银行系统中间业务安全解决方案

The intermediate business security solution of the Bank System

封振江　(建行沧州分行科技处)

摘要：怎样将银行和相关单位的业务进行安全有效的链接，已经成为当今银行系统优化的一个关键问题，本文就如何实现银行业务的特性作出了详细的阐述。

关键词：RSA 公钥密码体制 SSL 加密传输 数字签字

1　引言

银行系统为了更好的为广大用户服务，充分利用银行储蓄所多、服务面广的特点，开展了很多代理业务，如代收电话费、代收房租、代收水费、代收电费、代收税款、代收书报费、代收保险费、代收交通罚款等业务。这样，既方便了用户，又节省了各业务单位的工作人员的数量和工作压力，同时银行系统也增加了收入，但随着计算机网络的发展，网络安全问题日益成为关键。如何将银行系统与其他业务单位系统的资源共享，同时保护双方系统和所有资源信息的安全，构建安全有效的防火墙系统已经成为迫在眉睫的问题。网络结构如图1所示。

1.1 主干网络的隔离与访问控制安全

在综合业务网络与网上银行业务网络之间、网上银行业务网络与国际互联网之间，设置分段式网络防火墙(包括分组过滤与应用代理)，实现不同业务网络间的相互隔离与访问控制。

(1) 过滤进、出网络的数据；

(2) 管理进、出网络的访问行为；

(3) 封堵某些禁止的业务；

(4) 记录通过防火墙的信息内容和活动，对网络攻击的检测和告警。

1.2 中间业务应用安全

(1) 建立中间业务网络的隔离机制，防止代理方机侵入银行内部计算机网络；

(2) 利用SSL等协议建立交易双方的认证机制，采用数字签名保证交易的不可抵赖性和交易数据的完整性；

(3) 建立安全审计机制，记录双方的交易过程与行为。

2　Internet 业务网络安全

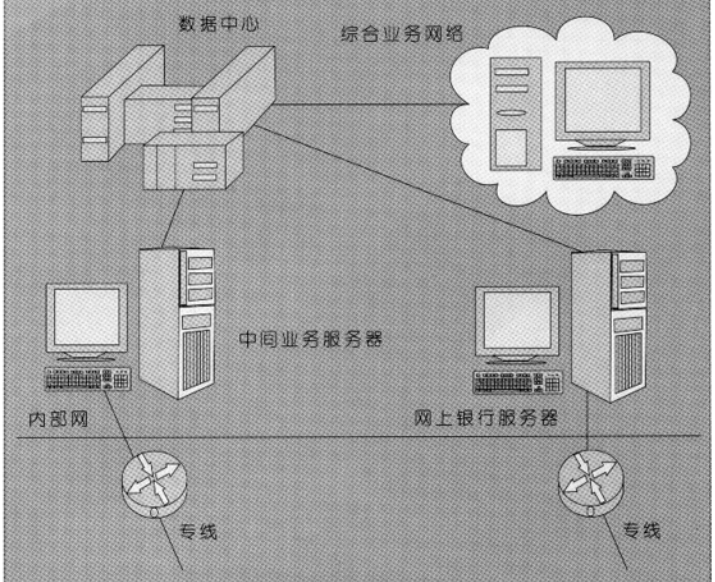
2.1 网上银行的交易安全

(1) 身份鉴别机制。在网上银行系统中，用户的身份认证依靠基于"RSA公钥密码体制"的加密机制、数字签名机制和用户登录密码的多重保证。服务方(银行)对用户的数字签名信息和登录密码进行检验，全部通过以后，才对此用户的身份予以承认。用户的唯一身份标识是银行发放给用户的"数字证书"，用户的登录密码以密文的方式进行传输，确保身份认证的安全可靠。

(2) 访问控制机制。网上银行系统中，Web服务器中的所有资源分级管理，在安全系统中建立安全等级标签，只允许符合安全等级的用户进行访问。对用户进行分级别的授权，每个用户只能在授权范围内进行操作，实现了对资源的访问控制机制。

(3) 数据加密机制。网上银行系统采用SSL加密传输的方式，用户登录并通过身份认证以后，用户和服务方之

图1　银行系统中间业务网络



间在网络上传输的所有数据全部用会话密钥加密，直到用户退出系统为止，而且每次会话所使用的加密密钥都是随机产生的。这样，攻击者就不可能从网络上的数据流中得到任何有用的信息。

(4) 数据完整性机制。网上银行系统将采用“数字签名”对数据传输的完整性进行保护，一旦数据信息遭到任何形式的篡改，篡改后的数据必然与“数字签名”不符，可以立即检验出原始的数据信息已经被他人篡改，这样就确保了数据的完整性。

(5) 防否认机制。用户每次业务操作的信息均由用户的私钥进行数字签名，因为用户的私钥只有用户自己才拥有，所以信息的数字签名就如同用户实际的签名和印鉴一样，可以作为确定用户操作的证据。交易发出者不能对自己的数字签名进行否认，保证了银行的利益不受损害，这样，就实现了交易的抗否认要求。

(6) 审计机制。网上银行系统中，对用户每次登录、退出及用户的每次交易都会产生一个完整的审计信息，并记录到审计数据库中备案，以便日后的查询、核对等工作。

2.2 Internet服务安全

(1) 建立WEB服务器的安全访问机制，实现银行内外的动静态信息发布；

(2) 建立e-Mail、FTP、NEWS和DNS代理服务机制，实现银行内外的信息交流、电子邮件、文件上下载、域名解析等服务。

(3) 建立RADIUS服务器，对远程客户提供身份认证和拨号接入服务。

3 防火墙方案设计

根据以上的需求分析，本方案从主干通讯网络、综合业务网络、Internet业务网络、中间业务网络四个方面，提出安全解决方案。整个方案包括主干通讯网络安全防范、综合业务网络安全防范、Internet业务网络安全防范、中间业务安全防范。

从长远角度看，银行将采用公网作为业务数据的传输数据，因此如何在公网上保障业务数据的安全，是目前主干通讯网络安全的重要内容，它既解决实际存在的问题，同时也对以后银行利用公网开展业务提供了良好的试验。

3.1 网络防火墙的结构配置

防火墙部署方案用于指明防火墙的在网络拓扑中的位置，图2给出了计算中心的网络拓扑以及防火墙的位置。

在图中，计算中心的网络被分成五个子网段，业务网，网上银行网段，企业内部网和公开服务器网、中间业务网段。这五个网络都是物理上连通的，业务网通过银行业务主干网(DDN)与其他分行和综合所相连。网上银行主机是一个Web服务器，透过防火墙与Internet相连，它与企业内部网接成SSN结构，企业内部网包括企业内部的办公用工作站和企业服务器，公开服务器网包括外部邮件服务器、www服务器（不同于网上银行服务器）等。为了避免影响网上银行的信道带宽，银行与Internet连接分为两个部分，其中网上银行主机通过DDN

图2 网络拓扑以及防火墙的位置

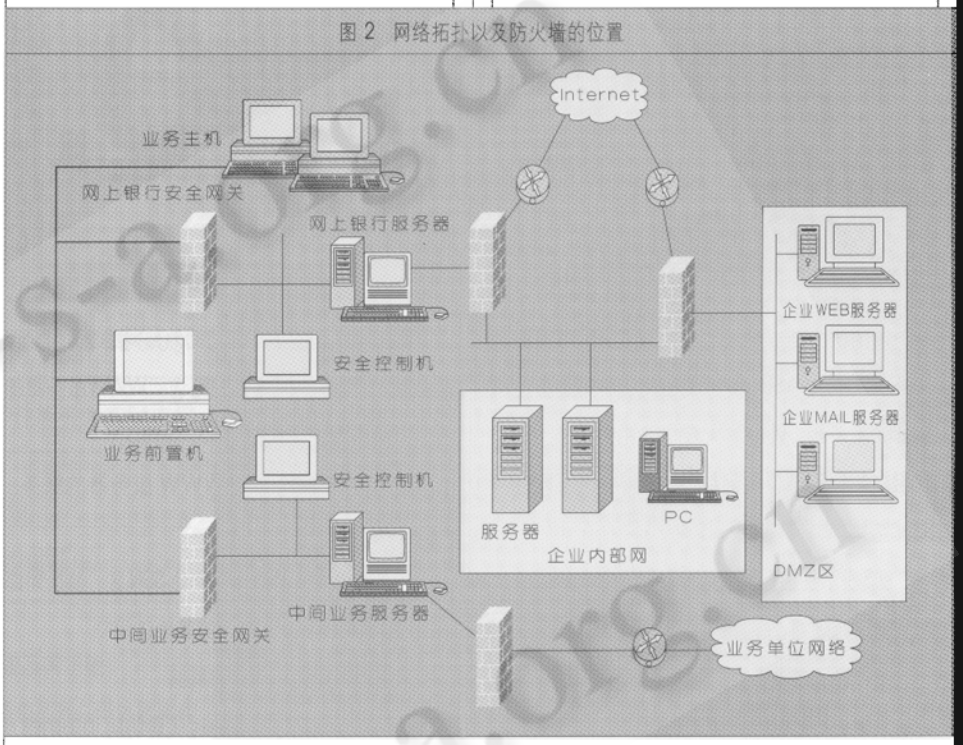


图3 业务网和网上银行网段防火墙示意图

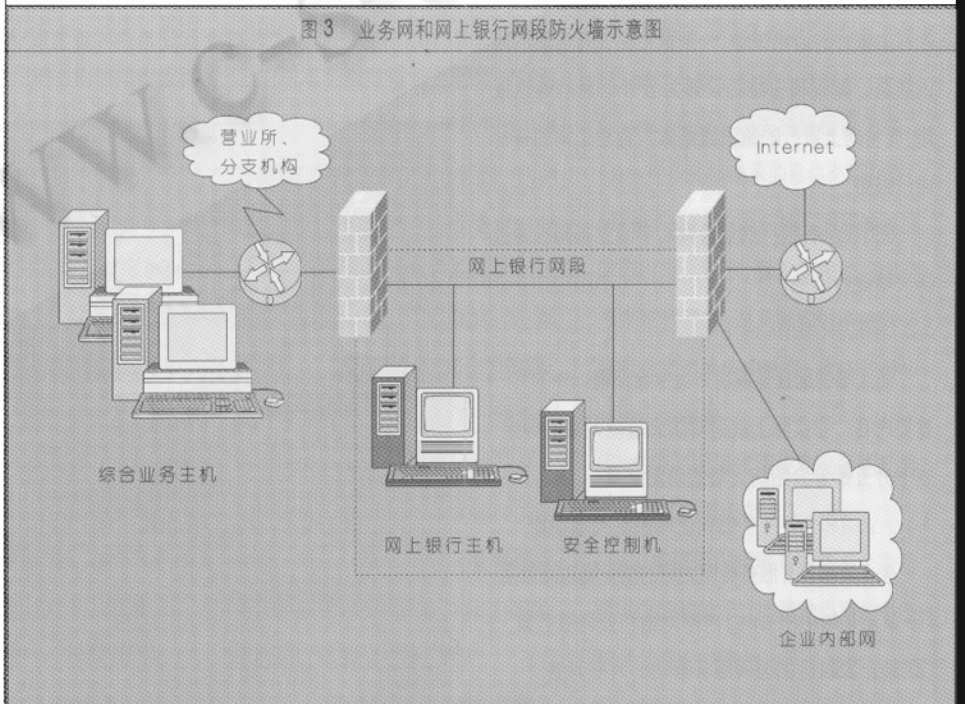
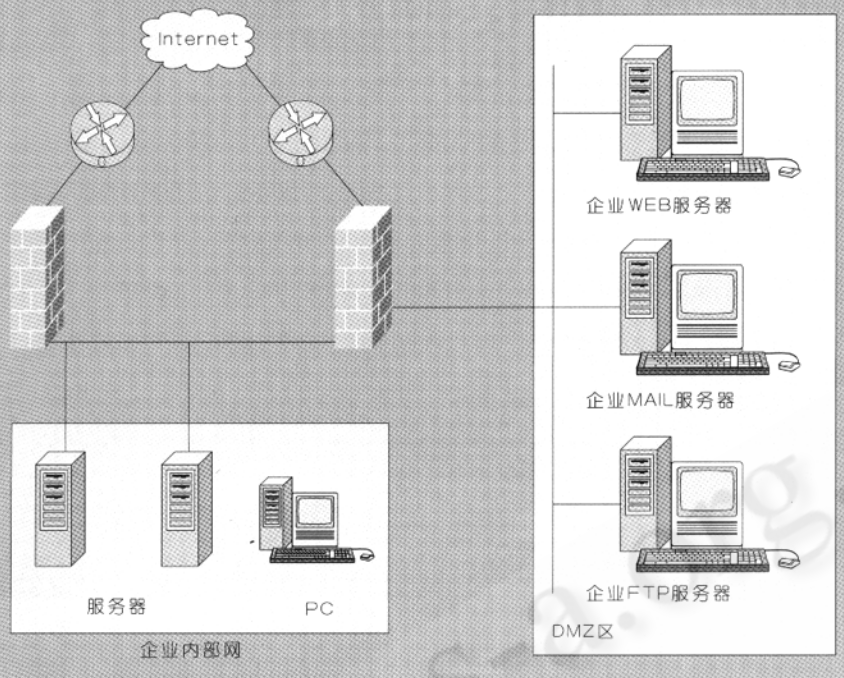


图 4　企业内部网和INTERNET通过防火墙示意图



与Internet相连，企业也可以通过DDN或通过拨号，ISDN或ASDL等方式上网。中间业务主机是一个服务器，透过防火墙与路由器相连，连接到相应的业务单位的网络，它与企业内部网接成SSN结构。

图3表示在银行的业务网和网上银行网段通过防火墙进行隔绝：

图4表示在银行的企业内部网和INTERNET通过防火墙进行隔绝：

说明：企业内部网可通过2条线路上网，一条为网上银行的通讯线路，一条是企业公开信息的通讯线路，建议将主线路设置为公开信息的通讯线路，而将网上银行的通讯线路做为企业上网的备份通讯线路。

图5表示在银行的业务网和中间业务网段通过防火墙进行隔绝：

3.2 网络防火墙的功能功能

防火墙的配置是解决方案中除部署以外的另一重要内容，它实际上就是对防火墙规则集的确定，以下分五部分介绍防火墙的功能配置。

3.3 企业网和公开服务器网之间的防火墙功能

企业网和公开服务器网之间的防火墙功能包括

(1) 禁止Internet ping 内部网络和公开服务器

(2) 禁止SSN区的公开服务器访问内部网络

(3) 允许SSN区的工作站访问外部网络

(4) 允许外部网络及内部网络访问WWW服务器的服务：WWW、Dns、Pop3、Smtp。

(5) 允许内部网络访问WWW服务器的服务：Ftp、Telnet。

(6) 允许某种或某些数据包到达SSN区，禁止外部网络及内部网络对SSN区的其他访问

(7) 禁止外部网络访问内部网络

(8) 允许内部网络访问获通过代理访问Internet

(9) 设置防黑客或入侵检测的范围

(10) 开放一些一次性口令认证用户并设置其访问权限

3.4 企业网和网上银行网段之间的防火墙功能

(1) 允许内部网络访问网上银行主机的某些特定应用端口，禁止所有其它访问。

(2) 禁止从网上银行网段向内部网络的所有访问

(3) 允许Internet用户通过SSL端口访问网上银行主机，禁止直接通过http端口访问。

(4)禁止Internet用户访问其他服务，包括Ping

(5) 禁止从网上银行网段访问Internet

3.5 网上银行网段和综合业务网之间的防火墙功能

(1) 允许网上银行主机通过特定应用端口代理访问综合业务网，禁止其他访问，包括Ping。

(2) 静止从综合业务网访问网上银行主机。

(3) 设置防黑客或入侵检测的范围。

3.6 中间业务网段和综合业务网之间的防火墙功能

(1) 允许综合业务主机通过特定应用端口代理访问中间业务网，禁止其他访问，包括Ping。

(2) 静止从中间业务网访问综合业务主机。

(3) 设置防黑客或入侵检测的范围。

3.7 中间业务网段与业务单位网络之间的防火墙功能

(1) 允许中间业务网段访问业务单位业务主机的某些特定应用端口，禁止所有其它访问。

(2) 禁止从业务单位网络向中间业务网段的所有访问

(3) 禁止业务单位网络访问其他服务，包括Ping。

图 5　业务网和中间业务网段防火墙示意图