兆到几百兆不等，千兆防火墙可以达到几个吉的性能。

(2) 时延

- 时延参数是防火墙的一个重要指标，直接体现了在系统重载的情况下，防火墙是否会成为网络访问服务的瓶颈。
- 时延指的是在防火墙最大吞吐量的情况下，数据包从到达防火墙到被防火墙转发出去的时间间隔。时延参数的测定值应与防火墙标称的值相一致。

(3) 丢包率

- 丢包率参数指明防火墙在不同负载的情况下，因为来不及处理而不得不丢弃的数据包占收到的数据包总数的比例，这是一个服务的可用性参数。
- 不同的负载量通常在最小值到防火墙的线速值（防火墙的最高数据包转发速率）之间变化，一般选择线速的10%作为负载增量的步长。

(4) 背对背

- **防火墙的背对背指的是从空闲状态开始，以达到传输介质最小合法间隔极限的传输速率发送相当数量的固定长度的帧，当出现第一个帧丢失时，发送的帧数。**
- 背对背包的技术指标结果能体现出被测防火墙的缓冲容量，网络上经常有一些应用会产生大量的突发数据包（如NFS、备份、路由更新等），而且这样的数据包的丢失可能会产生更多的数据包，强大缓冲能力可以减小这种突发对网络造成的影响，因此，背对背指标体现防火墙的数据缓存能力，**描述了网络设备承受突发数据的能力**，即对突发数据的缓冲能力。

(5) 最大位转发率

- 防火墙的位转发率指在特定负载下每秒钟防火墙将允许的数据流转发至正确的目的接口的位数。最大位转发率指在不同的负载下反复测量得出的位转发率数值中的最大值。

(6) 最大并发连接数

- 最大并发连接数指穿越防火墙的主机之间或主机与防火墙之间能同时建立的最大连接数。这项性能可以反映一定流量下防火墙所能顺利建立和保持的并发连接数及一定数量的连接情况下防火墙的吞吐量变化。
- 并发连接数主要反映了防火墙建立和维持TCP连接的性能，同时也能通过并发连接数的大小体现防火墙对来自于客户端的TCP连接请求的响应能力。

(7) 最大并发连接建立速率

- 在此项测试中，分别测试防火墙的每秒所能建立起的TCP/HTTP连接数及防火墙所能保持的最大TCP/HTTP连接数。测试在一条安全规则下打开和关闭NAT(静态)对TCP连接的新建能力和保持能力。

(8) 有效通过率

- 根据RFC 2647对防火墙测试的规范中定义的一个重要的指标：good put（防火墙的真实有效通过率）。由于防火墙在使用过程中，总会有数据包的丢失和重发，因此，简单测试防火墙的通过率是片面的，good put从应用层测试防火墙的真实有效的传输数据包速率。简单地说，就是防火墙端口的总转发数据量(bit/s)减去丢失的和重发的数据量(bit/s)。

(9) 其他性能指标

- 防火墙的其他性能指还包括最大策略数、平均无故障间隔时间、支持的最大用户数等。

5.9.3 防火墙的选择原则

- 一般认为，没有一个防火墙的设计能够适用于所有的环境，所以应根据网站的特点来选择合适的防火墙。选购防火墙时应考虑以下几个因素。

(1) 防火墙的安全性

- 安全性是评价防火墙好坏最重要的因素，这是因为购买防火墙的主要目的就是为了保护网络免受攻击。但是，由于安全性不太直观、不便于估计，因此，往往被用户所忽视。对于安全性的评估，需要配合使用一些攻击手段进行。

(2) 防火墙的高效性

- 用户的需求是选购何种性能防火墙的决定因素。用户安全策略中往往还可能会考虑一些特殊功能要求，但并不是每一个防火墙都会提供这些特殊功能的。用户常见的需求可能包括以下几种。
  1)双重域名服务DNS
  2)虚拟专用网络VPN
  3)网络地址转换功能NAT
  4)杀毒功能
  5)特殊控制需求

(3) 防火墙的适用性

- 适用性是指量力而行。
- 防火墙也有高低端之分，配置不同，价格不同，性能也不同。同时，防火墙有许多种形式，有的以软件形式运行在普通计算机之上，有的以硬件形式单独实现，也有的以固件形式设计在路由器之中。因此，在购买防火墙之前，用户必须了解各种形式防火墙的原理、工作方式和不同的特点，才能评估它是否能够真正满足自己的需要。

(4) 防火墙的可管理性

- 防火墙的管理是对安全性的一个补充。目前，有些防火墙的管理配置需要有很深的网络和安全方面的专业知识，很多防火墙被攻破不是因为程序编码的问题，而是管理和配置错误导致的。
- 对管理的评估，应从以下几个方面进行考虑。

  1)远程管理

  2)界面简单、直观

  3)有用的日志文件

(5) 完善的售后服务

- 只要有新的产品出现，就会有人研究新的破解方法，所以好的防火墙产品应拥有完善且及时的售后服务体系。
- 防火墙和相应的操作系统应该用补丁程序进行升级，而且升级必须定期进行。

作业和上机实践

✓作业

- 做实验并写实验报告：用netfilter/iptables可以将Linux虚拟机配置成路由器，这需要用iptables命令将网卡设置成转发(NAT)模式。将一台ubuntu虚拟机设置成路由器(配置2个虚拟网卡，内网和外网)，一台windows虚拟机配置成客户端(内网)，通过路由器访问Internet。

➢上机实践(自己练习)

- 用Windows2003实现包过滤防火墙
- 用Windows2003实现路由器的地址转换(NAT)