# 网络隔离技术在3G移动办公中的应用探讨

孙庆和[1,2] 刘道群[3]

(重庆邮电大学 重庆 400065)[1] (中国联通重庆市分公司 重庆 400042)[2]

(重庆理工大学 重庆 400054)[3]

**摘 要** 网络隔离技术在安全性要求高的领域得到广泛的应用。为了解决3G移动办公对信息传输的实时性和安全性需求,引入了网络隔离技术。详细描述了网络隔离的技术原理、主要功能及特点,并以网络隔离为基础设计了3G移动办公的安全解决方案。经应用证明,基于网络隔离的安全解决方案具有设计简单、隔离充分和安全性高等特点。

**关键词** 3G,移动办公,网络隔离,数据交换,网闸

## Discussion on Application of Technology of Network Isolation in Mobile Office Based on 3G Network

SUN Qing-he[1,2] LIU Dao-qun[3]

(Chongqing University of Posts and Telecemmunications, Chongqing 400065, China)[1]

(Chongqing branch of China Unicom, Chongqing 400042, China)[2]

(Chongqing University of Technology, Chongqing 400054, China)[3]

**Abstract** Network isolation technology is taken to increase importance to the system and network security in more companies. In order to slove the security problems in mobile office based on 3G network, network isolation is imported. This article pays more attention to technical theories, main functions and characteristics of network isolation. Finally we proposed the solution of security problem of mobile office in 3G based on network isolation technology. The practical application proves that the security solution has the advantages of simple design, fully separation and high security characteristics.

**Keywords** 3G, Mobile office, Network isolation, Data exchange, Netgap

## 1 引言

随着移动通信技术的发展和移动业务的不断创新,具有"移动性、实时性"优势的移动信息化解决方案已经深入到政府、公安、金融、教育等各行各业。然而,由于终端的安全以及在使用过程中无法判断用户的合法性,存在非法用户、非法外设的接入等问题。同时由于采用了移动网络进行通信,信息在空中传播,敏感信息在传输过程中存在被泄露或被篡改等风险[1]。因此,3G移动办公对维护敏感信息的完整性、及时性、准确性提出新的挑战。为便于涉密部门开展移动办公、支撑涉密单位的实战工作,必须设计有效安全机制,以在实现3G移动接入的同时,保障敏感信息的安全。

如今网络隔离技术已经得到越来越多用户的重视,安全性要求高的领域已广泛采用网络隔离设备来保护内部网络。为了解决3G移动办公的安全接入问题,本文引入网络隔离技术,从物理链路上断开内网与外网不可信任的直接网络连接,保持在安全可控的条件下进行适度的数据交换。

## 2 网络隔离的基本原理和主要功能

### 2.1 基本原理

在有线网络中,网络隔离技术已得到广泛应用,分别在电子政务系统、公安信息化、金融行业中解决涉密网络和公共网络互联互通的问题。

网络隔离的基本原理是[2]:切断网络之间的通用协议连接(TCP/IP),将外网数据包分解重组为静态数据;对静态数据进行安全审查,包括网络协议检查和代码扫描等;再将确认后的安全数据流入内网,内网用户通过严格的身份认证机制获取所需数据。

外网通过网络隔离设备(隔离网闸)与内网"连接"起来,隔离网闸将外网传送进来的IP数据包按照TCP/IP协议全部剥离,将原始数据通过存储介质,以"摆渡"的方式导入到内部主机系统,实现信息的交换。"摆渡"意味着隔离网闸在任意时刻只能与一个网络的主机系统建立非TCP/IP协议的数据连接,即当它与外部网络的主机系统相连接时,它与内部网络的主机系统必须是断开的;反之亦然,即保证内、外部网络不能同时连接在隔离网闸上。隔离网闸的数据"摆渡"机制是原始数据通过存储介质的存储(写入)和转发(读出)。

隔离网闸在网络的第七层将数据还原为原始数据文件,然后以"摆渡文件"的形式来传递原始数据。任何形式的数据包、信息传输命令和TCP/IP协议都不可能穿透隔离网闸。下面以内网与外网之间的隔离网闸为例,说明通过隔离网闸的信息交换过程,见图1。

孙庆和(1975-),男,硕士,工程师,主要研究方向为下一代网络技术,E-mail:sunqh16@chinaunicom.cn;刘道群(1975-),女,硕士,工程师,主要研究方向为网络安全。

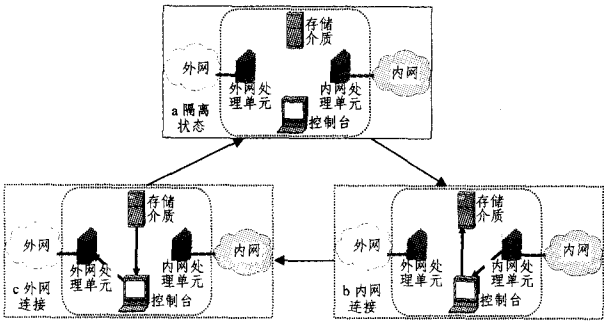


图 1　隔离网闸数据交换示意图

当内网与外网之间无信息交换时，隔离网闸与内网，隔离网闸与外网，内网与外网之间是完全断开的，即三者之间不存在物理连接和逻辑连接(a 隔离状态)。当内网数据需要传输到外网时，隔离网闸主动向内网处理单元发起非 TCP/IP 协议的数据连接请求，并发出“写”命令，将写入开关合上，并把所有的协议剥离，将原始数据写入存储介质。在写入之前，根据不同的应用，还要对数据进行必要的完整性、安全性检查，如病毒和恶意代码检查等。在此过程中，外网处理单元与隔离网闸始终处于断开状态(b 内网连接)。

一旦数据完全写入隔离网闸的存储介质，开关立即打开，中断与内网的连接。转而发起对外网的非 TCP/IP 协议的数据连接请求，当外网处理单元收到请求后，发出“读”命令，将隔离网闸存储介质内的数据导向外网处理单元；外网处理单元收到数据后，按 TCP/IP 协议重新封装接收到的数据，并将其交给应用系统，从而完成内网到外网的信息交换(c 外网连接)。

控制台收到信息处理完毕的消息后，立即中断隔离设备与外网的连接，恢复到完全隔离状态(a 隔离状态)。

至于从外网到内网的信息交换，与上述类似，只是方向相反。

由上不难看出，每一次数据交换，隔离网闸都经历了数据写入、数据读出两个过程；内网与外网永不连接；内网和外网在同一时刻最多只有一个同物理隔离网闸建立非 TCP/IP 协议的数据连接。

### 2.2　主要功能

网络隔离主要解决内外网之间的数据交换问题，针对内外网信息共享的类型和共享速度的需要，网络隔离主要包括以下功能：

1)文件交换，可以在内外网服务器上实时/定时地进行单向或双向的文件隔离交换，包括格式检查、内容过滤、签名校验等功能。

2)安全浏览，支持透明模式和非透明模式的安全上网功能。

3)邮件交换，在内外网邮件服务器之间进行邮件隔离交换，内网用户可以安全地收发外网邮件。

4)套接字(Socket)访问，提供客户端通过 TCP/IP 协议访问服务器的功能。

5)病毒防护，可以对交换的数据进行病毒检查，防止未知和已知木马攻击。

6)身份认证机制，对用户进行用户名/口令、证书认证等多种形式的身份认证。

## 3　隔离网闸的技术特点

隔离网闸能够解决内外网之间的大流量数据交换问题，主要包含以下技术特点[3]。

(1)独立模块架构

网闸采用三模块架构。这三个模块，有两个是主机，一个是基于独立的控制电路控制的固态存储介质，通常称之为“2+1”架构。

(2)物理层断开技术

网闸外部主机与固态存储介质之间存在一个开关电路，内部主机与固态存储介质之间存在一个开关电路，这两个开关不会同时闭合，从而保证从 OSI 模型上的物理层的断开机制。

(3)链路层断开技术

任何基于通信协议的数据交换技术都无法消除数据链路的连接，最多只能称为协议转换或协议隔离，因此不是完整的网络隔离技术。隔离网闸消除了所有的通信链路协议，在链路层完全断开。

(4)TCP/IP 协议剥离和重建技术

为了消除 TCP/IP 协议(OSI 的第三层和第四层)的漏洞，隔离网闸剥离了 TCP/IP 协议。在经过网闸之后，再代理重建 TCP/IP 协议。

(5)应用协议的剥离和重建技术

为了消除应用协议(OSI 的第五层至第七层)的漏洞，必须剥离应用协议。剥离应用协议后的原始数据，在经过网闸之后，代理重建应用协议。有时候称应用协议的剥离和重建技术为单边代理技术，单边代理技术是相对双边而言的。双边代理技术[4]，是指一台计算机有两个网卡，并且执行代理功能。数据包从一个网卡进，从另外一个网卡出。单边代理技术，只有一个网卡，这种情况下，应用协议必须还原成为原始数据给用户查看，而不能是包，因此是一个完整的应用协议剥离和重建技术。

## 4　基于网络隔离的 3G 移动办公安全解决方案

### 4.1　安全接入体系

分析 3G 移动办公的安全需求，借鉴网络隔离技术的成熟应用经验，综合了“终端加固”、“信道加密”、“认证接入”、“访问控制”和“网闸隔离”等五大安全措施共同构成独立完整的 3G 移动办公安全接入体系架构，见图 2。

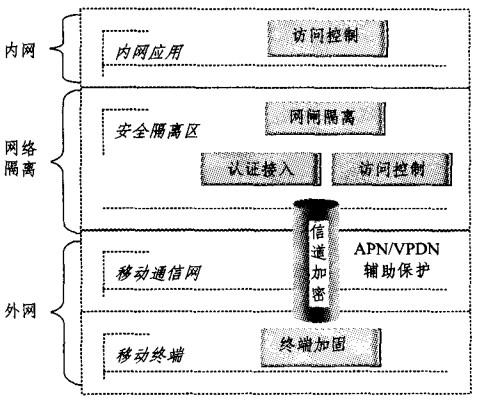


图 2　移动办公接入安全体系架构

终端加固：基于硬件密码对终端进行安全加固，保证终端

计算环境、资源和网络访问的安全和控制。

信道加密：采用密码算法实现移动终端到安全隔离区端到端的通信加密，保证内网信息在传输过程中的机密性和完整性。加密信道建立在通信运营商提供的 APN 专线之上。

认证接入：实现移动终端和安全隔离区接入设备之间的双向身份认证，保证持有合法身份证书的移动终端才能接入安全隔离区。

访问控制：保证内网信息资源只能被授权的终端访问，并对异常的访问进行阻断。

网闸隔离：实现外网和内网之间的网络隔离，对出入内网的数据进行协议剥离和内容过滤。

网络隔离采用专用通信硬件、专有安全协议、加密验证机制及应用层数据提取和鉴别认证技术进行不同安全级别网络之间的数据交换[5]，彻底阻断了网络间的直接 TCP/IP 连接，同时对网间通信的双方、内容、过程施以严格的身份认证、内容过滤、安全审计等多种安全防护机制，从而保证了网间数据交换的安全、可控，杜绝了由于操作系统和网络协议自身漏洞带来的安全风险。

### 4.2 3G 移动办公安全解决方案

根据 3G 移动办公安全体系架构，基于网络隔离技术组建一个端到端、安全可靠的移动办公解决方案[6]，将 3G 移动办公网络分成 3 个不同的区域：外网（包括移动终端、移动通信网）、安全隔离区和内网；网络部署见图 3。

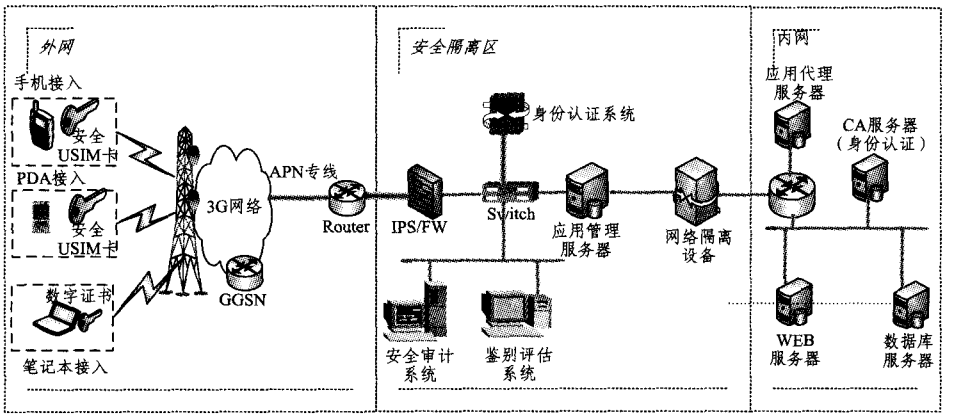


图 3 移动办公网络组网方案

全隔离区配置了入侵监测（IPS）、安全审计、身份认证、鉴别评估等边界安全防护措施，在移动终端接入内网之前进行安全防护；网络隔离设备从物理链路上断开内网与外网之间不可信任的直接网络连接。安全隔离区充分解决了移动办公的安全问题，在为合法访问提供方便的同时，还能防止内网信息资源被非法窃取。

**结束语** 随着 3G 移动办公在各行业的广泛应用，3G 移动办公的安全问题迫切需要系统的解决方案。本文引入成熟先进的网络隔离技术，建立了一个全方位、多层次的安全服务体系，提出了 3G 移动办公安全解决方案，解决了公网传输、内网保护等方面的安全需求。实践证明，这个安全解决方案不但能够满足内网、外网安全及物理隔离的要求，还能满足内外网信息实时传输的要求，为建设面向服务、安全高效的 3G 移动办公业务提供了有力的保障。

但是，由于在网络部署中增加了隔离网闸，导致组网节点增加，增大了网络时延，同时隔离网闸对所有的交换数据进行全方位、细颗粒的内容过滤，对系统资源有一定的影响，因此网络隔离技术在安全解决 3G 无线接入的同时，对网络的传输效率有一定的影响，这还有待进一步改进和完善。

## 参 考 文 献


[1] 刘道群，孙庆和. 信息敏感行业 3G 移动办公安全解决方案[J]. 电信科学，2011(S1)

[2] 王珺，李立新，李福林. 物理隔离和网闸的技术原理浅析[J]. 微计算机信息，2007，8(3)

[3] 邓霄博，杜勇，朱伟光. 基于 3G 网络的企业数据通信安全方案[J]. 电信科学，2010(8)

[4] 张红江. 网闸技术在社会保障信息系统种的应用[J]. 电子工程师，2007(11)

[5] 陈强，付强，张勇. 浅谈网络隔离技术[J]. 北方交通，2010(4)：195-197

[6] 张羽，冯朝辉. 安全网闸在公安信息化工作中的应用探讨[J]. 网络安全技术与应用，2007(05)

[7] "网络隔离"安全技术发展方向概述[EB/OL]. http://www.huacolor.com/article/737.html


（上接第 353 页）


[9] Wong R，Li J，Fu A，et al. (alpha，k)-anonymity：An enhanced k-anonymity model for privacy-preserving data publishing[C]// Proc of KDD 2006. New York：ACM，2006：754-759

[10] Xiao Xiao-kui，Tao Yu-fei. m-Invariance：Towards Privacy Preserving Re-publication of Dynamic Datasets[C]// Proc of the ACM SIGMOD Int'l Conf. on Management of Data. 2007：689-700

[11] 刘玉葆，黄志兰，傅慰慈，等. 基于有损分解的数据隐私保护方法[J]. 计算机研究与发展，2009，46(7)：1217-1224

[12] 周水庚，李丰，陶宇飞，等. 面向数据库应用的隐私保护研究综述[J]. 计算机学报，2009，32(5)：847-860