



## 龙湖地产 iGate 远程访问解决方案

### 一、企业概述：

重庆龙湖地产发展有限公司是由重庆中建科置业有限公司更名而来。公司成立于1995年6月，由重庆佳辰经济发展有限公司控股。拥有员工800余名。

1995年6月，公司正式介入房地产领域，确立了以房地产为核心的发展战略，将住宅开发作为主导方向。

公司凭借一贯的创新精神及专业开发优势，以其准确的市场定位、超前的规划设计以及优质的物业管理，在业内树立了良好的企业品牌形象。截止2003年11月，累计已开发面积约110万平方米，在建面积约150万平方米。现在龙湖地产发展有限公司为重庆地区最具知名度的房地产开发商之一。

### 二、需求分析

龙湖地产内部网络中使用一套 OA 办公系统及一套成本管理系统。两套系统均为客户端基于浏览器的 B/S 结构，系统在龙湖集团内部网络中使用。客户端通过浏览器使用。

系统在企业内部的局域网络上运行，现在经常遇到工作人员在出差时需要从外网访问内部服务器，现在的解决办法是通过防火墙集成的一个简单口令认证来访问！

随着新的成本系统的上线及使用量的增加，其中的一些问题也暴露出来。最主要的就是整个信息系统的安全使用问题，其中包括：

- 1、口令很容易被破解，而且服务器本身是暴露在外网的，即使不破解口令，也可以直接攻击！
- 2、通过这个口令认证，可以访问局域网内的任意一台服务器，这就存在极大的安全隐患！
- 3、所有数据完全以明文方式传输，没有经过任何方式加密！

### 方案选择

根据他们的需求，目前市场上可选用的方案有以下几种：

1. 使用 IPSec VPN——这种传统的 VPN 系统已经发展了很多年，他可以在客户端和总部局域网之间利用 Internet 建立一条 IPSec 隧道，使这两点间的数据就像



在一个专用网络中传输而不被截获。而且，只有连通了 VPN 的客户端才可以访问服务器，从而对服务器的安全性有了很大提高。在用户认证方面，只有安装了 VPN 客户端软件的电脑才可以建立连接，并且在建立 VPN 连接时还需要使用用户名+密码进行认证，在一定程度上提高了认证的安全强度。同时，IPSec VPN 的价格比起专网要便宜很多，是可以接受的。但是，使用 IPSec VPN 也存在着它的局限性。首先，每一个客户端都需要安装客户端软件，设置这些软件需要一定的网络知识，因此大大增加了销售人员的工作难度。其次，由于 IPSec VPN 的通道建立在网络层，在 Internet 中传输会遇到大量 NAT 和穿越防火墙的问题，尤其是各个地方的环境的上网方式不同，可能会同时存在 Modem 拨号、ADSL、宽带等多种方式，更增加了连接 VPN 的困难。一旦由于这些问题造成了系统不能使用，整个业务就无法开展，因此势必需要一支维护队伍随时提供支持，无形中又增加了成本。再有一点，客户端的电脑直接连入数据中心内部网络，有可能会将病毒、蠕虫等威胁带入数据中心。

2. 使用 SSL VPN——这是一种新兴的 VPN 技术，其核心技术是利用在 Web 上广泛使用的 SSL 技术在应用层构建针对应用程序的 VPN 通道，部署成本更低。与传统的 IPSec VPN 不同，SSL VPN 无需在客户端安装和设置任何软件，只要会使用浏览器上网浏览就可以毫无障碍的使用 SSL VPN。在网络传输中，使用标准的 Https 协议，能够提供极其安全的网络隧道，保证数据不回被截获和破解；同时，也不会受 NAT 和穿越防火墙问题的困扰，任何能连接 Internet 的方式都可以构建 SSL VPN 通道。同时，在应用层建立的通道可以防止病毒、蠕虫等经由网络层传输的威胁。另外，由于 SSL VPN 还可以起到代理服务器的作用，所有客户端的访问都是由 iGate 转发，而不能直接访问应用服务器，从而使服务器不易受到攻击。

经过对这些方案的比较，龙湖地产认为 SSL VPN 更符合他们目前的需求，解决员工频繁出差和分支机构的用户使用不同的连网方式访问应用服务器的需求。经过对市场上几种

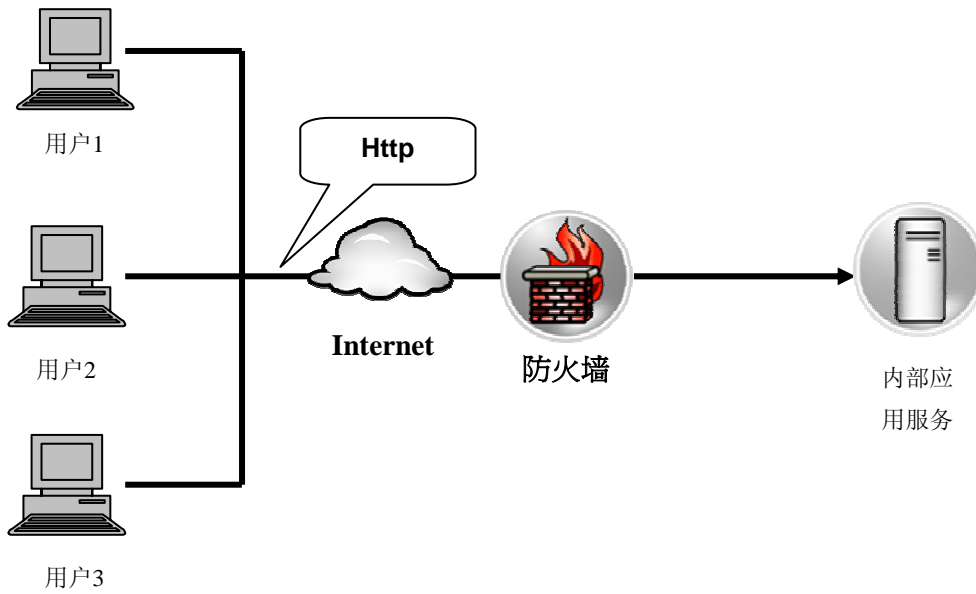


SSL VPN 产品的比较及测试，他们选择了 SafeNet 公司的 iGate SSL VPN 产品来保护内部信息系统，实现安全远程访问。因为相对于其他产品，iGate 具有以下两点主要优势：

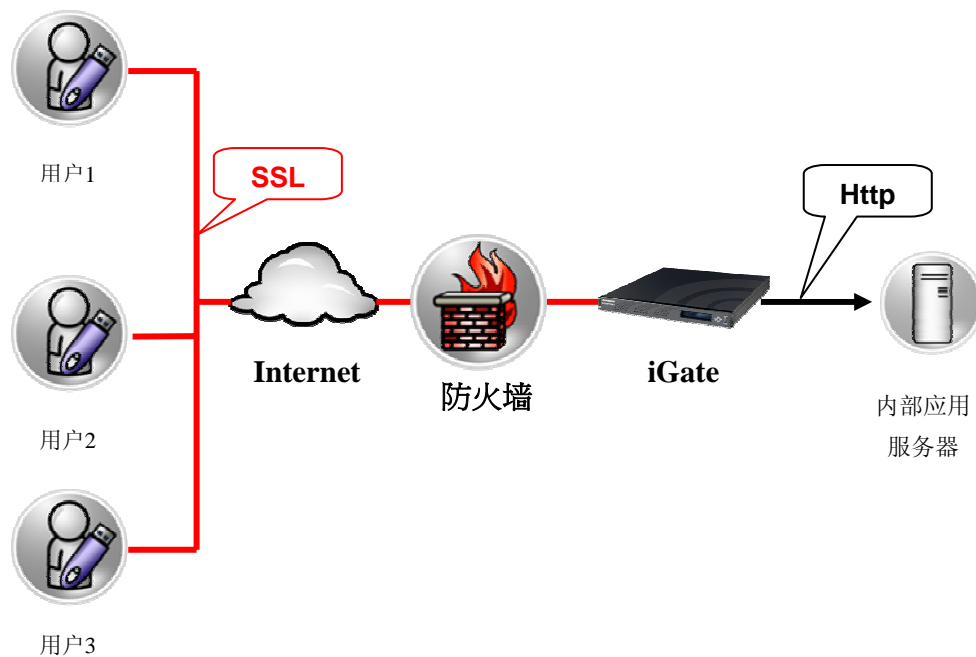
1. 客户端集成了 iKey 双因素认证令牌（需要同时提供令牌和 PIN 码进行认证）——正如我们前面所提到的，使用用户名+密码的认证方式存在着种种缺陷。而 SafeNet 公司的 iGate 是目前市场上唯一直接集成了客户端双因素认证令牌的 SSL VPN。用户需要同时知道 iKey 的 PIN 码，并且拥有 iKey 硬件才能通过认证，仅持有其中一个因素是无法通过访问验证的。这和我们使用银行卡在 ATM 提款机上取款时同样的道理。用户在连接 VPN 通道时，需要把 iKey 插入电脑的 USB 接口，然后输入只有他自己知道的 PIN 码才能通过认证。而且 PIN 码只是由数字组成，容易记忆；同时它还受重试次数的保护，不会被其他人通过暴力手段破解。
2. 内置 SSL 加速卡——iGate SSL VPN 里面内置了 SafeNet 所独有的 CryptoSwift 加速卡，专门针对 SSL 加解密运算，即使有大量并发的 SSL 连接也不会造成访问延迟。这对于绍兴联通的充值卡在线销售系统这样要求实时性很强的应用显得尤为重要。

## 方案实施

在选定产品后，龙湖集团开始进入实施测试阶段。在没有使用 iGate SSL VPN 之前，信息系统的网络构架如下：



而将 iGate SSL VPN 应用到网络中之后，整个网络的连接效果将会变成：



可以看到，不需要更改网络结构，只需在防火墙和服务器之间，通过使用交换机和网线，将 iGate 和这些设备物理连接，通过软件配置放置于同一个网段上。通过 iGate 内置的协议转换、IP 地址的跳转功能，将公网的域名和 iGate 的虚拟 IP 地址捆绑在一起，从物理上将后台服务器保护起来。从而起到一个第二层防火墙的功能。

iGate 服务器通过硬件的方式来完成数据的加密处理功能。一旦用户要访问 iGate 保  
地址：成都市磨子桥磨子街 7 号新棕北大厦 6-11  
电话：028-85224730(四线中继) 85221359 85219026  
传真：028-85224730  
网址：<http://www.dinknet.com>



鼎科信息

DinkNet Information co.,Ltd

护的应用，iGate 就会在用户的客户端机器和 iGate 服务器之间建立 SSL 安全通道。从而实现了数据的加密传输，同时硬件的加密实现方式极大的提高了整个网络传输的速度性能。

### 实施效果

整个方案从开始布置到实施完毕只用了一天的时间。实施了 SafeNet iGate 远程访问解决方案后，员工在使用过程中需要插入 iKey 并输入 PIN 码或输入用户名、密码即可完成验证，其他步骤与使用 iGate 之前没有任何区别，能够和原有的系统很好的结合。而这简单的一步却达到了上面所提到的众多安全访问需求。