黑客防线 2004

精华奉献本（防册）

《黑客防线》编辑部　编

150个全程攻防录像演示
助您成为高手

150个黑客高手倾情力作
各有千秋

200篇精心挑选的精彩文
章使您爱不释手

200种攻击防范案例分析
使您一饱眼福

人民邮电出版社
POSTS & TELECOM PRESS

黑客防线 2004

[redacted]

黑客防线 2004

精华奉献本（防册）

《黑客防线》编辑部　编

人民邮电出版社

内容提要

《黑客防线2004精华奉献本》是在《黑客防线》杂志攻、防两册明确定位后推出的第一个精华本，汇总了从《黑客防线》总第25期到总第36期的精华内容，并且增加新的专题内容融合而成。全书按照攻防关系分为攻册和防册2本，内容通俗易懂，图文并茂，非常便于读者阅读。在栏目划分上，选取了《黑客防线》最受读者欢迎的15个栏目，特别是漏洞攻击、脚本攻击、黑兵器库和漏洞攻击防范、脚本攻击防范、黑器攻击防范6个栏目一一呼应，攻防分明，非常适合读者学习和研究。

本书附赠2张光盘。光盘内容包括书中涉及到的不便于书面印刷的所有代码和大量流行的经典工具、技术文献、最新补丁，以及150个全程攻防录像演示。

本书适合网络管理人员、网络爱好者和网络安全技术人员阅读。

《黑客防线》总　　编　：孙　彬
《黑客防线》执行主编　：郭聪辉
《黑客防线》编辑策划　：徐生震　吴田锋　彭国军
《黑客防线》技术支持　：hacker@hacker.com.cn
《黑客防线》网　　址　：http://www.hacker.com.cn

黑客防线2004精华奉献本（防册）目录

※ 最新奉献

※ 专题企划

※ 漏洞攻击防范

※ 脚本攻击防范

※ 黑器攻击防范

※ CVC病毒专栏

※ 网管之家

※ 安全方案

本文以现有大中院校的校园网络为基础，提出一种基于双边界路由策略的校园网解决方案。首先介绍的是处于边界处路由器的使用问题，其次是通过访问控制列表解决内部网络的基本安全问题。重点介绍整个园区网络使用有限个数的IP，使内部网络众多用户同各个出口处的网络顺利通信的问题，所使用的技术是网络地址转换和代理服务器，同时分析了二者的区别和优缺点，并给出了二者的具体实现方法。

基于双边界的路由策略

文／丁岚

随着互联网的迅速普及和发展，我国各教育基地和大中专院校基本都已接入Internet，其中网络结构多以双出口或多出口的园区网为主，即内部为校园局域网，边界处使用路由器，一条高速接入CERNET（China Education and Research Network）中国教育和科研网，一条连接到当地的ISP（Internet Service Provider）Internet服务提供商。

基于现在校园网络的规模及以后的网络扩建需求，出口处数据流量会显著的增加，边界处路由器的负荷也会不断加重，如不妥善处理这一问题，必将成为数据传输的瓶颈，网络内部的安全也会受到威胁。为了提高路由器及网络带宽的利用率，增加本地网络的安全性，解决通过边界路由器数据的路径选择问题，网络管理人员就必须针对边界路由器所处的特殊环境而采用更加合理的路由策略以达到这些目的，故此对边界路由器的合理配置和网络的规划成为我们需要解决的首要问题。

一、边界路由器的策略需求规划

1. 路由器的高效利用

（1）边界路由器的所有权属于本地管理部门

图1中的网络环境是，在不设置任何策略的情况下，连接到ISP的其它网络和CERNET网络可以免费使用此路由器BCA相互通信，这样就会占用路由器中CPU对数据的处理进程及现存的网络带宽，本地网络与外部网络的数据通信会受到影响，所以要

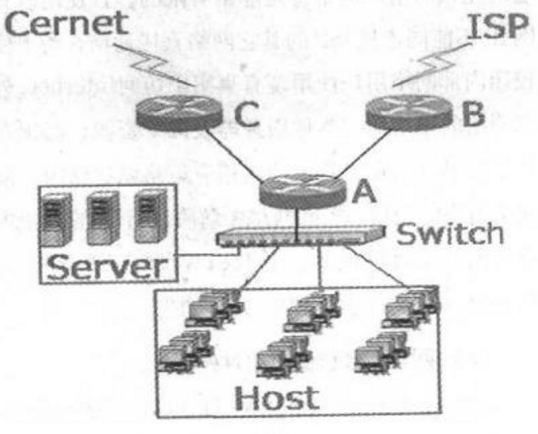

图1

避免边界路由器被网络外部的其它通路使用，就要在边界路由器的相应接口上使用相应的策略以阻止对本地网络无用的数据的流通。

（2）校园内部网络机器会不断增多

边界路由器与外部网络通信的数据报文的数量在不断增大，路由器中CPU的负荷也加重。默认的情况下，路由器采用的都是进程交换的机制。这种情况下，报文的吞吐量取决路由器CPU处理报文的速度。为了提高路由器的性能，和对数据报文的吞吐量，就要使用一种更快速的交换技术——交换缓存技术。

2．路由器的安全策略

随着计算机网络的不断发展，全球信息化已成为人类发展的大趋势。网络安全和信息保密也被提高到至关重要的地位。对于网络内部各种用户(学生，教师，家属等)，服务器（DNS，WWW，E-Mail 等）的敏感数据的计算机网络系统而言，其网上信息的安全和保密尤为重要。因此，上述的网络必须有足够强的安全措施，否则该网络将是个无用网络。

3．数据的路径选择

由于校园网络内部的各种服务器的域名都是向教育网或当地的Internet服务提供商申请的，真实IP由教育网和当地的ISP提供的两部分组成，其数量对庞大的用户群来说是非常有限的。且使用教育网IP不能同连接ISP的其它网络直接通信，为了使校园内部网络用户使用现有真实IP访问Internet，外部网络的用户访问本地服务器及共享资源，必须在处于边界处的路由器上使用相应策略以达到内外部网络用户的通信。实际网络中解决IP不足的方法主要有网络地址转换NAT[Network Address Translator]和使用代理服务器两种方法。

（1）网络地址转换（NAT）

网络地址转换NAT技术是Internet网络应用中一项非常实用的技术。以往主要被应用在并行处理的动态负载均衡以及高可靠性系统的容错备份的实现上。最初，NAT技术是紧随CIDR(Classless Inter Domnin Routing)技术的出现而出现的。二者的主要目的都是为了解决当时传统IP网络地址紧张的问题。CIDR技术通过允许用任意长度子网掩码来划分网段，大大提高了对已注册地址的有效利用率。NAT技术则是一个有惟一出口的桩网络(STUB NETWORK)，通过地址复用来提高对已注册地址的有效利用率，二者都为解决这一问题提供了有效的手段。

事实上，在实现NAT技术之前，已经出现了一种类似的技术——IP地址掩盖(IP Masquerading)。它是在外部网与内部网中某一台主机进行通信时，将内部的这台主机所使用的IP地址映射为网关上的一个特定的TCP端口，使得每次外部网主机访问网关上的某一端口时，其连接中的所有IP包都被转发给这一内部主机。这样整个内部网在与外部进行通信时，再无需任何IP地址了，只需网关对外具有一个IP地址，而不同的内部网主机对外的不同连接使用网关上的不同TCP端口即可。但IP地址掩盖技术并未得到广泛认可，因为它的功能极其有限，当内部网中与外部网联系的主机数量稍有增多时，网关的TCP连接控制部分就难以应付了，而且内部主机对外映射成不同的网关TCP端口。这对于客户端并没有什么关系，但对于提供服务的主机，就会出现服务端口不符合标准TCP规范的问题。而NAT技术的出现弥补了其中的缺陷，迅速地取代了IP地址掩盖技术，在网络中广泛使用。

（2）代理服务器（Application Proxy）

应用代理也叫应用网关，掌握着应用系统中可用作安全决策的全部信息，是内部网与外部网的隔离点，其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。应用网关系统对网络用户运行的各个应用都使用特殊目的代码，需要特殊的应用软件（如现在常用的代理服务软件Netscape Proxy Server和Microsoft Server Proxy）。

实现的方法是在一台主机中插装两块网卡，并

在其上运行代理服务器软件，内部网和外部网之间不能直接进行通信，必须经过此主机，也就是内部网络中的主机与该主机可以通信，Internet网络中的主机也可以与该主机通信，但两个网络中的主机不能直接通信。

使用代理服务器的目的就是通过有限的真实IP使网络内部的所有主机与网络外部通信，内外互相访问只有惟一通道即教育网通道。而对非教育网的访问通过非教育网的代理服务器完成，这些信息可顺利的通过ISP数据网出口进出。

二、路由策略中关键技术

1. 路由

（2）静态路由

静态路由是指由网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在缺省情况下是私有的，不会传递给其他的路由器。当然，网管员也可以通过对路由器进行设置使之成为共享的。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。最常用的静态路由记录就是把包传向连接本地网络路由的主机。静态路由系统无法对网络变化作出响应，所以对今天的大型，动态网络来说并不适用。静态路由也可以手工地被加在系统的路由表中。这些静态记录定义那些不是直接连接，但可以通过另一个称为路由器的主机或设备而到达的目标网络。

静态路由在全局设置模式如下：

ip route 目地子网地址 子网掩码 相邻路由器相邻端口地址或者本地物理端口号

静态路由在缺省路由时配置如下：

ip route 0.0.0 0.0.0.0 相邻路由器的相邻端口地址或本地物理端口号

（2）动态路由

动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际实际情况的变化适时地进行调整。动态路由的原理是路由器向它知道的网络进行广播，其他主机听到这些定期的广播后，就用最新的正确的信息来更新路由表。这样，在路由表中只保留有效的记录。路由器监听，同时也广播。动态路由用于那些不是直接连接但通过路由器可以到达的网络目标。一旦路由表识别到了其他可到达的网络，被识别的路由器可以将包进行转发或投递。目前所使用的绝大多数的主流路由算法都是动态路由算法，可以通过分析接收到的路由更新信息针对变化的网络环境作出相应的调整。动态路由机制的运作依赖路由器的两个基本功能：对路由表的维护；路由器之间适时的路由信息交换。

静态路由和动态路由并不是完全对立的，在适当的环境下，两者可以有机的结合在一起，互为补充。这样，就可以保证所有的信息都能够以某种方式被处理。

2. 访问控制列表

访问控制列表(Access-list)的主要作用是基于已经建立的标准来允许或拒绝报文流，它应用到路由器的某个端口之后才会产生作用。路由器访问控制列表分为静态和动态两种。通常采用静态的控制列表，它能支持多种路由协议，而动态的控制列表只能支持IP协议，但可以提供相对多的安全功能。访问控制列表提供了基于路由器端口的一种基本安全访问技术，可认为是一种内部防火墙技术。访问控制列表可以分以下几类。

（1）静态访问控制列表

◆ **标准访问控制列表**

标准访问控制列表只允许过滤源地址，而且功能十分有限。也就是说，它只能允许具有某个特定IP地址的主机的数据流进出路由器的端口，或者禁止其进出路由器的端口。这样我们就可以控制本地网络外部或内部的计算机进出内部网络，提供对本地内部网络主机的一种简单保护。

◆ 扩展访问控制列表

扩展访问控制列表用于扩展报文过滤能力。一个扩展的访问表允许用户根据如下内容过滤报文：源地址和目的地址、所采用的网络协议，源端口和目的端口以及在特定报文字段中允许进行特殊位比较的各种选项和上层应用数据。扩展访问控制列表对本地网络提供更详细的保护措施。尤其增加了被过滤的协议项，例如IP、TCP、UDP、ICMP等等。

随着网络的发展和用户要求的变化，一些厂商的路由器新增加了一种基于时间的访问列表。通过它，可以根据一天中的不同时间或者根据一星期中的不同日期（当然也可以二者结合起来）控制网络数据包的转发。这种基于时间的访问列表就是在原来的标准访问列表和扩展访问列表中加入有效的时间范围来更合理有效的控制网络。它需要先定义一个时间范围，然后在原来的各种访问列表的基础上应用它。并且，对于编号访问表和名称访问表都适用。

（2）动态访问控制列表

动态访问控制列表是对传统访问表的一种主要功能的增强，它是一种能够创建动态访问表项的访问表。传统的标准访问表和扩展的访问表不能创建动态访问表项，一旦在传统访问表中加入了一个表项，除非手工删除，该表项将一直产生作用。而在动态访问表中，网络管理员可以根据用户认证过程来创建特定的、临时的访问表。

网络管理员可以根据本地网络实际的需要定义自己的规则来进行数据包的路由，使用基于策略路由的办法来解决网络中的一系列问题。在具体的应用中，基于策略的路由有：

◆ 基于源IP地址的策略路由；

◆ 基于数据包大小的策略路由；

◆ 基于应用的策略路由；

◆ 通过缺省路由平衡负载。

（3）设计访问控制列表时需考虑的规则

◆ 自上而下的处理方式

访问控制列表项的检测按自上而下的顺序进行，并且从第一个表项开始，所以必须考虑在访问表中放入语句的次序。

◆ 添加表项

新的表项被添加到访问表的末尾，也就是说，不可能改变已有访问表的功能。如果要改变，就必须创建一个新访问表并删除已存在的访问表，并且将新访问表用于接口上。

◆ 访问表位置

尽量考虑将扩展的访问表放在靠近过滤源的位置上，这样创建的过滤器就不会反过来影响其他接口上的数据流。另外，尽量使标准的访问表靠近目的，由于标准访问控制列表只使用源地址，因此将其靠近源会阻止报文流向其他端口。

◆ 语句的位置

由于IP协议包含ICMP、TCP和UDP，所以应将更为具体的访问控制列表项放在不太具体的表项前面，以保证位于另一语句前面的语句不会否定表中后面语句的作用效果。

◆ 其他注意事项

如果没有access-list，则默认选项等于permit any，允许。一旦添加了访问控制列表，最后缺省为deny any，禁止。

可见，网络管理员可以通过本地网络的边界路由器本身所提供的访问控制列表，实现本地网络很多的安全及其他应用要求。

3. 网络地址转换

NAT网络地址转换，其功能是将企业内部自行定义的非法IP地址转换为Internet公网上可识别的合法IP地址。NAT转换是静态或动态地转换IP报文的源IP 地址和（或）目的IP地址，使离开和（或）进入地址与原来不同，该功能可以隐藏内部网络的IP地址，以达到保护企业内部网络的目的。

（1）配置方法

NAT设置可以分为静态地址转换、动态地址转换、复用动态地址转换。

◆ 静态地址转换

静态地址转换将内部本地地址与内部合法地址

进行一对一地转换，且需要指定和哪个合法地址进行转换。如果内部网络有E-mail服务器或FTP服务器等可以为外部用户提供服务，则这些服务器的IP地址必须采用静态地址转换，以便外部用户可以使用这些服务。

◆ 动态地址转换

动态地址转换也是将内部本地地址与内部合法地址一对一地转换，但是动态地址转换是从内部合法地址池中动态地选择一个未使用的地址来对内部本地地址进行转换的。

◆ 复用动态地址转换

复用动态地址转换首先是一种动态地址转换，但是它可以允许多个内部本地地址共用一个内部合法地址。对只申请到少量IP地址但却经常同时有多个用户使用外部网络的情况，这种转换极为有用。

(2) 网络地址转换技术(NAT)

目前市场上的路由器支持内部地址翻译、外部地址翻译和双向地址翻译功能。

内部地址翻译包括：源地址的静态单一地址翻译、源地址的静态子网翻译、源地址静态TCP翻译、源地址静态UDP翻译、源地址访问列表+地址池翻译、源地址访问列表+设备接口翻译、目的地址访问列表+地址池翻译。

外部地址翻译包括：源地址的静态单一地址翻译、源地址的静态子网翻译、源地址静态TCP翻译、源地址静态UDP翻译、源地址访问列表+地址池翻译。

NAT技术的应用环境是一个有惟一出口的桩网络，这样才能保证所有的通信都必须经过NAT技术的网关，地址的转换不发生歧义。它通过地址复用来提高对已注册地址的有效利用率。NAT技术中具体的IP地址复用方法是：在内部网中使用私有的虚拟地址，即由Internet地址分配委员会(IANA)所保留的几段Private Network IP地址。

以下是预留的Private Network地址范围：

10.0.0.0 ——10.255.255.255

172.16.0.0 ——172.31.255.255

192.168.0.0 ——192.168.255.255

由于这部分地址的路由信息被禁止出现在Internet骨干网络中，所以如果在Internet中使用这些地址是不会被任何路由器正确转发的，因而也就不会因使用这些地址而相互之间发生冲突。在边界路由器中设置一定的地址转换关系表并维持一个注册的真实IP地址池(IP Pool)，通过路由器中的转换功能将内部的虚拟地址映射为相应的注册地址，使得内部主机可以与外部主机间透明地进行通信。

NAT技术一般的形式为：NAT网关依据一定的规则，对所有进出的数据包进行源与目的地址识别，并将由内向外的数据包中源地址替换成一个真实地址(注册过的合法地址)，而将由外向内的数据包中的目的地址替换成相应的虚地址(内部用的非注册地址)。

从网关的出入方向看，NAT有入向地址转换(inbound)、出向地址转换(outbound)和双向转换(bi-directional)3种形式。绝大多数应用都属于入向转换形式，其他2种形式极少用到。从转换对应关系的角度来看，NAT还可分为静态转换和动态转换二类。所谓静态转换就是在网关上预先设置好虚拟地址与实际地址的一一对应关系，在工作时不作实时更改；而动态转换则无需预先设置，直接由网关在运行时根据网络连接和地址空间的使用情况自行决定地址对应关系。

(3) NAT术语

◆ NAT用语

Inside local，即内部局部地址——在内部网络上一个主机分配到的IP地址，通常是网管人员自己定义的私有地址。这个地址可能不是网络信息中心(NIC)或服务提供商所分配的合法IP地址。

Inside global，即内部全局地址——一个合法的IP地址(由NIC或服务供应商分配)，向外部网络描述一个或多个本地合法IP地址。

Outside local，即外部局部地址——出现在内部网络的一个外部主机的IP地址。不一定是合法地址，它可以在内部网络中，从可路由的地址空间进

行分配。

Outside global，即外部全局地址——主机的拥有者在外部网络上分配给主机的IP地址。该地址可以从全局可路由地址或网络空间进行分配。

◆ 内部全局地址的超载

通过允许路由器为多个局部地址使用一个全局地址，可以在内部全局地址池中保存地址。当配置了超载后，路由器从较高级的协议（例如TCP或UDP端口号）中保持足够的信息，将这个全局地址转换到正确的局部地址。当多个本地地址映射到一个全局地址时，每一个内部主机的TCP或UDP端口号用于在诸多本地地址之间区分。一个内部全局地址代表多个内部局部地址时的NAT操作。TCP端口号充当区分者。

◆ 翻译重叠地址

NAT探讨了转换IP地址，也许是因为IP地址不是合法正式分配的IP地址，也许是选择了一个正式属于另一个网络的IP地址。上面这种地址既被合法的使用又被非法的使用的情况称做重叠。可以使用NAT去翻译与外部地址重叠的内部地址。

◆ 提供TCP负载均衡

另一种使用NAT的方式是与Internet地址无关的。你的机构可能有多个主机必须与一个频繁使用的主机通信。使用NAT，在内部网上建立一个虚拟主机用于在那些真实主机中协调负载均衡。匹配一个访问列表的目地地址用循环地址池中的地址替换。分配是在一个循环中完成的，且只当打开了一个从外部到内部的新连接时。非TCP的通信不用经过翻译(除非其他翻译有效)。

◆ 改变翻译超时

缺省时，在经过一段时间的空闲后，动态地址翻译会超时。如果需要可以改变超时的缺省值。当超载没有配置时，在1h后简单的翻译项就会超时。如果配置了超载，就会对翻译超时有一个较好的控制，因为每一项包含了更多的内容。

◆ 监视和维护NAT

缺省时，动态地址翻译将按NAT转换表所规定的时间超时。可以在超时前，通过在管理态方式下清除超时项。

◆ NAT池

NAT池指用户向ISP申请了一组合法IP，在路由器中，将这一组IP定义成NAT池，通过动态分配的办法，共享很少的几个外部合法IP地址。如果NAT池中动态分配的外部IP地址全部被占用后，后续的NAT翻译申请将会失败。用地址超载功能，通过端口号区分不同的连接，可解决这个问题。

◆ PAT端口地址转换

通过PAT技术，用户只需向ISP申请一个合法IP，就可以满足所有的用户访问Internet。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。PAT可以支持同时连接64500个TCP／IP、UDP／IP，但实际可以支持的工作站个数会少一些。

4．交换缓存技术

所谓的交换缓存技术即一个报文到达后，将它从接口存储器拷贝到主CPU的内存中，CPU从中抽取IP地址，确定网络号，执行路由表查找，再将其拷贝到输出接口的输出队列。这种方法的数据报文的吞吐量取决于CPU处理报文的速度。这样也很容易使CPU超载，CPU性能会因为高负荷而降低。通过路由器的数据达到10M bit/s会完全耗尽像2500这种配置的路由器CPU。在边界路由器的接口上配置允许路由缓存，这样数据流中的第一个报文同前面说描述的那样进行进程交换。在进程交换时，路由器装入一个缓存，其中有目的地址，要使用的接口和一个预先建立的合适于输出接口的数据帧头。当具有同一目的地址的另一个报文到来时，只有所需的IP头的信息被拷贝进CPU的内存，减少了被拷贝的数据量，节约了时间，增加了路由器的吞吐量，使路由器更加高效。解决方法，对于图1中所示的路由器的两条输出路径而言，就要采用路由缓存技术来提高网络性能。

5．虚拟局域网

虚拟局域网是一种通过将局域网内设备逻辑划

分成一个个网段从而实现虚拟工作组的新兴技术。这些工作站可以分布在多个实际的局域网网段上，而可以像都处于同一个局域网内一样地通信。有关虚拟局域网的技术详见下一篇文章：虚拟局域网。

6. 网络防火墙

(1) 防火墙 (Fire Wall)

防火墙就是一个或一组网络设备（计算机系统或路由器等），用来在两个或多个网络间加强访问控制，其目的是保护一个网络不受来自另一个网络的攻击。防火墙一般采用如下几种结构。

◆ **最简单的结构**

这种网络结构能够达到使受保护的网络只能看到“桥头堡主机”（进出通信必经之主机）。桥头堡主机不转发任何TCP/IP通信包，网络中的所有服务都必须有桥头堡主机的相应代理服务程序来支持。但它把整个网络的安全性能全部托付于其中的单个安全单元，而单个网络安全单元又是攻击者首选的攻击对象，防火墙一旦破坏，桥头堡主机就变成了一台没有寻径功能的路由器，系统的安全性不可靠。

◆ **单网端防火墙结构**

其中屏蔽路由器的作用在于保护堡垒主机（应用网关或代理服务）的安全而建立起一道屏障。在这种结构中可将堡垒主机看作是信息服务器，它是内部网络对外发布信息的数据中心，但这种网络拓扑结构仍把网络的安全性大部分托付给屏蔽路由器，系统的安全性仍不十分可靠。

◆ 增强型单网段防火墙的结构

在内部网与子网之间增设一台屏蔽路由器，这样整个子网与内外部网络的联系就各受控于一个工作在网络级的路由器，内部网络与外部网络仍不能直接联系，只能通过相应的路由器与堡垒主机通信。

(2) 分布式防火墙

◆ **广义分布式防火墙**

包括网络防火墙、主机防火墙和中心管理3部分。网络防火墙部署于内部网与外部网之间以及内网子网之间。网络防火墙区别于边界防火墙的特征在于，网络防火墙需支持内部网可能有的IP和非IP协议，而边界防火墙并不需要。主机防火墙对网络中的服务器和桌面系统进行防护，主机的物理位置可能在企业网中，也可能在企业网外。由于边界防火墙只是网络中的单一设备，因此对其进行的管理也只能是局部管理。对于广义分布式防火墙来说，每个防火墙作为安全监测机制的组成部分，必须根据不同的安全要求被布置在网络中任何需要的位置上，它的管理必须是统一进行的，中心管理是分布式防火墙系统的核心和重要特征之一。安全策略的分发及日志的汇总都是中心管理具备的功能。

◆ **狭义分布式防火墙**

指驻留在网络主机（如服务器或桌面机）并对主机系统提供安全防护的软件产品，驻留主机是这类防火墙的重要特征。这类防火墙将该驻留主机以外的其他网络都认作是不可信任的，并对驻留主机运行的应用和对外提供的服务设定针对性很强的安全策略。

三、边界路由器策略具体实现

1. ACL的利用

(1) 边界处路由器的高效利用策略

◆ **边界处路由器的所有权**

使用访问控制列表可以实现边界路由器不被其他网络无偿使用，通过命令拒绝目的地址不是网络内部地址的信息包，这样当无用的信息包到达边界路由器时，就会被丢弃。

具体配置如下：

```
1）教育网和ISP数据网络的出口处的路由器设置：
router C(config)#access-list 100 permit 本地网真实IP段 通配符掩码
router B(config)#access-list 101 permit 本地网真实IP段 通配符掩码
多个出口可使用此命令重复配置。
2）选择ACL应用到入站接口：
router C(config)#access-list 100 in
router B(config)#access-list 101 in
```

◆ 交换缓存技术

使用交换缓存技术，在进程交换时，路由器装入一个缓存，包括目的地址，要使用的接口和一个预先建立的适合于输出接口的数据帧头。当具有同一目的地址的另一个报文到来时，只有所需的IP头的信息被拷贝进CPU的内存，从而减少了被拷贝的数据量，增加了路由器的吞吐量，使路由器更加高效。配置时只须在路由器上启用交换缓存。

（2）在路由器上为服务器作关于源地址的策略路由

```
1）指明针对哪些服务器作策略路由，对源地址作控制，使用标准控制列表：
router A(config)#access-list 2 permit 主机IP地址
2）创建路由映射，指明服务器数据包输出接口，并指定匹配的访问控制列表和路由器下一跳地址：
router A(config)#route-map djz permit 10
router A(config-route-map)#match ip address 2
router A(config-route-map)#set ip next-hop 出口处路由器段口地址
服务器数据包输出的接口由映射标记djz指明，序列号（sequencenumber）为10，第二行中即1中定义的访问控制列表号码。
3）在校园网的接口上为路由器映射启用策略路由。
router A(config-if)#ip policy route-map djz
```

其中djz即在2中指明的映射标记，这样2中服务器输出接口即指哲理的接口。按规定，路由映射标记对一个接口只能由一个，但序列号(sequencenumber）可以有多个，系统会依据序列号顺序匹配路由入口。

2. 安全的实现

大中型网络基本上都是由局域网、广域网、外部网接入3大部分组成。为了建立起强大、稳定、安全的网络，可以从以下3大安全层次着手设计与管理：局域网的安全、广域网的安全、外部网的安全。这三大安全层次针对的是网络结构的不同部分，应结合起来才能构成完善的园区网络安全保障体系。

（1）以交换式集线器代替共享式集线器

为了达到最好的网络性能，一般企业局域网结构采用分层结构，局域网的中心交换机为网络的核心，网络最终用户的接入往往是通过分支集线器而不是交换机，使用最广泛的分支集线器通常是共享式集线器，如图2所示。

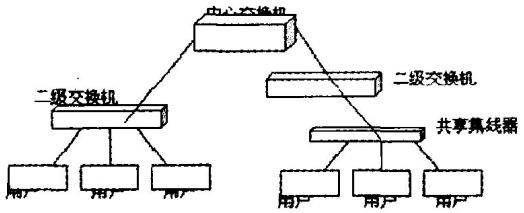

图2

这种最终用户接入方法正是网络安全性的隐患所在。用交换式集线器代替共享式集线器可以较好地消灭这一网络安全隐患。其中防火墙技术可根据防范的方式和侧重点的不同而分为多种类型，但总体来讲可分为两大类：分组过滤和应用代理。

◆ 分组 滤 (Packet Filter)

分组过滤作用在网络层和传输层，与应用层无关。它根据分组报头源地址、目的地址和端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤条件的数据包才能转发到相应的目的地出口端，其余数据包则从数据包中丢弃。分组过滤或包过滤，是一种通用、廉价、有效的网络安全手段。

目前，多数情况下校园网是通过路由器与Internet相连，校园网内的IP地址范围是确定的，而且有明确的闭合边界（如图1），网络地址为202.119.224.0。以校园网中心为例，设它有一个C类IP地址202.119.224.1，有DNS、Email、WWW、FTP等服务器，可以制定以下防火墙存取控制策略：

```
① 对进入Internet网络的控制
每个校园网都有自己合法的IP地址，应禁止非法IP地址用户从本企业路由器访问Internet，用如下命令设置校园网的防火墙：
router A(config)#Interface E0
router A(config-if)#ip address 202.119.224.1
```

```
255.255.255.0
router A(config-if)#Ip access-group 20 out
对于出防火墙的数据包的限制
router A(config)#access-list 20 permit ip 202.119.224.0 0.0.0.255
允许源网络地址为202.119.224.0用户发出的IP数据包经过
网络地址202.119.224.0→Firewall→Internet→S0→E0→园区网→SMTP NS→DNS→WWW→FTP NS
```

② 对网络中心资源主机的访问控制

校园网络中心的DNS、Email、FTP、WWW等服务器是重要的资源，要进行特别的保护，可以采取以下的策略。对网络中心所在的子网禁止DNS、Email、WWW、FTP以外的一切服务，这样可以保证网络中心在提供基本服务的前提下，获得最大的安全性。配置方法如下，其中202.119.224.2，202.119.224.3，202.119.224.4，202.119.224.5分别为dns、smtp、www、ftp服务器的IP地址：

```
router A(config)#interface s0
router A(config-if)#ip access-group 101 in
router A(config)#access-list 101 permit tcp any host established
router A(config)#access-list 101 permit udp any host
202.119.224.2 eq dns
允许外部网络用户的DNS请求。
router A(config)#access-list 101 permit tcp any host
202.119.224.3 eq smtp
允许外部网络用户的Email请求。
router A(config)#access-list 101 permit tcp any host
202.119.224.4 eq www
允许外部网络用户的WWW请求。
router A(config)#access-list 101 permit tcp any host
202.119.224.5 eq ftp
允许外部网络用户的FTP请求。
```

◆ **应用代理（Application Proxy）**

应用代理也叫应用网关（Application Gateway），它作用在应用层，掌握着应用系统中可用作安全决策的全部信息，是内部网与外部网的隔离点，其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

应用网关系统对网络用户运行的各个应用都使用特殊目的代码，需要特殊的应用软件（如Netscape Proxy Server和Microsoft Server Proxy）。

3. 实现路径选择

（1）使用网络地址转换

整个校园网对外访问的缺省路由指向连通数据网出口，访问教育网站点的路由指向教育网出口；在ISP数据网出口上做地址转换以确保通过该出口对外访问的数据信息能按同路径返回；做关于源地址的策略路由（policy based routing，PBR），以解决网络外部用户对学校服务器（如DNS、WWW、E-MAIL等）的顺利访问，ISP数据网上建立学校主页的镜像站点，家属区用户开通访问校园网的路由使家属区用户可以直接访问校园网服务。

具体配置如下：

```
在router A上作缺省路由指向ISP数据网出口，访问教育网的静态路由指向教育网出口：
router A(config)#ip router 0.0.0.0 0.0.0.0
router A(config)#ip router 教育网的静态地址段。其子网掩码
ISP出口处IP
在路由器上作超载地址转换：
1）在校园网的接口上设置地址转换内部接口：
router A(config-if)#ip nat inside
2）在连接router B的接口上设置地址转换外部接口：
router B(config)#ip nat outside
3）在全局配置模式下设置nat池：
router A(config)#ip nat pool sdust 真实IP段 子网掩码
4）全局配置模式下配置控制列表：
router A(config)#access-list 1 permit 可作NAT的IP 通配 掩码
5）全局配置模式下配置超载NAT，启动地址转换并关联源地址于转换地址
router A(config)#ip nat inside source list 1 pool sdust overload
```

（2）不使用网络地址转换

缺省路由指向教育网出口；在该出口上做访问控制以拒绝对非教育网信息的访问请求校内提供Web服务、服务的服务器、允许其通过教育网出口向Internet上任何地点传送。ISP数据网申请若干企