# 浅析校园网的安全

黄慧

上海济光职业技术学院信息中心　上海　201901

摘要：计算机网络已经应用了几十年，互联网已经发展成为一个全球的大网络。期间校园网也得到了飞速的发展，但是到目前为止，网络的安全仍然存在着很大的风险，整个校园网络的安全一直是各学校重点关心及研究的领域。

关键词：校园网；安全

## 0　引言

随着计算机网络的不断发展，网络的开放性、共享性、互连性随之扩大。特别是互联网的普及，使得网上交易、网络银行等一些网络新生业务的迅速兴起，计算机网络安全性问题显得相当重要。目前造成网络不安全的主要因素是系统、协议及数据库等的设计上存在缺陷。由于当今的计算机网络操作系统在本身结构设计和代码设计时偏重考虑系统使用时的方便性，导致了系统在远程访问、权限控制和口令管理等许多方面存在安全漏洞。网络互连一般采用 TCP/IP 协议，它是一个工业标准的协议簇，但该协议簇在制订之初，对安全问题考虑不多，协议中有很多的安全漏洞。同样，数据库管理系统(DBMS)也存在数据的安全性、权限管理及远程访问等方面问题，在 DBMS 或应用程序中可以预先安置从事情报收集、受控激发、定时发作等破坏程序。

由此可见，针对系统、网络协议及数据库等，无论是其自身的设计缺陷，还是由于人为的因素产生的各种安全漏洞，都可能被一些另有图谋的黑客所利用并发起攻击。因此要保证校园网网络安全，则必须熟知黑客攻击网络的一般过程。只有这样方可在黑客攻击前做好必要的防备，从而确保网络运行的安全和可靠。

## 1　校园网防火墙配置的总原则

在校园网防火墙的配置时，要考虑以下两个问题：

(1) 可伸缩性问题：某学院校园网对防火墙的需求不同于一般性的商业公司。按照校园网要求配置防火墙的时候，防火墙应当具有伸缩性，可以随着它所保护网络的发展而升级。它应该考虑到教工和学生的需求，他们希望能网上冲浪和发送 e_mail。如今，由于 TCP/IP 协议既用于 Internet 又用于内部网络，防火墙也需要根据学校的具体需要对 IP 地址进行一些处理，例如，IP 转发或 NAT 等。

防火墙需要根据它所保护网络不同要求作相应的改变。很可能，这其中的变化之一就是某学院自身的发展，而更多教学方面信息来自 Internet 这些意味着将需要更多的防火墙资源，要注意进行定期检查并按需要升级软件和硬件来更新防火墙。

(2) 系统效率问题：安装防火墙的挑战之一，就是上网人员用来通信和交换数据的速度。防火墙的功能越强大，数据的传送速度可能就越小。

可供堡垒主机使用的处理资源和内存资源是防火墙的两个重要特征。尽管堡垒主机可能不是防火墙组成结构中惟一的硬件部分，当其防火墙软件运行时，它具有重要的作用。如果主机运行得太慢，或者它没有足够的内存来处理大量的包过滤决策、代理服务请求和其他通信，整个系统的效率将会受到严重的影响，这是因为堡垒主机处于网络的周边，并且如果没有设置其他的堡垒主机和防火墙来保证网络负载平衡的话，该堡垒主机将是通信能否顺利通过的惟一网关。

堡垒主机并不仅仅是一台经过特别配置的，可以运行的防火墙、代理服务器和其他软件的计算机，它还需要足够快的处理器速度和大容量的内存来处理网络的当前通信。对防火墙和堡垒主机来说，可伸缩性和安全性都很重要，但是，内存状况对防火墙的性能发挥和它所保护的个人用户的工作效率很重要。堡垒主机需要足够的 RAM，以便支持每个程序的运行，这些程序对本机加载必不可少，否则，堡垒主机需要执行内存交换，从而降低了效率。

关键资源是和硬件或者软件相关的内容，它在服务或者

作者简介：黄慧(1976-)，男，硕士研究生，研究方向：计算机网络、多媒体技术。

程序的运行过程中起重要作用。表 1 列出了防火墙成功运行的关键资源。

表 1 防火墙服务的关键资源

| 关键资源 | 有待限制的服务 |
|---|---|
| DISK I/O | 电子邮件 |
| DISK I/O | 新闻 |
| 堡垒主机操作系统的性能 | IP 路由 |
| 堡垒主机操作系统的性能 | WEB 缓存 |
| 堡垒主机操作系统的性能 | WEB |

表中第二列中的限制项目可以节省关键资源。

## 2 校园网防火墙配置的具体策略

设置了安全策略，并且决定了防火墙要遵循的规则以后，就可以按照既定的策略来配置防火墙。不同防火墙配置的特点，如表 2 所示。

表 2 不同防火墙配置的特点

| 名称 | 说明 |
|---|---|
| 屏蔽路由器 | 位于客户计算机和 internet 之间的包过滤路由器 |
| 双宿主主机 | 用于 internet 连接的客户计算机来主控防火墙软件 |
| 屏蔽式主机 | 专用于提供安全功能的主机来主控防火墙软件 |
| 共用一个防火墙的两个路由器 | 路由器放置在防火墙的内外部接口上，对数据包进行过滤 |
| DMZ 屏蔽子网 | 该网络与防火墙相连，具有公共服务器(DMZ)，但处在受保护的内部网络的外面 |
| 多重防火墙 DMZ | DMZ 附带两个防火墙，有更高的安全性 |
| 反向防火墙 | 防火墙监控出站而不是入站的通信 |
| 专用防火墙 | 防火墙用来保护特殊类型的通信，比如电子邮件 |

表 3 防火墙受到的威胁及相应的抵御措施

| 威胁 | 防御 |
|---|---|
| SYN flooding | cisco PIX 防火墙配有 flood Defender，可以阻断此类攻击 |
| 端口扫描 | 检查防火墙日志，并阻断有恶意的 ip 地址访问 |
| 病毒 | 确保病毒防护软件已和防火墙的软硬件结合使用 |
| 有害的电子邮件附件 | 使用软件扫描 Port25 的 SMTP 通信，例如 Cisco PIX 防火墙自带的 Mail Guard |

### 2.1 DMZ 屏蔽子网的防火墙

某学院校园网的防火墙系统类似于 DMZ 屏蔽子网的防火墙。所谓 DMZ 屏蔽子网的防火墙是在内部网络和外部网络之间建立一个被隔离的子网，用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开，在很多实现中，两个分组过滤路由器放在子网的两端，在子网内构成一个“非军事区”DMZ。有的屏蔽子网中还设有一堡垒主机作为惟一可访问点，支持终端交互或作为应用网关代理。这种配置的危险带仅包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。

如果攻击者试图完全破坏防火墙，他必须重新配置连接三个网的路由器，既不切断连接又不要把自己锁在外面，同时又不使自己被发现，这样也还是可能的。但若禁止网络访问路由器或只允许内网中的某些主机访问它，则攻击会变得很困难。在这种情况下，攻击者得先侵入堡垒主机，然后进入内网主机，再返回来破坏屏蔽路由器，整个过程中不能引发警报。屏蔽子网防火墙能够帮助建立一个非防护区，这种类型防火墙利用堡垒主机夹在两个路由器中间，所以它是最安全的防火墙系统。

对于进来的信息，外面的这个路由器用于防范通常的外部攻击(如源地址欺骗和源路由攻击)，并管理 Internet 到 DMZ 网络的访问。它只允许外部系统访问堡垒主机(还可能有信息服务器)。里面的这个路由器提供第二层防御，只接受源于堡垒主机的数据包，负责的是管理 DMZ 到内部网络的访问。

对于去往 Internet 的数据包，里面的路由器管理内部网络到 DMZ 网络的访问。它允许内部系统只访问堡垒主机(还可能有信息服务器)。外面的路由器上的过滤规则要求使用代理服务(只接受来自堡垒主机的去往 Internet 的数据包)。如图 1 所示。

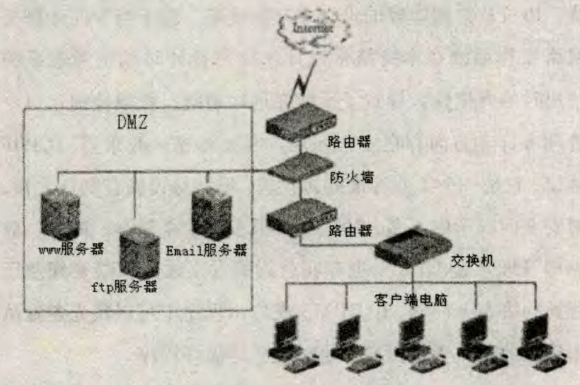


图 1 DMZ 屏蔽子网示意图

部署 DMZ 屏蔽子网防火墙系统有如下优点：

(1) 入侵者必须突破 3 个不同的设备(无法探测)才能侵袭内部网络：外部路由器，堡垒主机，还有内部路由器。

(2) 由于外部路由器只能向 Internet 通告 DMZ 网络的存在，Internet 上的系统不需要有路由器与内部网络相连。这样网络管理员就可以保证内部网络是“不可见”的，并且只有在 DMZ 网络上选定的系统才对 Internet 开放(通过路由表和 DNS 信息交换)。

(3) 由于内部路由器只向内部网络通告 DMZ 网络的存在，内部网络上的系统不能直接通往 Internet，这样就保证了内部网络上的用户必须通过驻留在堡垒主机上的代理服务才能访问 Internet。

(4) 包过滤路由器直接将数据引向 DMZ 网络上所指定的系统，消除了堡垒主机双宿的必要。

(5) 内部路由器在作为内部网络和 Internet 之间最后的防火墙系统时，能够支持比双宿堡垒主机更大的数据包吞吐量。

(6) 由于 DMZ 网络是一个与内部网络不同的网络，NAT(网络地址变换)可以安装在堡垒主机上，从而避免在内部网络上重新编址或重新划分子网。

## 2.2 校园网防火墙系统的新功能

为了使学校的校园网络更加安全可靠，某学院对其校园网的防火墙添加了一些特殊的功能。

(1) NAT

学校的路由器或者防火墙执行 NAT 时，可以把公共 IP 地址转变为专用地址，反之亦然，这样可以对外部的计算机隐藏受保护网络上计算机的 IP 地址。使用 NAT 进行简单的数据传送的步骤如图 2 所示。

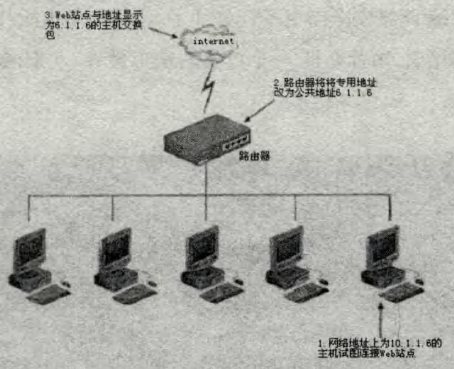


图 2 网络地址转换示意图

(2) 加密

做SSL或者其他类型加密的路由器或者防火墙在接收一个请求后，通过私钥将它转为杂乱数据，然后通过接收者的路由器或者防火墙交换公钥。接着就可以对消息进行解密，并以一种容易理解的形式把它提供给终端用户，如图 3 所示。

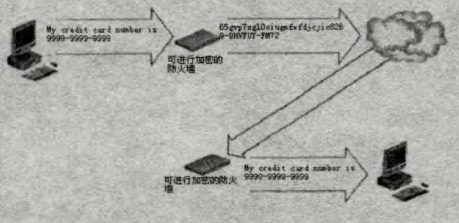


图 3 路由器或者防火墙可以对消息加密

(3) 应用程序代理

应用程序代理是一个软件，它根据主机的要求，接收请求，重建请求，把它们发送到指定的位置，就像是从它(代理)那里发出的请求一样。它可以通过双宿主主机来创建。在双宿主主机设置中，包括防火墙或者代理服务器软件的主机拥有两个接口，一个和 Internet 相连，另一个和受保护的内部网络相连(见图 4)。某学院校园网采用的是应用程序代理，因为它是一套软件相对来讲比较易维护、易操作；同时也比较安全可靠。

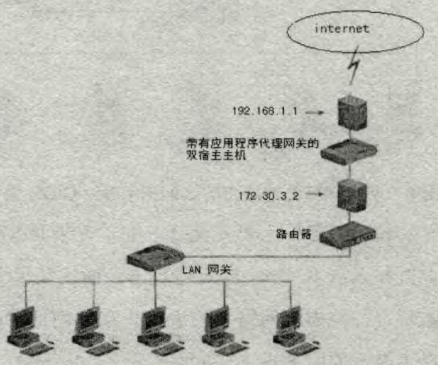


图 4 双宿主主机上的应用程序代理

因为双宿主主机位于内部 LAN 和 Internet 之间，位于内部网络上的主机永远不能直接访问 Internet。根据双宿主主机的要求，代理服务器程序发出请求，并且将来自 Internet 的包转发到主机上去。

在屏蔽子网中，提供代理服务器软件的主机拥有一个独立的网络接口。除了代理服务器软件指定的数据类型，主机过滤器两端的包过滤器会过滤掉所有的通信。

(4) 入侵检测系统(IDS)

监控到可能的入侵袭击并及时报警，可以有多种选择。入侵检测系统安装在处于网络边界的外部或者内部的路由器上(见图 5)。许多流行的软件防火墙包中内置 IDSB 了，包括 Secure Computing 的 Sidewinder。

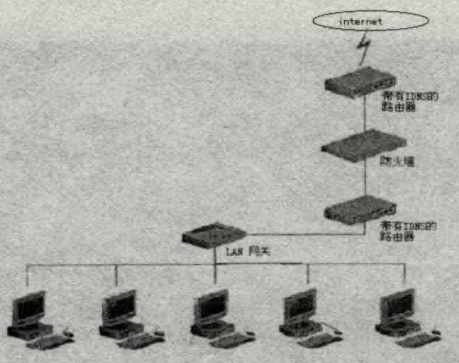


图 5 并入边界路由器的 IDS 系统

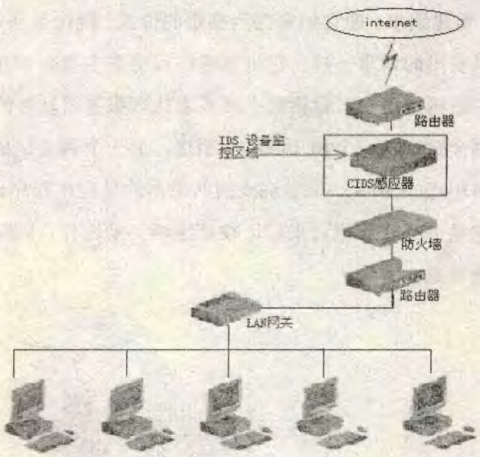


图 6 防火墙与外部路由器之间的 Cisco CIDS 设备

某学院校园网为什么要安装 IDS 呢？安装 IDS 的外部路由器负责告知来自 Internet 的入侵攻击，而安装了 IDS 的内部路由器负责监控内部网络上的主机，在他们试图通过可疑端口或者不寻常的服务进入 Internet 时通知管理员，这些动作可能是已侵入计算机的特洛伊木马病毒引起的。IDS 也可以用来寻找是否有大量的 TCP 连接请求发送到了目标计算机的许多端口上，因此可以发现是否有人正企图进行 TCP 端口的扫描。若有则发送警报通知管理员，及时阻断此类攻击。

Cisco CIDS 的入侵检测系统(IDS)可以有不同的工作方式。它负责监控防火墙和 Internet 之间的区域。通过配置，能够检测到来自 Internet 上对防火墙的攻击时间(见图 6)。

## 3 小结

校园网的安全性是校园网正常运行的前提，对校园网健康发展至关重要。首先，提出了防火墙配置总的策略，主要关心两点：(1)可伸缩性；(2)运行效率。对不同的防火墙配置进行了列表比较，某学院选用的是性价比较高的 DMZ 屏蔽子网防火墙系统，因为其对安全性有较大的保证，所以被人们认为是目前最好的校园网防火墙。在此基础上，某学院又对防火墙添加了新功能有 4 个：(1)NAT；(2)加密；(3)应用程序代理；(4)入侵检测系统。

## 参考文献

[1]孙锋编著.网络安全与防黑技术.北京：机械工业出版社.2004.

[2]赵泉编.网络安全与电子商务.北京:清华大学出版社.2005.

[3]朱传靖著.知者无畏:一个真实的病毒世界.北京:金城出版社.2002.

**On the campus network security**

Huang Hui
Shanghai Jiguang College Information Center,Shanghai,201901,China

**Abstract:**Computer networks have been applied for decades, the Internet has become a major global network. During the campus network has also been rapid development, but so far, network security remains a big risk, the entire campus network security has been the focus of concern for schools and research areas.

**Keywords:**campus network;security

[上接 38 页]

**Micro blog:new Measure Influence Public Security**

Pang Ping
Xi'an Institute of politics military security department,Shanxi,710068,China

**Abstract:**As a new kind of social network, micro blog has more and more influence in public opinion. The messages with intense consedment from mirco blog spread faster and has large impact. The negative information spread and specalate in a wide range,which could not be ignored as a potential threat for the public security. For strengthen supervision,guidance-control and investigation afterward,we should start our work from enlarge pre-prevention awareness and ability, innovate public-security management and using law and technology strategy.

**Keywords:**Micro blog;Functional features;Public security;Countermeasures researches