

山东体育学院

鲁体院网字〔2022〕3 号

关于印发山东体育学院网络安全技术方案 的通知

各部、处、室、系、校：

《山东体育学院网络安全技术方案》已经院长办公会研究通过，现予印发，望认真贯彻执行。



二〇二二年十月十五日

山东体育学院

网络安全技术方案

目录

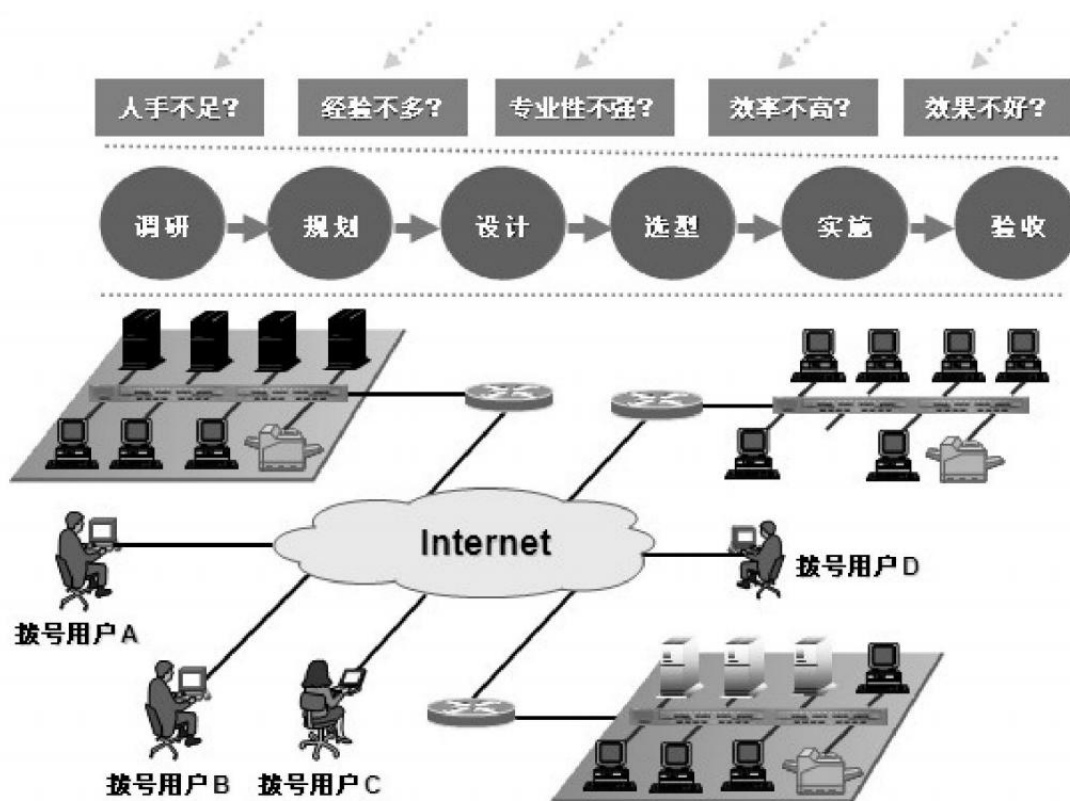
1	网络安全实施的难点分析.....	1
1.1	IT 系统建设面临的问题	1
1.2	IT 系统运维面临的问题	2
2	系统安全.....	2
2.1	网络系统安全风险分析.....	2
2.1.1	设备安全风险分析.....	2
2.1.2	网络安全系统分析.....	3
2.1.3	系统安全风险分析.....	3
2.1.4	应用安全风险分析.....	4
2.1.5	数据安全风险分析.....	4
2.2	网络系统安全设计.....	4
2.2.1	设备安全.....	4
2.2.2	网络安全.....	4
2.2.3	系统安全.....	5
2.2.4	应用安全.....	6
2.2.5	数据安全.....	6
2.3	系统的网络安全设计.....	7
2.3.1	防火墙系统.....	7
2.3.1.1	防火墙的基本类型.....	7
2.3.1.2	常用攻击方法.....	10
2.3.1.3	常用攻击对策.....	10
2.3.2	VPN 路由器.....	11
2.3.3	IDS 入侵检测	11
2.3.4	CA 认证与 SSL 加密	13
2.3.4.1	CA 的作用	13
2.3.4.2	CA 系统简介	14
2.3.4.3	SSL 加密.....	17
2.3.5	防病毒系统.....	19
2.3.5.1	病毒的类型.....	19
2.3.5.2	病毒的检测	22
2.3.5.3	防病毒建议方案.....	24
2.3.6	网站监控与恢复系统.....	24
2.3.7	SAN 网络存储/备份/灾难恢复:	24
3	业务网络安全设计.....	24
3.1	网络安全设计原则.....	24
3.2	系统的安全设计.....	25
3.2.1	威胁及漏洞.....	25
3.2.2	计说明.....	26
3.3	系统的安全设计.....	27
3.3.1	各业务系统的分离.....	27
3.3.2	敏感数据区的保护.....	28
3.3.3	通讯线路数据加密.....	29

3.3.4	防火墙自身的保护.....	30
3.3.5	网络安全设计.....	31
3.3.5.1	设计说明:	33

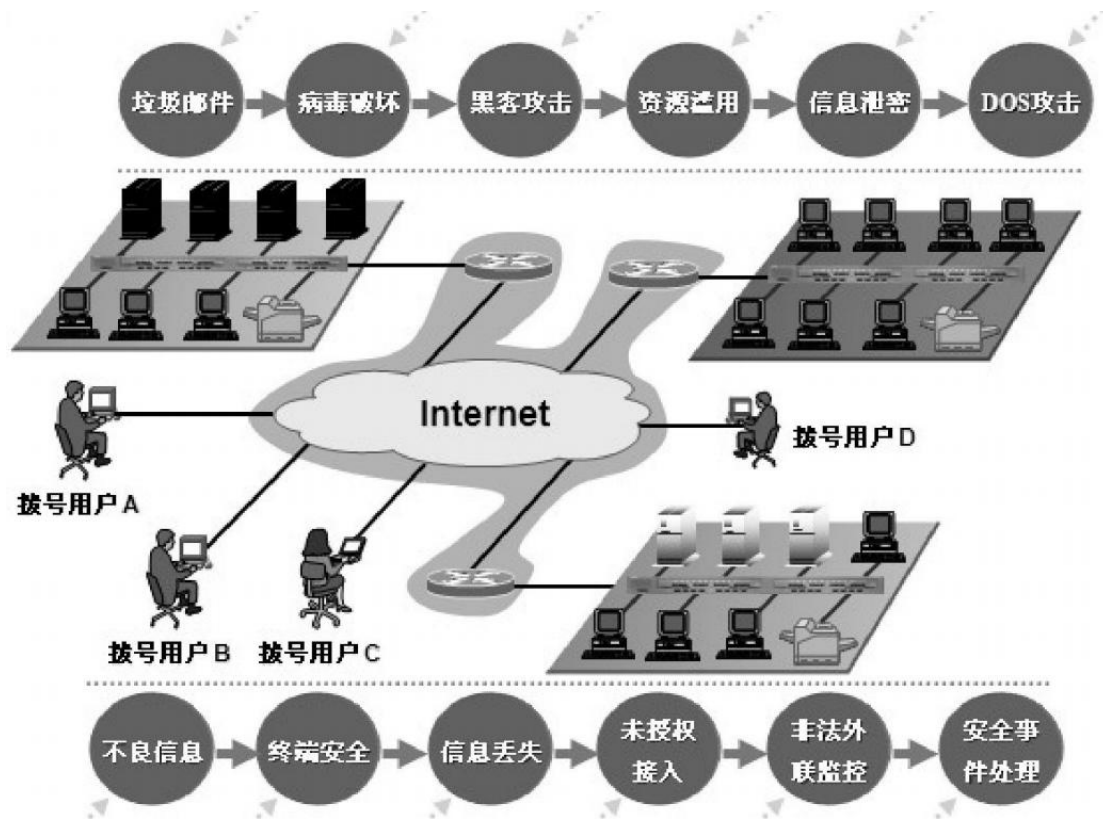
1 网络安全实施的难点分析

1.1 IT 系统建设面临的问题

高校在 IT 系统建设过程中，往往面临以下方面的问题；其一：专业人员少，因为任何一个高校的 IT 系统建设，往往都是为高校内部使用，只有自己最为了解自己高校的需求，但是往往高校内部的专业人员比较少。其二：经验不足，专业性不强，由于高校内部的专业人员仅仅着眼于本高校自身的需求，项目实施的少，相应的项目经验欠缺专业性不强；其三：效率不高，效果不好，应为欠缺对系统建设的系统知识和经验，总是在摸索着前进，在这个过程中，实施人员和使用人员的积极性就会降低，无法按照预期完成项目。



1.2 IT 系统运维面临的问题



2 系统安全

2.1 网络系统安全风险分析

2.1.1 设备安全风险分析

网络设备、服务器设备、存储设备的安全是保证网络安全运行的一个重要因素。为了保证网络的安全而制定的安全策略都是由网络设备执行的，如果一些非网络管理人员故意或无意对网络设备进行非法操作，势必会对网络的安全造成影响，甚至是重大的安全事故。因此，没有网络设备的安全，网络设备的安全就无从谈起。所以，必须从多个层面来保证网络设备的安全。

2.1.2 网络安全系统分析

网络层位于系统平台的最低层，是信息访问、共享、交流和发布的必由之路，也是黑客（或其它攻击者）等进行其截获、窃听窃取信息、篡改信息、伪造和冒充等攻击的必由之路。所以，网络层所面临的安全风险威胁是整个系统面临的主要安全风险之一。

网络层的安全风险包括以下几方面：

- 黑客攻击

外网通过防火墙与 Internet 公众网相连，所以 Internet 上的各种各样的黑客攻击、病毒传播等都可能威胁到系统的安全。其存在的安全风险主要是黑客攻击，窃取或篡改重要信息，攻击网站等。

许多机器临时性（甚至经常性的）连接到外网上或直接连接到 Internet 上。这样 Internet 上的黑客或敌对势力使用木马等黑客攻击手段，就可以将该员工机器用作一个侦察站。

- 网内可能存在的相互攻击

由于公司内网中的各级网络互连，这些设备在网络层是可以互通的，在没有任何安全措施的情况下，一个单位的用户可以连接到另一个单位使用的机器，访问其中的数据。这样就会造成网络间的互相病毒等其他因素引起的网络攻击。

2.1.3 系统安全风险分析

系统安全通常分为系统级软件比如操作系统、数据库等的安全漏洞、病毒防治。

1、系统软件安全漏洞

系统级软件比如操作系统、数据库等总是存在着这样那样的安全漏洞，包括已发现或未发现的安全漏洞。

2、病毒侵害

计算机病毒一直是困扰每一个计算机用户的重要问题，一旦计算机程序被感染了病毒，它就有可能破坏掉用户工作中的重要信息。

网络使病毒的传播速度极大的加快，公司内部网络与 Internet 相连，这意味着每天可能受到来自世界各地的新病毒的攻击。

2.1.4应用安全风险分析

基于 B/S 模式的业务系统由于身份认证、数据传输、访问控制、授权、口令等存在安全隐患，从而对整个系统造成安全威胁。

2.1.5数据安全风险分析

在系统中存放有的重要的数据。这些数据如被非法复制、篡改、删除，或是因各种天灾人祸丢失，将威胁到数据的保密性、完整性和一致性。

2.2 网络系统安全设计

针对上面提到的种种安全风险，对系统安全进行设计。

2.2.1设备安全

设备安全在这里主要指控制对交换机等网络设备的访问，包括物理访问和登录访问两种。针对访问的两种方式采取以下措施：

对基础设施采取防火、防盗、防静电、防潮措施。

系统主机应采用双机热备（主备/互备）方式，构成集群系统；

系统关键通信设备应考虑冗余备份；

要求利用系统监控工具，实时监控系统中各种设备和网络运行状态，及时发现故障或故障苗头，及时采取措施，排除故障，保障系统平稳运行。

2.2.2网络安全

为保障网络安全，在网络上要采取以下措施：

- 设立防火墙。防火墙作为内部网络与外部公共网络之间的第一道屏障，一般用在高校网与 Internet 等公众网之间的连接点处，防护来自外部的攻击，并过滤掉不安全的服务请求和非法用户进入；
- 在内部系统的 Web 服务器到应用服务器之间设置防火墙，防止来自内部的攻击和破坏，保证系统的安全；

- 进行入侵检测。对计算机网络和计算机系统的关键节点的信息进行收集分析，检测其中是否有违反安全策略的事件发生或攻击迹象，并通知系统安全管理员。
- 采用相应技术和手段，保证网络安全。对传输数据进行加密，保障数据传输安全
- 防止网页的篡改；利用防护工具防止黑客篡改或非法破坏网页，保证网站网页安全。针对防止网页篡改，推荐使用 InforGuard。InforGuard 主要提供文件监控保护功能，保证文件系统安全，防止被非法修改。InforGuard 适用于网站网页文件的安全保护，解决了网站被非法修改的问题，是一套安全、高效、简单、易用的网页保护系统；采用数字证书技术实现 InforGuard 的用户管理，加强了对 Web 站点目录的 ftp 用户和口令的保护，防止了 ftp 口令泄漏造成的安全隐患；通过用户操作日志提供对网页文件更新过程的全程监控。从而保证了网站网页文件的绝对安全。
- 定期进行安全检查，查补安全漏洞，采用漏洞扫描软件对内部服务器浏览器和所有网络设备进行漏洞扫描，及时弥补各类安全漏洞。

2.2.3 系统安全

应用安全的解决往往依赖于网络层、操作系统、数据库的安全，所以对系统级软件的安全防范突显其重要性；由于病毒通过 Internet 网，可以在极短的时间内传到 Internet 的各个角落，而病毒对系统稳定性和数据安全性的威胁众所周知，所以对病毒的预防是一项十分重要的工作；同时对一些专用服务器的特别防护也是我们保证系统良好运行的前提。下面就从系统漏洞防护、病毒防护和专用服务器防护等方面来阐述安全防范的措施。

- 系统安全漏洞防护：通过系统扫描工具，定期检查系统中与安全有关的软件、资源、各厂商安全“补丁包”的情况，发现问题及时报告并给出解决建议。
- 病毒防护：在内网和外网中分别设置网络防病毒软件控制中心，安装网络版的防病毒控制台，在服务器系统和网络内的主机均安装防病毒软件的客户端。管理员负责每天检查有没有新的病毒库更新，并对防病毒服务器上的防病毒软件进行及时更新。然后再由防病毒服务器将最新的病毒库文件下发到各联网的机器上，实现全网统一、及时的防病毒软件更新，防止因为少数内部用户的疏忽，感染病毒，导致病毒在全网的传播。
- 专用服务器的专门保护：针对重要的、最常受到攻击的应用系统实施特别的保护。对 WEB 服务器保护对 Web 访问、监控/阻塞/报警、入侵探测、攻击探测、恶意 applets、恶意 Email 等在内的安全政策进行明确规划。对 E-mail 服务程序、浏览器，采取正确

的配置与及时下载安全补丁实现。

2.2.4应用安全

针对人为操作造成的风险，必须从系统的应用层进行防范，因此应用系统在建设时需考虑系统的安全性。具体包括以下几个方面：

- 访问控制：操作系统的用户管理、权限管理；限制用户口令规则和长度，禁止用户使用简单口令，强制用户定期修改口令；按照登录时间、登录方式限制用户的登录请求；加强文件访问控制管理，根据访问的用户范围，设置文件的读、写、执行权限；对重要资料设置被访问的时间和日期。
- 权限控制和管理：按照单位、部门、职务、工作性质等对用户进行分类，不同的用户赋予不同的权限、可以访问不同的系统、可以操作不同的功能模块；应用系统的权限实行分级管理，每个系统的管理员自己定义各类用户对该系统资源的可访问内容。
- 身份验证：通过采用口令识别、数字认证方式，来确保用户的登录身份与其真实身份相符，保证数据的安全性、完整性、可靠性和交易的不可抵赖性、增强顾客、商家、高校等对网上交易的信心。
- 数据加密存储：关联及关键数据加密存储，提取数据库中表间关联数据或重要数据信息，采用 HASH 算法，生成一加密字段，存放在数据表中，保证数据库中关联数据的一致性、完整性，防止重要数据的非法篡改。
- 日志记载：数据库日志：使得系统发生故障后能提供数据动态恢复或向前恢复等功能，确保数据的可靠性和一致性。应用系统日志：通过记录应用系统中操作日志，通过事后审计功能为将来分析提供数据分析源，确保业务的可追溯性。

2.2.5数据安全

业务数据是业务系统运行的重要元素，也是高校中宝贵的资源。这些数据如被非法复制、篡改、删除，或是因系统崩溃及各种天灾人祸丢失，将威胁到数据的保密性、完整性和一致性。由此造成的损失将是巨大的。

为了保证数据的安全，通常的做法是对数据进行备份。数据备份解决方案大致可以分为两种：数据级的备份和系统级的备份。数据级的备份是指对存储在磁盘阵列、磁带库等设备上的数据的备份。系统级备份主要是指对服务器系统、数据库系统等系统的备份。

对于数据库系统备份，有两种方式可以选择：

第一种是采用数据库自身的备份功能，其优点是不需要追加额外的投资，缺点是这种备份方式是手工进行的，备份效率较低，并且在备份时需要关闭数据库，即需要 shutdown 数据库实例。

第二种方式是采用专业的备份工具，这种方式能够实现在线备份的方式，即在备份的过程中不需 Shutdown 数据库实例。同时，在备份过程中，通过追踪数据块的变动记录来实现增量备份，缩短备份窗口。在保持数据库 online 的前提下，这种方式还能够充分保证数据库的 OLTP 联机事务处理的性能。

数据库的数据量庞大，可以通过同时驱动多个磁带驱动器来保证数据库备份的效率。通过这种方式，能够在夜间的非工作时段内完成全备份，并在相对更短的时间段内完成日增量备份。

在上述数据备份环境中，可以对操作系统及应用程序环境实现动态即时在线快速备份，即在不影响用户和应用程序运行的前提下，备份系统的动态数据，同时能够将传统文件系统的备份速度成倍提高。

在前面的服务器平台设计中，我们为每台服务器都配置了两块硬盘，通过磁盘镜像（RAID 1）技术实现系统冗余备份，可以极大提高服务器系统的安全性。保证数据安全，对数据进行备份。

2.3 系统的网络安全设计

2.3.1 防火墙系统

2.3.1.1 防火墙的基本类型

实现防火墙的技术主要包括四类：包过滤防火墙、电路网关防火墙、应用层防火墙以及动态包过滤防火墙。其各自的特点如下：

包过滤防火墙：

包过滤防火墙技术主要通过分析网络传输层数据，并通过预先定义的规则对数据包转发或丢弃。其检查信息为网络层、传输层以及传输方向等报头信息，典型的包过滤主要利用下面的控制信息：

数据包到达的物理网络接口

数据包的源网络层地址

数据包的目网络层地址

传输层协议类型

传输层源端口

传输层目的端口

包过滤防火墙有以下先进性：

包过滤防火墙通常性能高，因为他们执行的评估比较少而且通常可以用硬件完成。

可以简单地通过禁止特定外部网络和内部网络的连接来保护整个网络。

包过滤防火墙对客户端是透明的，所有工作都在防火墙中完成。

结合 NAT（网络地址转换功能，可以将内部网络从外部网络中屏蔽起来。

包过滤防火墙具有以下缺点：

包过滤防火墙不能识别上层信息，因此，同应用层防火墙以及电路网关防火墙相比，其安全性较低。

包过滤防火墙不是基于连接状态的，因此，它不保存会话连接信息或上层应用信息。

包过滤只利用了数据包中有限的信息。

包过滤不提供增值服务，如 HTTP Cache，URL 过滤等。

电路网关防火墙

电路网关防火墙是一种基于连接状态的防火墙技术，它能确认、证实一个数据包是两个传输层之间连接请求、两个传输层之间已建连接中的数据包或两个传输层之间的虚电路。

电路网关防火墙检查每一个连接的建立过程来保证连接的合法性，以及利用一个合法的连接信息表（包括状态以及序列号）来检查数据包的正确性。当一个连接关闭时，这个连接信息表就被关闭。

电路网关级防火墙主要应用下列状态信息：

一个唯一的会话识别用于跟踪处理。

连接状态，包括：握手、建立以及关闭。

序列号信息。

源网络地址。

目的网络地址。

数据包到达的物理网络接口。

数据包离开的物理网络接口。

电路网关级防火墙具有以下优点：

电路网关防火墙通常性能高，因为他们执行的评估比较少。

可以简单地通过禁止特定外部网络和内部网络的连接来保护整个网络。

包过滤防火墙对客户端是透明的，所有工作都在防火墙中完成。

结合 NAT（网络地址转换功能，可以将内部网络从外部网络中屏蔽起来。

电路应用网关具有以下缺点：

电路应用网关不能限制TCP 之外的其他协议集。

电路应用网关防火墙不能进行严格的高层应用检查。

包过滤不提供增值服务，如 HTTP Cache，URL 过滤等。

应用层防火墙

应用层防火墙检查所有的数据包、连接状态信息以及序列号，同时还能验证应用层特定的安全控制，包括：用户名，口令等。

大多数应用层防火墙包括一个特定服务程序和代理服务，代理是一个面向特定应用的流量管理程序，如 HTTP、FTP 等，能提供增强的访问控制、细节检查以及审计记录等信息。

每一个应用代理一般由两部分组成，代理服务器以及代理客户，相对于发起连接的客户端来说，代理服务器充当一个最终服务器。代理客户端代替实际的客户应用同外部服务器进行数据交换。

应用层防火墙具有以下优点：

代理服务能完全理解和实施上层协议。如 HTTP、FTP 等。

代理服务维护所有的应用状态信息，包括：部分的通讯层状态信息、全部应用层状态信息以及部分会话信息。

代理服务能处理和利用数据包。

代理服务不允许外部服务器和内部主机之间的直接通讯，可有效的隐含内部网络信息。

代理服务能提供增值特征，包括：HTTP Cache、URL 过滤以及用户认证等。

代理服务能很好的产生审计记录，允许管理员监控企图违反网络安全策略的行为。

应用层防火墙具有以下缺点：

代理服务需要替换防火墙服务器的本来的网络堆栈。

由于代理服务要监听服务端口，因此，在防火墙服务器上不能提供同样的服务。

代理服务对数据包需要处理两次，因此，性能比较差。

通常，对于不同的应用，需要对每一个服务提供一个代理服务程序。

应用级防火墙不能提供 UDP、TCP 以及其他协议代理功能。

代理服务通常需要修改客户应用程序端或应用配置。

代理服务通常依赖操作系统提供设备驱动，因此，一个操作系统或应用 Bug 都有可能造成代理服务容易受到攻击。

代理服务经常会遇到多次登录的情况。

动态包过滤防火墙

动态包过滤防火墙类似电路网关防火墙，但它提供了对面向非连接的传输层协议，如 UDP 的支持。其同电路网关有相同的优缺点。

2.3.1.2常用攻击方法

了解常用的攻击方法可以更好的制定安全防范措施，常用的攻击方法包括以下几种：

被动监听：这种攻击方法是攻击者利用网络监听或分析工具，直接窃获用户的报文信息，从而获得用户/口令信息，这时，攻击者就可以以合法用户的身份对应用进行破坏。

地址欺骗：在这种方法中，攻击者伪装成一个信任主机的 IP 地址，对系统进行破坏。

端口扫描：这是一种主动的攻击方法，攻击者不断的扫描安全控制点上等待连接的监听端口，一旦发现，攻击者就集中精力对端口上的应用发起攻击。

否认服务：这种攻击方法又细分为两种：即洪水连接和报文注入，洪水连接是向目的主机发出大量原地址非法的 TCP 连接，这样，目的主机就一直处于等待状态，最后由于资源耗尽而死机。报文注入就是在合法连接的报文中插入攻击者发出的数据包，从而对目的主机进行攻击。

应用层攻击：这种攻击方法是利用应用程序的缺陷，从而获得对系统的访问权利。

特洛伊木马：在这种攻击方法中，攻击者让用户运行一个用户误认为是一个合法程序的攻击程序，从而寄生在用户系统中，为以后的攻击埋下伏笔。这种攻击方法最常见的应用就是在 WEB 服务嵌入 Java Applet、Active-X 等控件，使用户在浏览网页时，不知不觉中被寄生了攻击程序。

2.3.1.3常用攻击对策

下面我们对上面所述的攻击方法提出自己的防范措施。

被动监听：在共享式以太网结构中，一个主机发送的数据会发送到一个网段上的每主机数据包被监听是不可避免的。而交换式网络根据目的地址选择发送的端口，因此，尽量连接桌面工作站到交换机端口会避免数据包被监听。对于同各个分支机构的按 Extranet方式连接

的采用 IPSec 技术对 IP 数据包加密，该加密算法对数据加密采用 DES 算法，其 DES 密钥是动态产生的，连接双方加密密钥是通过 RAS 算法传送的，因此，具有很高的安全性。对于 Internet 个人用户的访问，数据被监听是不可避免的，因此，对这种攻击的防范是合理设定用户权限。

地址欺骗：对这种攻击的防范采用扩展访问过滤列表方式，凡是从其他网段进来的数据包，如果其源地址不是来自该网段的合法地址，就抛弃该数据包。

端口扫描：对这种攻击的防范采用扩展访问列表方式，拒绝非授权网络访问特定的网络服务。

否认服务：对于洪水连接攻击我们采用 TCP 拦截技术，对一个主机的访问限制在一个可接受范围内，对于超过的可按几种设定方式丢弃连接。对于报文注入，Cisco PIX 防火墙产品是一种基于状态的包过滤产品，本身能很好的防范报文注入攻击。

应用层攻击：改进、替换具有安全漏洞的应用服务器。

特洛伊木马：对于这种攻击方式，首先应该教育公司职员不要运行不明来源的程序，避免内部主机被攻破，一旦内部主机被攻破，攻击者就可以以被攻破主机为落脚点，对内部所有主机进行攻击。对 Java Applet 和 Active-X 的防范采用员工教育方式，教育职员不要访问不明站点，尽量在浏览器中关闭 JavaApplet 和 Active-X 功能。

2.3.2 VPN 路由器

- 采用 Cisco Router 进行 IP 数据包过滤，安全 VLAN 子网划分
- 作为 VPN 配置路由使用，可方便进行安全访问的划分
- 结合 PIX 防火墙、NetRanger 入侵检测系统和 NetSonar 安全扫描程序三者配合，最大限度地保证了高校 VPN 的可靠性和安全性

2.3.3 IDS 入侵检测

入侵检测 (eTrust Intrusion Detection 简称 eID) 提供了全面的网络保护功能，其内置主动防御功能可以防止破坏的发生。这种高性能且使用方便的解决方案在单一软件包中提供了最广泛的监视、入侵和攻击探测、非法 URL 探测和阻塞、警告、记录和实时响应。

- 网络访问控制

入侵检测 (eTrust Intrusion Detection) 使用基本规则定义可以访问特定网络资源的用户，从而确保只对网络资源进行授权访问。

- 高级反病毒引擎

能够探测包含计算机病毒的网络流量的病毒扫描引擎。它可以防止用户在不知情的情况下下载受病毒感染的文件。从 CA web 站点可以得到最新和更新后的病毒特征码。

- 全面的攻击模式库

入侵检测 eID 可以自动探测来自网络流量的攻击模式（即使是正在进行中的攻击）。定期更新的攻击模式库 - 可以从 CA web 站点获得 - 能够确保入侵检测保持最新。

- 包检测技术

入侵检测 eID 在隐蔽模式下工作，攻击者是察觉不到的。因为黑客不知道他们正在被监视，因此通常在未察觉的情况下被捕获。

- URL 阻塞

管理员可以指定不允许用户访问的 URL，从而防止了非工作性 Web 冲浪。

- 内容扫描

管理员通过入侵检测 eID 可以定义策略对内容进行检查。这可以防止在没有授权的情况下通过电子邮件或 Web 发送敏感数据。

- 网络使用情况记录

入侵检测 eID 允许网络管理员跟踪最终用户、应用程序等的网络使用情况。它有助于改进网络策略规划和提供精确的网络收费。

- 集中化监控

网络管理员可以从本地或远程监控运行入侵检测 (eTrust Intrusion Detection) 的一个或多个站，在不同网络段（本地或远程）上安装了受中央站控制的入侵检测 (eTrust Intrusion Detection) 代理后，管理员可以根据收集到的合并信息查看报警和生成报告。

- 远程管理

远程用户可以使用 TCP/IP 或者调制解调器连接访问运行入侵检测 (eTrust Intrusion Detection) 的站。在连接后，根据入侵检测 (eTrust Intrusion Detection) 管理员定义的权限，用户可以查看和监控入侵检测 (eTrust Intrusion Detection) 数据、更改规则以及创建报告。

- 入侵记录和分析

入侵检测 (eTrust Intrusion Detection) 为捕获信息和进行分析提供了全面的系统功能。在安装软件并指定归档地点后，用户可以定义在档案中记录会话的规则。然后用户可以通过浏览器过滤、排序和查看归档信息，并创建详细的报告。

入侵检测 eID 代表了最新一代高校网络保护技术，具有前所未有的访问控制、用户透

明性、高性能、灵活性、适应性及易用性等。它提供给高校一个易于部署的网络保护方案。

2.3.4CA 认证与 SSL 加密

2.3.4.1CA 的作用

- 数字证书能为你做什么：

个人数字证书是网友进入 21 世纪的必需品。网上证券少不了它；网上缴款不能没有它；进入全球知名网站，更不得没有它。它简单易懂、安装容易，它比“卡”还要重要，是您身份的表征，网络新贵的识别证。现今不论 X、Y、Z 世代，您皮夹中至少必备四五张卡（提款卡、万事达卡、威士卡、会员卡、金卡、普卡、电话卡、保健卡...），因为目前是“卡”的时代。而在网际路上，您如果没有数字证书，不管您外表多 young、多炫，多酷，依旧是寸步难行。因为“一证在手，走遍天下”的时代已经到来。CA 为了更好地满足客户的需要，给客户提供更大的便利，设计开发的通用证书系统使得一证多用成为可能。

- 数字证书和电子教务的关系

电子教务正以不可逆转之势席卷全球的各行各业，但世界各地也面临着共同的阻碍——电子教务的安全问题，必须要采用先进的安全技术对网上的数据、信息发送方、接收方进行身份确认，以保证各方信息传递的安全性、完整性、可靠性和交易的不可抵赖性。以数字证书为核心的身份认证、数字签名、数字信封等数字加密技术是目前通用可行的安全问题解决方案。数字安全证书建立了一套严密的身份认证系统，可以确保电子教务的安全性。

- 信息的保密性

交易中的教务信息均有保密的要求。如信用卡的帐号和用户名被人知悉，就可能被盗用，订货和付款的信息被竞争对手获悉，就可能丧失商机。因此在电子教务的信息传播中一般均有加密的要求。

- 交易者身份的确定性

网上交易的双方很可能素昧平生，相隔千里。要使交易成功首先要能确认对方的身份，对商家要考虑客户端不能是骗子，而客户也会担心网上的商店不是一个玩弄欺诈的黑店。因此能方便而可靠地确认对方身份是交易的前提。对于为顾客或用户开展服务的银行、信用卡公司和销售商店，为了做到安全、保密、可靠地开展服务活动，都要进行身份认证的工作。对有关的销售商店来说，他们对顾客所用的信用卡的号码是不知道的，商店只能把信用卡的确认工作完全交给银行来完成。银行和信用卡公司可以采用各种保密与识别方法，确认顾客的身

份是否合法，同时还要防止发生拒付款问题以及确认订货和订货收据信息等。

- 不可否认性

由于商情的千变万化,交易一旦达成是不能被否认的。否则必然会损害一方的利益.例如订购黄金,订货时金价较低,但收到订单后,金价上涨了,如收单方能否认受到订单的实际时间,甚至否认收到订单的事实,则订货方就会蒙受损失。因此电子交易通信过程的各个环节都必须是不可否认的。

- 不可修改性

交易的文件是不可被修改的,如上例所举的订购黄金。供货单位在收到订单后,发现金价大幅上涨了,如其能改动文件内容,将订购数 1 吨改为 1 克,则可大幅受益,那么订货单位可能就会因此而蒙受损失。因此电子交易文件也要能做到不可修改,以保障交易的严肃和公正。

2.3.4.2CA 系统简介

人们在感叹电子教务的巨大潜力的同时,不得不冷静地思考,在人与人不见面的计算机互联网上进行交易和作业时, 怎样才能保证交易的公正性和安全性,保证交易方身份的真实性。国际上已经有比较成熟的安全解决方案,那就是建立安全证书体系结构。数字安全证书提供了一种在网上验证身份的方式。安全证书体制主要采用了公开密钥体制,其它还包括对称密钥加密、数字签名、数字信封等技术。

我们可以使用数字证书,通过运用对称和非对称密码体制等密码技术建立起一套严密的身份认证系统,从而保证:信息除发送方和接收方外不被其它人窃取;信息在传输过程中不被篡改;发送方能够通过数字证书来确认接收方的身份;发送方对于自己的信息不能抵赖。

系统特性

- 高强度加密和认证

Universal CA 采用基于 RSA 加密算法的公钥体系加密和认证,可以生成 512、768、1024 位三种不同密钥的长度的证书,确保证书的安全性和可靠性。

多种生成证书的方法

由用户的请求文件生成证书。

在服务器端由管理员为用户生成证书。

利用已有的数据库为用户生成证书。Universal CA 可以以上述三种方法生成证书,使用户应用极为方便。

支持国际互联网

Universal CA 发放的证书不依赖于固定的内部用户，只需一个 Email 地址即可实现证书的申请及应用，因此具有广泛的应用性。

具有同其他系统交换数据的能力

Universal CA 后台应用了东大阿尔派自主知识产权的数据库 Oopenbase 可以实现证书的海量管理，并具有同其他系统交换数据的能力，这使得系统具有良好的开放性与通用性。

易使用、功能强

Universal CA 运行在 Windows 环境下,将各种复杂操作屏蔽于后台，前台界面简单，且支持请求、证书的批量操作，以及可以实现过期证书的自动撤消。

CA 机构，又称为证书授证(Certificate Authority)中心，作为电子教务交易中受信任和具有权威性的第三方，承担公钥体系中公钥的合法性检验的责任。CA 中心为每个使用公开密钥的客户发放数字证书，数字证书的作用是证明证书中列出的客户合法拥有证书中列出的公开密钥。CA 机构的数字签名使得第三者不能伪造和篡改证书。它负责产生、分配并管理所有参与网上信息交换各方所需的数字证书，因此是安全电子信息交换的核心。

为保证客户之间在网上传递信息的安全性、真实性、可靠性、完整性和不可抵赖性，不仅需要对客户的身分真实性进行验证，也需要有一个具有权威性、公正性、唯一性的机构，负责向电子教务的各个主体颁发并管理符合国内、国际安全电子交易协议标准的安全证书。

数字证书管理中心是保证电子教务安全的基础设施。它负责电子证书的申请、签发、制作、废止、认证和管理，提供网上客户身份认证、数字签名、电子公证、安全电子邮件等服务等业务。

CA 为电子教务服务的证书中心，是 PKI (Public Key Infrastructure) 体系的核心。它为客户的公开密钥签发公钥证书、发放证书和管理证书，并提供一系列密钥生命周期内的管理服务。它将客户的公钥与客户的名称及其他属性关联起来，为客户之间电子身份进行认证。证书中心是一个具有权威性、可信赖性和公证性的第三方机构。它是电子教务存在和发展的基础。认证中心在密码管理方面的作用如下：

自身密钥的产生、存储、备份/恢复、归档和销毁

从根 CA 开始到直接给客户发放证书的各层次 CA，都有其自身的密钥对。CA 中心的密钥对一般由硬件加密服务器在机器内直接产生，并存储于加密硬件内，或以一定的加密形式存放于密钥数据库内。加密备份于 IC 卡或其他存储介质中，并以高等级的物理安全措施保护起来。密钥的销毁要以安全的密钥冲写标准，彻底清除原有的密钥痕迹。需要强调的是，

根 CA 密钥的安全性至关重要，它的泄露意味着整个公钥信任体系的崩溃，所以 CA 的密钥保护必须按照最高安全级的保护方式来进行设置和管理。

为认证中心与各地注册审核发放机构的安全加密通信提供安全密钥管理服务。在客户证书的生成与发放过程中，除了有 CA 中心外，还有注册机构、审核机构和发放机构（对于有外部介质的证书）的存在。行业使用范围内的证书，其证书的审批控制，可由独立于 CA 中心的行业审核机构来完成。CA 中心在与各机构进行安全通信时，可采用多种手段。对于使用证书机制的安全通信，各机构（通信端）的密钥产生、发放与管理维护，都可由 CA 中心来完成。

确定客户密钥生存周期，实施密钥吊销和更新管理。每一张客户公钥证书都会有有效期，密钥对生命周期的长短由签发证书的 CA 中心来确定。各 CA 系统的证书有效期限有所不同，一般大约为 2~3 年。

密钥更新不外为以下两种情况：密钥对到期、密钥泄露后需要启用新的密钥对（证书吊销）。密钥对到期时，客户一般事先非常清楚，可以采用重新申请的方式实施更新。

采用证书的公钥吊销，是通过吊销公钥证书来实现的。公钥证书的吊销来自于两个方向，一个是上级的主动吊销，另一个是下级主动申请证书的吊销。当上级 CA 对下级 CA 不能信赖时（如上级发现下级 CA 的私钥有泄露的可能），它可以主动停止下级 CA 公钥证书的合法使用。当客户发现自己的私钥泄露时，也可主动申请公钥证书的吊销，防止其他客户继续使用该公钥来加密重要信息，而使非法客户有盗取机密的可能。一般而言，在电子教务实际应用中，可能会较少出现私钥泄露的情况，多数情况是由于某个客户由于组织变动而调离该单位，需要提前吊销代表高校身份的该客户的证书。

提供密钥生成和分发服务。CA 中心可为客户提供密钥对的生成服务，它采用集中或分布式的方式进行。在集中的情形下，CA 中心可使用硬件加密服务器，为多个客户申请成批的生成密钥对，然后采用安全的信道分发给客户。也可由多个注册机构（RA）分布生成客户密钥对并分发给客户。

提供密钥托管和密钥恢复服务。CA 中心可根据客户的要求提供密钥托管服务，备份和管理客户的加密密钥对。当客户需要时可以从密钥库中提出客户的加密密钥对，为客户恢复其加密密钥对，以解开先前加密的信息。这种情形下，CA 中心的密钥管理器，采用对称加密方式对各个客户私钥进行加密，密钥加密密钥在加密后即销毁，保证了私钥存储的安全性。密钥恢复时，采用相应的密钥恢复模块进行解密，以保证客户的私钥在恢复时没有任何风险和不安全因素。同时，CA 中心也应有一套备份库，避免密钥数据库的意外毁坏而无法恢复

客户私钥。

其他密钥生成和管理、密码运算功能。CA 中心在自身密钥和客户密钥管理方面的特殊地位和作用，决定了它具有主密钥、多级密钥加密密钥等多种密钥的生成和管理功能。

对于为客户提供公钥信任、管理和维护整个电子教务密码体系的 CA 中心来讲，其密钥管理工作是一项十分复杂的任务，它涉及到 CA 中心自身的各个安全区域和部件、注册审核机构以及客户端的安全和密码管理策略。

2.3.4.3 SSL 加密

SSL 是一种国际标准的加密及身份认证通信协议，您用的浏览器就支持此协议。SSL (Secure Sockets Layer) 最初是由美国 Netscape 公司研究出来的，后来成为了 Internet 网上安全通讯与交易的标准。SSL 协议使用通讯双方的客户证书以及 CA 根证书，允许客户/服务器应用以一种不能被偷听的方式通讯，在通讯双方间建立起了一条安全的、可信任的通讯通道。它具备以下基本特征：信息保密性、信息完整性、相互鉴定。

2.3.4.3.1 SSL (Secure Socket Layer)：安全套接层协议

SSL 协议是由 Netscape 首先发表的网络资料安全传输协定,其首要目的是在两个通信间提供秘密而可靠的连接。该协议由两层组成，底层是建立在可靠的传输协议（例如：TCP）上的是 SSL 的记录层，用来封装高层的协议。SSL 握手协议准许服务器端与客户端在开始传输数据前，能够通过特定的加密算法相互鉴别。SSL 的先进之处在于它是一个独立的应用协议，其它更高层协议能够建立在 SSL 协议上。

目前大部分的 Web Server 及 Browser 大多支持 SSL 的资料加密传输协定。因此，可以利用这个功能，将部分具有机密性质的网页设定在加密的传输模式，如此即可避免资料在网络上传送时被其他人窃听。

SSL 是利用公开密钥的加密技术（RSA）来作为用户端与主机端在传送机密资料时的加密通讯协定。目前，大部分的 Web Server 及 Browser 都广泛使用 SSL 技术。

对消费者而言，SSL 已经解决了大部分的问题。但是，对电子教务而言问题并没有完全解决，因为 SSL 只做能到资料保密，厂商无法确定是谁填下了这份资料，即使这一点做到了，还有和银行清算的问题。

SSL 是目前在网上购物网站中最常使用的一种安全协议，它主要的设计目的在于确保信

息在网际网络上流通的安全性，让主从式结构的应用程序（如浏览器与 web 服务器）能够安全地进行沟通。当然，这里的安全指的是信息不被伪造，不被网络上的黑客中途拦劫解毒及擅自更改。

SSL 的协议中结合了许多密码学的技术，其中包括：

1. 信息加解密。
2. 数字签名与签证技术。

除此之外，在进行安全联机之前，SSL 会先采取“握手”（Handshaking）的动作，以确保网络上通信的双方都能够按部就班的根据预定步骤建立起两者之间的安全通道。

2.3.4.3.2 SSL 可以提供以下三种安全防护：

数据的机密性与完整性：主要是通过数据的加解密来实现。

1. 服务器端的个体识别服务：利用服务器的数字证书来验证商店的资格，这是必要的手续，如此我们才能保证商店的有效性。

2. 客户端的个体识别服务：同样是通过客户自己的数字证书来完成。但这个服务并不是必要的，可根据需求来设置。

以网上购物的例子来说，为了不让网络上的第三者看到我们的信用卡数据，因此必须先将数据加密之后再传送，而当数据到达对方服务器时再将数据解密，同时检查数据是否有被他人更改过，如果发现任何的错误，那么这份数据就不会被接受。

3. 除此之外，SSL 也利用数字证书的方法类确定商店的资格。因此商家如果想要提供网上交易的服务，他必须先向认证中心是、提出商店的合法证明，如营业执照，负责人等等（不同的认证中心所要求的文件可能不同）。检查通过后才能取得数字证书。

SSL 内部使用的是 RSA 公司所授权的公开金钥加密法，服务器必须申请属于自己的数字证书，加装到服务器中作为识别之用。如此一来，一个加装 SSL 的服务器便可以与支持 SSL 的浏览器相互传送机密数据了，即使是 internet 也不用担心。

2.3.4.3.3 SSL 协议运行的基点是商家对客户信息保密的承诺。

SSL 协议有利于商家而不利于客户。客户的信息首先传到商家，商家阅读后再传到银行，这样，客户资料的安全性便受到威胁。商家认证客户是必要时，但整个过程中缺少了客户对商家的认证。在电子教务的开始阶段，由于参与电子教务的公司大都是一些大公司，信誉较

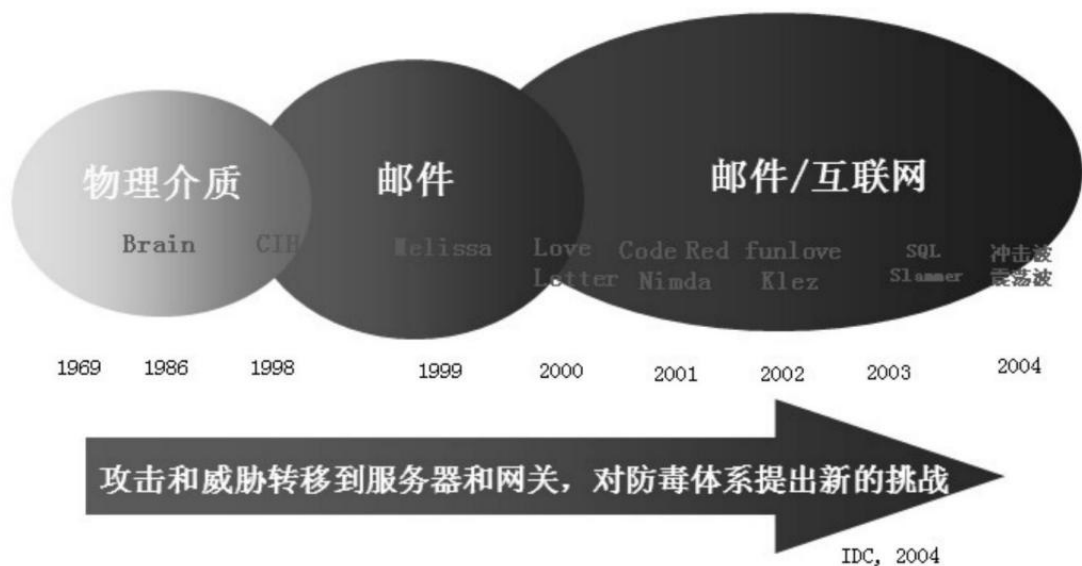
高，这个问题没有引起人们的重视。随着电子教务参与的厂商迅速增加，对厂商的认证问题越来越突出，SSL 协议的缺点完全暴露出来。SSL 协议逐渐被新的 SET 协议所取代。目前我国开发的电子支付系统，无论是中国银行的长城卡电子支付系统，还是上海长途电信局的网上支付系统，均没有采用 SSL 协议。主要原因就是无法保证客户资金的安全性。

2.3.5防病毒系统

计算机病毒是附属在其它文件上的一种程序，可以自行复制。计算机病毒十分有害，如果没有检测和防护，用户经常不知道自己感染上病毒，直到病毒发作并产生危害。病毒中的破坏进程可以格式化硬盘、破坏分区表或占用计算机资源。

病毒十分流行。事实上，目前世界上已存在超过 10,000 种，计算机存在病毒的比率高达 35-85%，中国、香港、台湾为高发区。尽管病毒在 Apple 机和 PC 上都存在，但在 PC 系统中更为广泛，这是因为 MS-DOS 结构使用中断和向量表，编写病毒相对容易。

清除病毒十分困难。据分析，对于数据丢失，病毒发作的损失在 US\$2000-50,000，而恢复数据的代价十分昂贵甚至不可能，而且清除后病毒还可能再感染。因此，每个用户有 50% 的可能感染病毒并招致损失。大的计算机网络几乎必然被病毒感染。

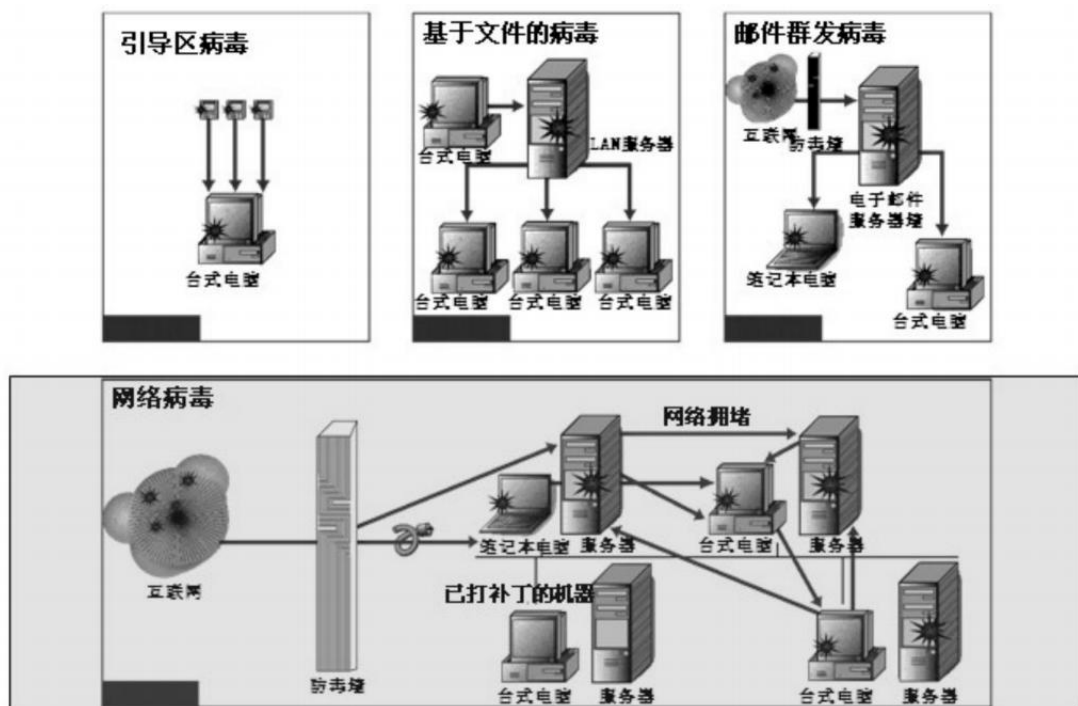


2.3.5.1病毒的类型

2.3.5.1.1 介质病毒

病毒可分为两类：文件型和引导型。文件型病毒驻留在另一个 .EXE 或 .COM 文件中，

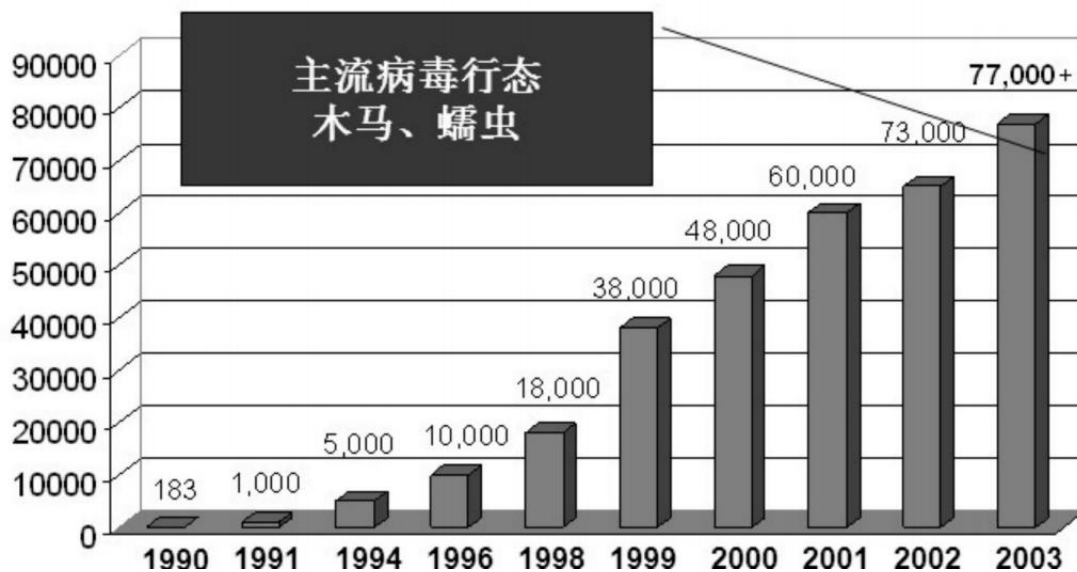
当文件执行时截取系统控制，并将自身附加到另外的文件上。引导型驻留在软盘或硬盘的引导区，在系统启动时装入内存，然后监视 DOS 中断并感染插在软驱中的磁盘。



有两种病毒不容易被检测：隐身病毒和多态病毒。隐身病毒使用 DOS 中断，并不断变换方式，避开文件大小监测。多态病毒目前很多，在传染时修改本身的版本，使根据模式扫描的病毒检测程序无能为力。

最初，大约 80% 的病毒是引导型病毒。随着 Internet 的普及，文件型病毒变得越来越多。另外，一种新型的文件病毒感染文档和图表的病毒，被称作宏病毒，使用文字处理器和表格中的编码，是目前最多的病毒。这种病毒通过电子邮件的附件快速传染，躲过了许多只检查 .EXE 和 .COM 文件的防病毒程序。

病毒数目增长趋势图 (1990- 04/2003)



2.3.5.1.2 网络病毒

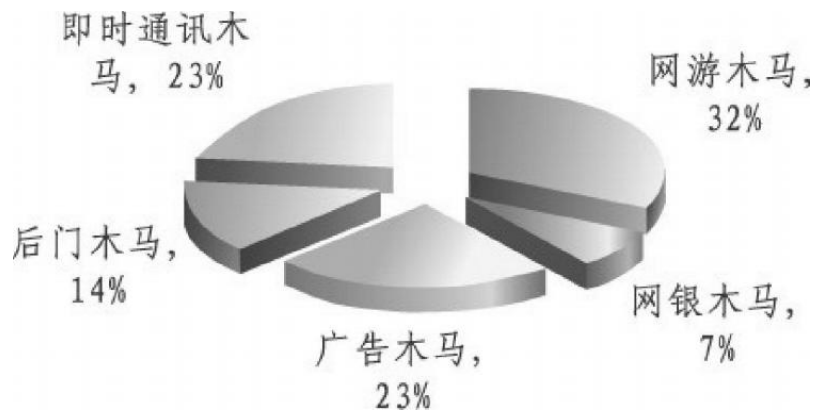
网络病毒的特性

- 通过攻击操作系统或应用软件的已知安全漏洞来获得控制权
- 在本地硬盘上并不留下文件
- 由于其在网络上进行扫描的动作，可能会引起严重的网络负载
- 如果攻击是属于常规的应用，例如 SQL, IIS 等就可能穿过防火墙

2.3.5.1.3 木马病毒

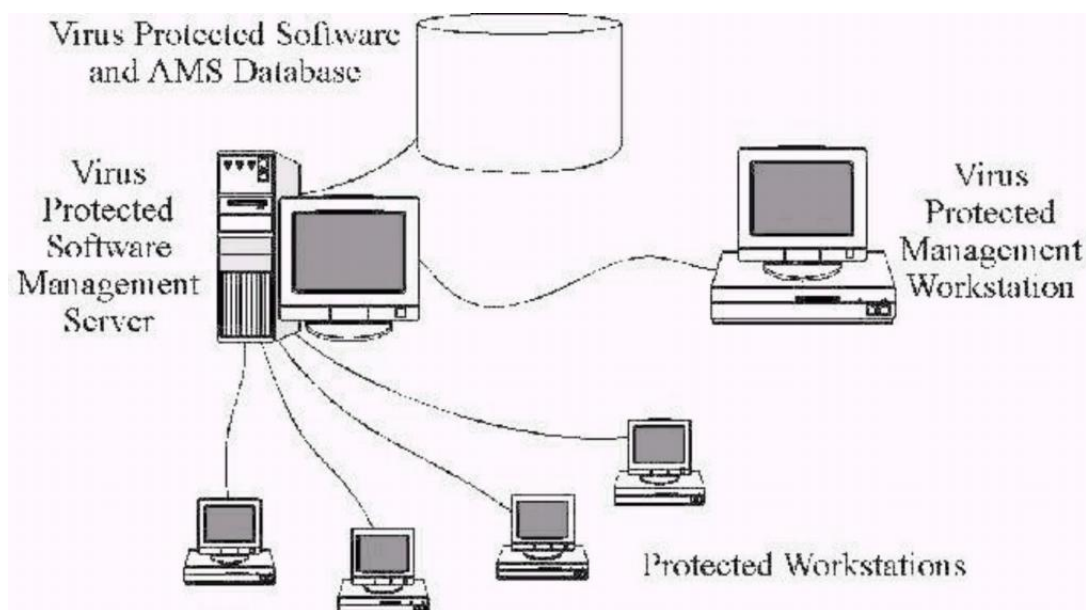
木马病毒有可能洗劫用户网上银行存款、造成网络游戏玩家装备丢失、被黑客利用执行不法行为等。如今，针对以上各种现象的危害越来越多，木马病毒已成为威胁数字娱乐的大敌。

根据木马病毒的特点与其危害范围来讲，木马病毒又分为以下五大类别：针对网游的木马病毒、针对网上银行的木马病毒、针对即时通讯工具的木马病毒、给计算机开后门的木马病毒、推广广告的木马病毒。



2.3.5.2 病毒的检测

客户端防病毒软件安装在客户计算机上，当用户启动计算机时或用户手动运行时检查硬盘或软盘。好的桌面产品使用多种检测方式，例如监视病毒的行为（如格式化硬盘）、根据已知病毒代码库比较文件、检查无法解释的文件大小改变等。

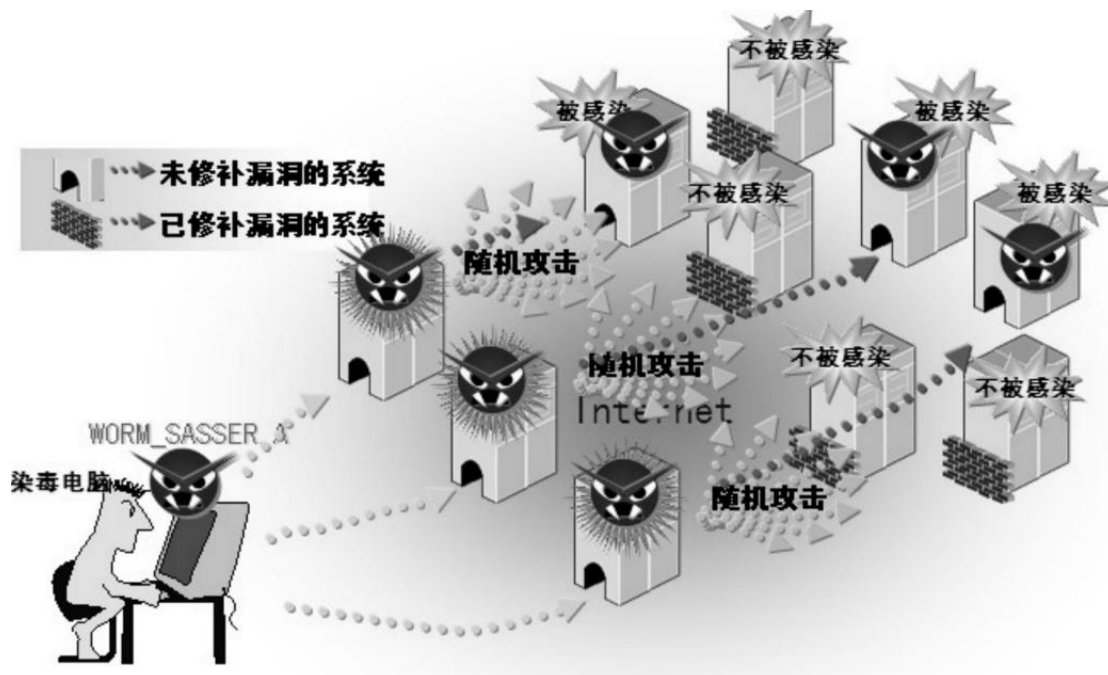


但是，客户端防病毒软件有一个致命弱点：只是在用户使用周期地检测病毒，对下载的、或其他方式传输的文件则不检测，而这些文件可能带有病毒。另外，每个客户端要同时安装防病毒软件，更新、维护十分麻烦。因此，出现了网络防病毒软件，驻留在网络服务器上，运行于 NetWare 或 Windows NT 环境，对通过服务器传递的文件病毒进行检测。

服务器防病毒软件比客户端防病毒软件效率提高了很多，可以集中管理病毒防范、经常扫描文件病毒，并及时更新病毒库。然而，文件服务器型防病毒软件也有一些缺点：很强的网络服务器防病毒功能，客户端则没有，对于不通过文件

服务器的文件型病毒，如从 Internet 下载的文件和电子邮件，则无法防护。其次，服务器防病毒软件不能扫描电子邮件附件上的病毒。这是因为在 LAN 中，电子邮件和附件被加密，只有附件在“另存为”在硬盘上时病毒扫描程序才启动，从而导致病毒扫描不及时、效率低。

随着 Internet 的普及，越来越多的高校、大学、政府和消费者共享文件、发送信息、通过网络交谈。最重要的两种方式是通过电子邮件和 FTP 交换邮件和文件。伴随而来的问题是许多病毒通过文件下载和电子邮件传播，而且传播的速度十分惊人。



本质上, Internet 成为传播病毒的电脑空间, 计算机系统管理员很少能控制网络用户下载带病毒的免费软件、共享软件或游戏。在公司内部网络上传输文件也不是没有风险, 因为存在附加在非可执行文件, 如 Word、Excel 或电子邮件上的病毒。

Internet 上的病毒不经过文件服务器, 因此服务器防病毒软件不起作用。许多网络都配置了防火墙, 可以拒绝没有授权的访问或阻止可能引起问题的外部用户访问内部网, 但防火墙无法防病毒。因此出现了新型的防病毒软件: 病毒墙 (Virus-Wall)。病毒墙驻留在 Internet 网关, 在病毒进入系统搞破坏前进行检测并清除。

2.3.5.3防病毒建议方案

由于在这次网站的建设中，服务器使用 Linux 操作系统。现在流行的病毒通常情况下只是针对 windows 操作系统中。因此，系统在针对病毒方面是相对安全的。

2.3.6网站监控与恢复系统

近几年，随着 Internet 的普及，网络上发生的攻击事件越来越普遍，一个普通人员在 Internet 上可以很容易的找到攻击工具，然后攻击网站。网站被篡改的事件时有发生。因此，对网站进行保护是非常必要的。

网站实时监控与恢复系统是一种网站的灾难恢复技术，它的立足点是在其它的网站安全措施，如使用防火墙、加强 Web 服务器软件自身的安全性、清查不安全的 CGI 程序都失败，网页文件被黑客破坏的情况下，网站文件系统的自动恢复问题。

2.3.7SAN 网络存储/备份/灾难恢复：

采用目前流行的群集技术 SAN 技术，将存储设备从传统的以太网中隔离出来，成为独立的存储域网络。完全采用光纤连接，保证了数据传输带宽达到 100MB/S。使大量的数据只是在服务器和存储设备之间流动，不占用网络带宽及服务器资源。建立远程备份中心，进行远程容灾备份，确保系统的数据安全。

3 业务网络安全设计

3.1 网络安全设计原则

- 防止来自外部的黑客攻击
- 防止来自内部的恶意攻击
- 网络资源访问控制
- 网络传输的实时监控

- 强大的安全审计
- 事件分析与告警

在本方案中，网络的对外出口处以及在总行和分行之间的连接都设置防火墙将是最理想的选择，外部网出口都配置防火墙，以及在总行与分行的业务网的连接处也配置防火墙，对外防止黑客入侵，对内以防止内部人员的恶意攻击或由于内部人员造成的网络安全问题。

本方案中主要用到 NetScreen-10 和 NetScreen-100，在总行与分行连接点采用 NetScreen-100 作为防火墙，同时在重要的业务连接点采用 NetScreen 独特的多机备份技术用两台作为热备份，保证整个系统的网络安全。在分行采用 NetScreen-10 防火墙，为连接各终端以及服务器节点提供安全防护。

3.2 系统的安全设计

3.2.1 威胁及漏洞

作为一个网络营销和管理系统，由于涉及信息的敏感性自然会成为内部和外部黑客攻击的目标，当前面临的主要风险和威胁有：

非法访问：一个远程互连的网络营销和管理系统。现有网络系统利用操作系统网络设备进行访问控制，而这些访问控制强度较弱，攻击者可以在任一终端利用现有的大量攻击工具发起攻击；由于整个网络通过公用网络互连同样存在链接终端进行攻击的可能；另一方面开发的很多增值业务、代理业务，存在大量与外界互连的接口这些接口现在没有强的安全保护措施存在外部网络通过这些接口攻击，可能造成巨大损失。

窃取 PIN/密钥等敏感数据：系统目前没有使用任何的数据加密技术，因此安全的关键是对数据进行加密保护，可以使用密钥加密技术，从而避免主机中敏感数据的丢失。

假冒终端/操作员：网络中存在大量远程终端通过公网与前置机相连，因此，网络服务器存在大量安全隐患。现有操作员身份识别唯一，但口令的安全性非常弱因此存在大量操作员假冒的安全风险。

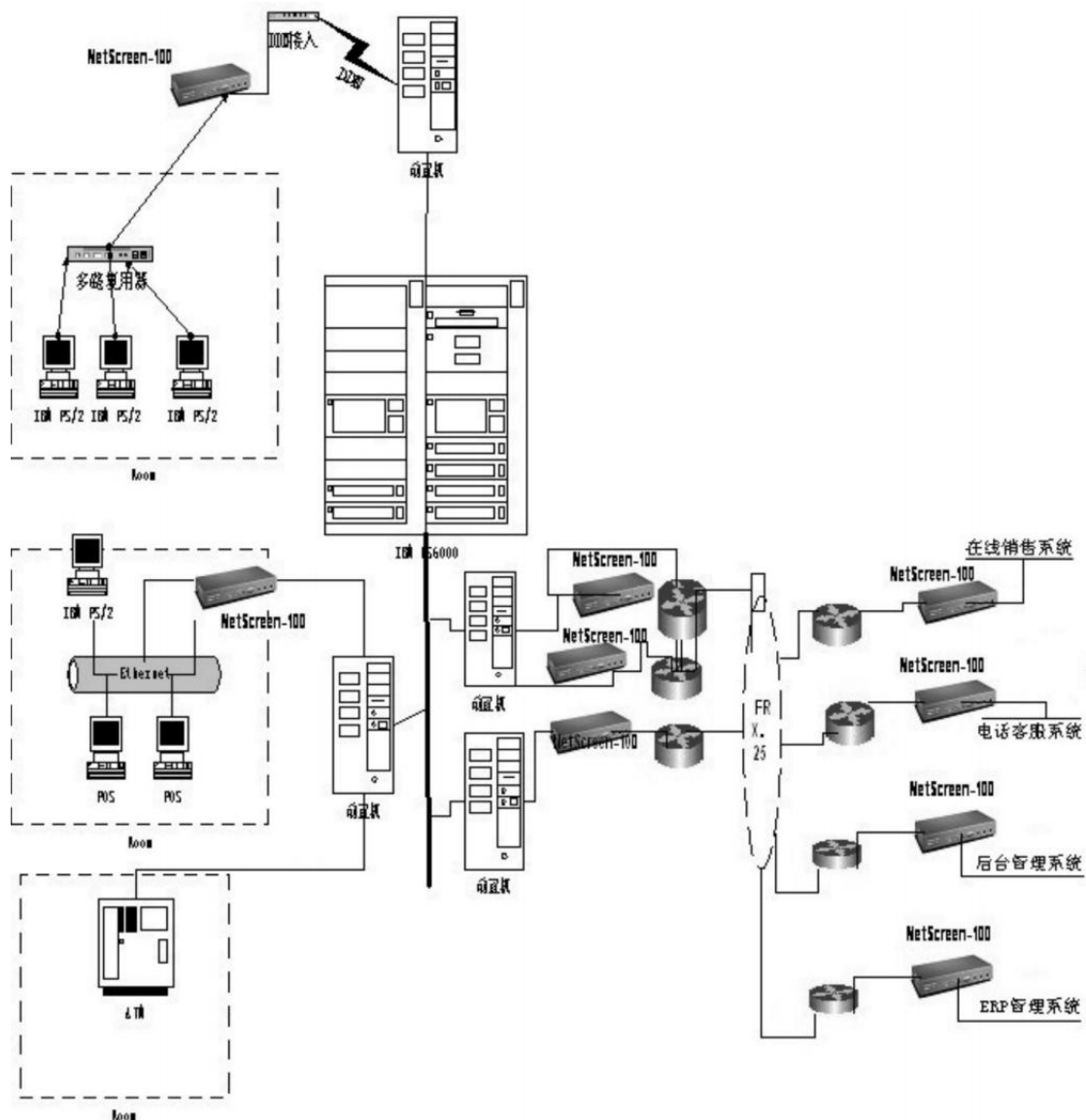
截获和篡改传输数据：现有网络系统通过公网传输大量的数据没有加密，

由于信息量大且采用的是开放的 TCP/IP，现有的许多工具可以很容易的截获、分析甚至修改信息，主机系统很容易成为被攻击对象。

其他安全风险：主要有病毒、系统安全（主要有操作系统、数据库的安全配置）以及系统的安全备份等。

3.2.2 计说明

在对 网络结初步分析后我们提出以下安全措施来安全处理。



图四、 网络安全防火墙保护总体示意图

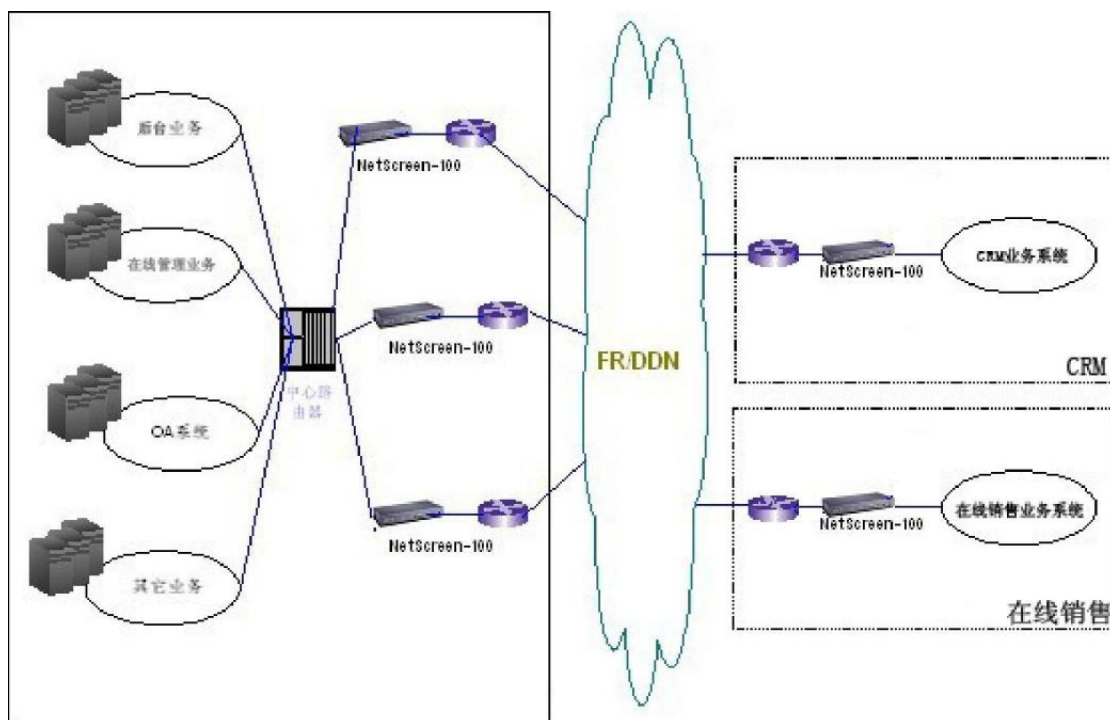
通常电子教务，也包括 网络中用到的通信线路涉及到：X.25、FR、DDN、ISDN、拨号等通信接口和协议，因此，最佳的方案是在网络层上采用先进的 NETSCREEN

网络安全技术，以有效的阻止外来的攻击和保证业务数据在公网上的安全传输，同时在应用层上提供对敏感数据加密消息进行完整性鉴别及密钥管理因此可以通过各级节点配备 NETSCREEN100 来保证 IP 包的机密性。在业务系统中为了保护用户敏感信息防止信息被非法篡改实现对业务数据加密、身份认证等安全功能。

3.3 系统的安全设计

3.3.1 各业务系统的分离

现有网络上部署了多种应用，包括 ERP 系统、CRM 系统、内部 OA 系统、在线销售系统、在线销售管理系统等一系列的业务系统，这些业务系统之间存在一定的联系，但又要防止侵权使用资源，特别是在线销售系统与 ERP 和管理系统，所以各业务系统的隔离是保障业系统安全的一个重环节。



图五、各业务系统隔离方案

在高校内部，各业务系统使用的主机 IP 地址要有严格的区分，为建立访问控制机制为核心的隔离措施提供方便。

在局域网当中，通过具有第二层（支持 VLAN 划分，VLAN 为虚拟局域网）

或三层交换的交换机（支持VLAN划分及网内路由），划分业务系统在一个VLAN范围内，OA系统在另的一个VLAN范围内，各VLAN之间不直接交换数据，在必要的情况下，采取一定技术实现部分数据交换。

在各个业务内可以象总部一样，通过VLAN的划分，划分业务VLAN和OA VLAN，隔离办公网与业务网。

VLAN技术是近阶段较流行的局域网隔离技术，在一套硬件网络环境内运行许多个（视交换机支持数据）完全独立、互不通信的局域网，看起来就象两个完全分隔开的局域网系统。

使用VLAN划分开之后，当网络信息通过路由器后，MAC地址信息都会被路由器的MAC地址所替代，VLAN的隔离作用消失。就是说总行内和分行内划分出的业务VLAN和OAVLAN，在局域网内根据路由策略，及对对MAC地址的判别，可使隔离的业务VLAN和OAVLAN按需实现通讯。

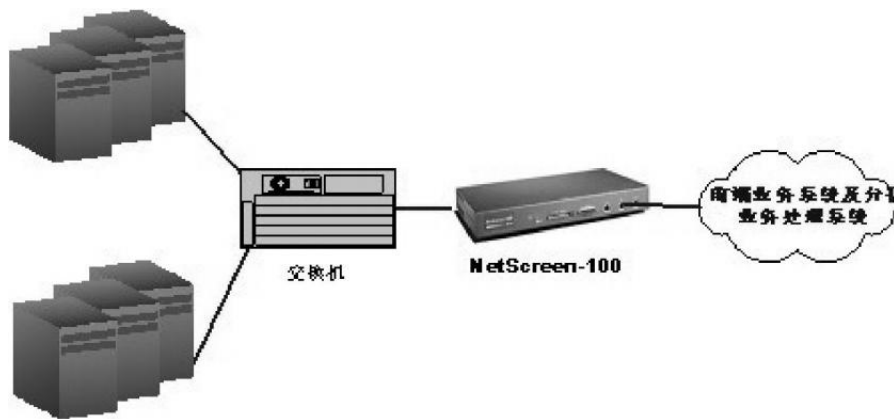
远程通讯是通过路由器的同一个广域网端口，经过广域网传输后的业务网和OA网是无法通过VLAN技术加以隔离的。如不加以控制，总行的业务网和OA网虽然不能互相访问，但总行的业务网可以和分行的OA网相互通讯，因此必须建立一定的访问控制加以限制。因此要在路由器之后配备防火墙，执行访问控制功能，分划业务网与OA网的通讯界线。

3.3.2敏感数据区的保护

在线销售和ERP系统内存在许多敏感数区域（如业务系统主机等），这些敏感的数据区域要求严格保密，对访问的权限有严格的限制，但所有的主机处于同一个网络系统之内，如不加以控制，这样很容易造成网内及网外的恶意攻击，所以在这些数据区域的出入口要加以严格控制，在这些地方放置防火墙，防火墙执行以下控制功能。

1. 对来访数据包进行过滤，只允许验证合法主机数据包通过，禁止一切非授权主机访问。
2. 对来访用户进行验证。防上非法用户侵入。
3. 运用网络地址转换及应用代理使数据存储区域与业务前端主机隔离，业务前端主机不直接与数据存储区域建立网络连接，所有的数据访问通过防火墙的

应用代理完成，以保证数据存储区域的安全。



敏感数据区保护方案

3.3.3 通讯线路数据加密

在广域网传输系统中，广泛应用到帧中继、X.25、DDN、PSTN 等等之类的通用线路，但这些线路大多数都是由通讯公司提供，与许多用户在一套系统上使用他们的业务，由于这些线路都是暴露在公共场所，这样很容易造成数据被盗。传输数据当中如果不进行数据加密，后果可想而知。所以对数据传输加密这是一非常重要的环节。

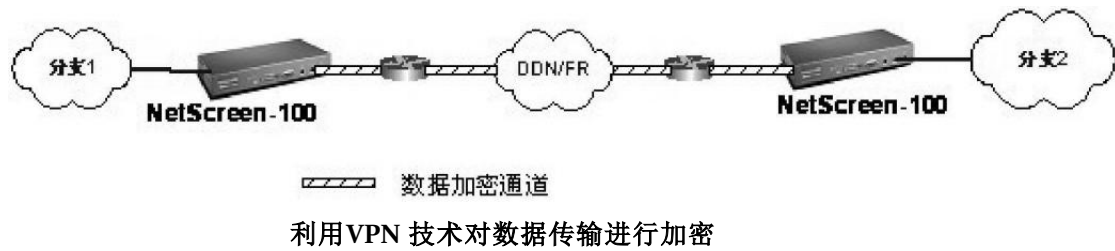
对网络数据加密大致分为以下几处区域：

1. 层加密

层加密，应用程序对外界交换数据时进行数据加密。主要优点是使用方便、网络中数据从源点到终点均得到保护、加密对网络节点透明。缺点是某些信息必须以明文形式传输，容易被分析。此种加密已被广泛应用于各应用程序当中，并有相应的标准。

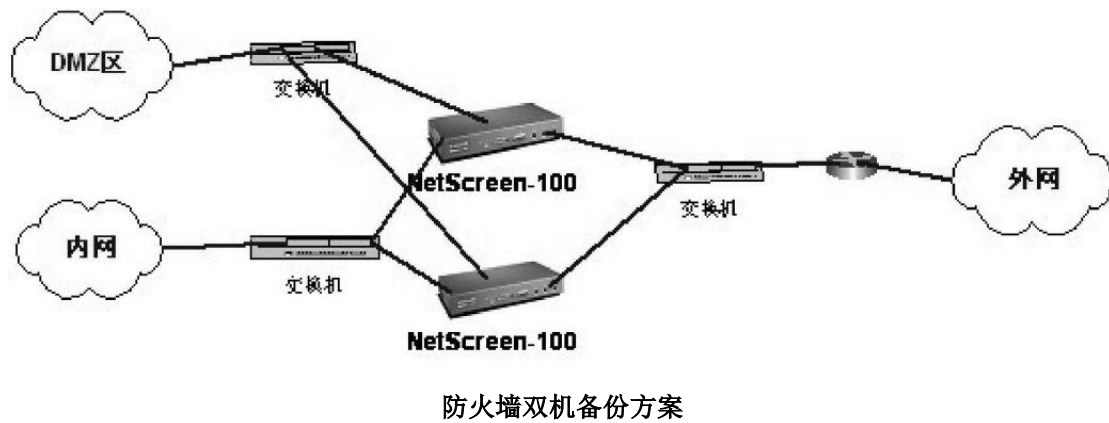
2. 网络层的数据加密

在 的各个业务分支服务器之间建议采用 VPN 加密技术进行数据加密。VPN 是通过标准的加密算法，对传输数据进行加密，在公用网上建立数据传输的加密“隧道”。加密实现是在 IP 层，与具体的广域网协议无关，也就是说适应不同的广域网信道（DDN、X.25、帧中继、PSTN 等）。由于 VPN 技术已经拥有标准，因此所有的 VPN 产品可以实现互通。



3.3.4 防火墙自身的保护

要保护网络安全，防火墙本身要保证安全，由于系统供电、硬件故障等特殊情况的发生，使防火墙系统瘫痪，严重阻碍网络通讯，网络的安全就无法保证，所以要求防火墙有冗余措施及足够防攻击的能力。

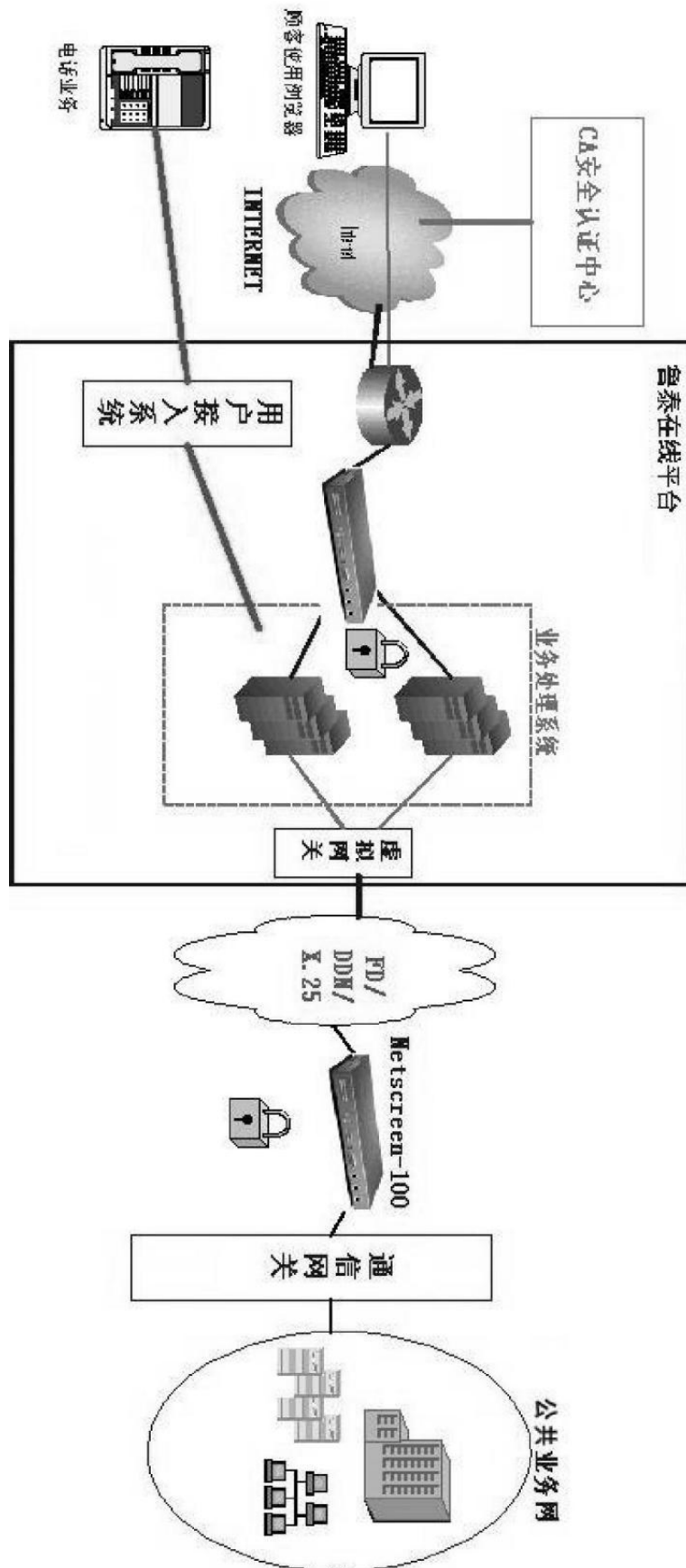


3.3.5 网络安全设计

目前，在发达国家，电子教务发展十分迅速，电子教务技术已趋成熟，通过 Internet 进行交易也已逐渐成为潮流，全球电子教务的应用也已拉开帷幕。网上银行在电子教务中的一个具体应用，自 1995 年 10 月，全球第一家网上银行开张，到 1996 年 8 月，已有 600 多家银行上网，提供服务信息甚至在网上提供全套金融服务。1997 年，研究高校对 17 个国家的 130 家大型金融机构调查，发现 13% 已经在网上与客户直接交易。而 1999 年，60% 在网上营业。

在我国，Internet 的应用发展也很快，而且金融通讯网络正在迅速扩大，我国的银行金融系统，以银行金融网络为基础，以现代支付系统为龙头的金融电子化工程已经全面铺开，进展很快。建设网上银行已是大势所趋，而其中非常重要的一点就是整个系统的安全保证，包括数据的安全保证、交易的安全保证、支付的安全保证。现今有许多实现手段，以保证电子教务系统的安全运行，其中比较流行有如下几种：

- 电子教务系统防火墙
- 信息加密
- 身份认证
- 信息签名

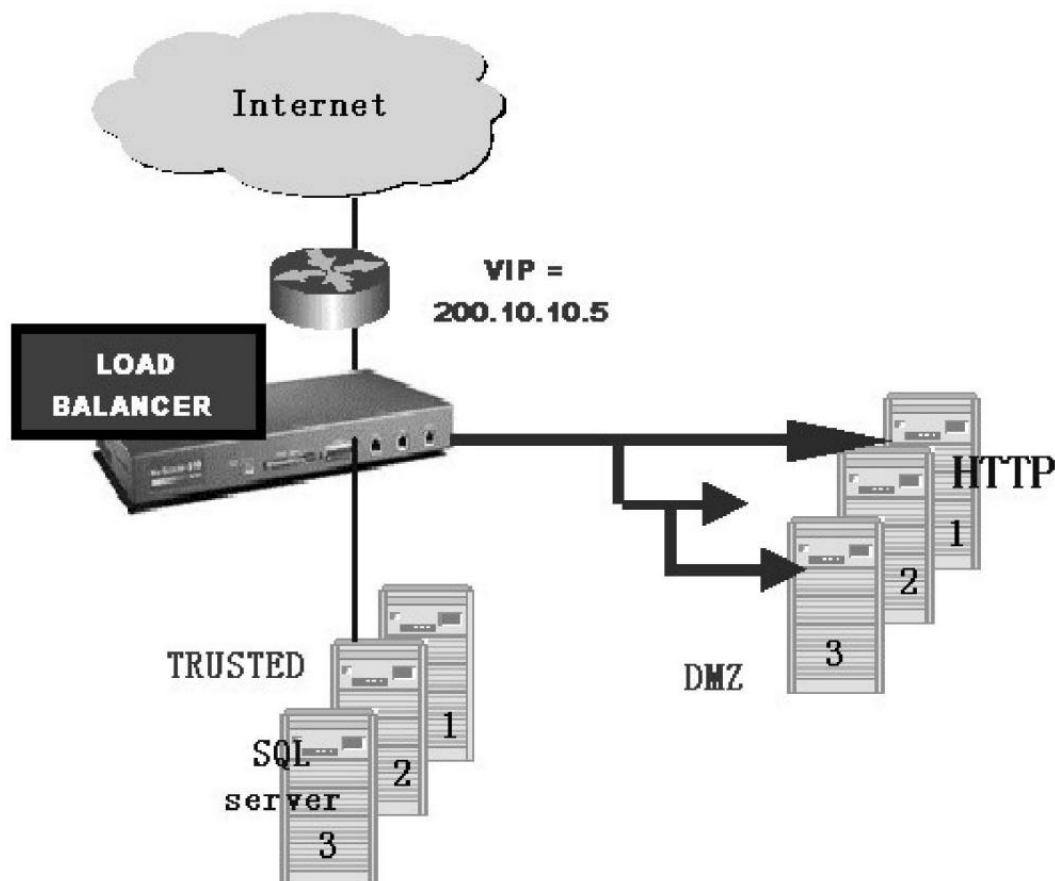


系统示意图

3.3.5.1设计说明:

通过在电子教务平台和 INTERNET 之间安装 NetScreen-100, 通过其基于状态检测包过滤, 能有效的将非法的数据包排除在防火墙以外, 通过 NAT (网络地址翻译), 将内部服务器 (如提供电子教务服务的服务器) 的 IP 地址转换成外部 IP 地址, 能有效的防止黑客通过各种手段来攻击或入侵内部的服务器。可以保证电子教务平台不受到入侵, 能够对所有的信息流封锁, 并且开放希望提供的服务。

Netscreen-100 可以设置虚拟 IP, 选择负载平衡算法, 如轮询、带优先级的轮询、最少连接数、带优先级的最少优先级等多种算法实现电子教务服务器的负载平衡。



负载平衡示意

可以将一个合法的外部 IP 地址映射给内部多台服务器的 IP, 由多台服务器

分担网络上访问服务器的流量。如上图中将一个 IP 地址：200.10.10.5 指定给 DMZ 区的多台服务器（各服务器 IP 不相同），以此来分担整个网络的流量，以保证网上银行电子教务平台能够安全、快速、稳定的运行。

同样在电子教务平台和高校管理网间也安装 Netscreen-100，确保数据源控制，并且开启防火墙的 VPN 功能，采用 IPSEC 协议，用点对点的 DES 和三倍 DES 加密，对传输数据加密，并且支持人工、自动 ISAKMP 密钥管理，保证通过 Internet 进行教务活动不受破坏。