

SafeEnterprise™ SSL iGate在绍兴联通代理商综合业务受理系统中的应用

业务需求:

深圳发展银行是中国历史上第一家向社会公众公开发行的商业银行。“敢为天下先”是深圳发展银行引以为豪的独特品质。

经过 17 年发展，深圳发展银行已经由最初的 6 家农村信用社，成长为在 18 个经济中心城市拥有 200 多家分支机构的全国性股份制商业银行，在自身规模不断扩大、综合实力日益增强的同时，也为客户、为股东、为社会奉献了丰厚的回报。

近年来，在对传统业务精益求精的基础上，深圳发展银行不断加强在中间业务、金融创新领域的探索，努力打造“服务创新银行”的品牌形象。

在公司银行领域，深圳发展银行坚持“业务发展专业化”道路，较早建立了货权质押业务中心、票据业务处理中心等专业化集中作业处理平台。由深发展率先引入的“产业链金融”理念，在能源企业得以成功运用并迅速推广至多个行业；“CPS—以票据业务为核心的企业短期融资解决方案”，在得到客户广泛好评的同时，也引起业界良好反响。与此同时，深发展国际业务、离岸业务稳健发展，市场份额与品牌知名度不断提高，为公司客户搭建起全方位的银行服务体系。

随着综合实力的全面提升，深圳发展银行在深圳、北京、上海、天津、重庆、广州、珠海、佛山、海口、杭州、南京、宁波、温州、大连、济南、青岛、成都、昆明等经济中心城市设立了分支机构。今天的深发展，已经基本形成了覆盖华东、华北、西南、华南的全国性战略布局，机构与业务网络日臻完善。

根据市场的需要，绍兴联通为了利用更多渠道开展公司的各项业务，在有条件接入互联网的众多代理商处引入了一套 B/S 结构的应用系统。利用该系统，代理商可以做各项业务的受理：如套餐变更、特服变更、话费查询、补卡等等。随着市场竞争的加剧和服务意识的提高，绍兴联通结合广大代理商的要求，采用了在 Internet 上直接为用户缴费的方式（我们称为现金缴费），大量取代了以前的纸或塑料介质“缴费充值卡”，取得了良好的效果。

其优势在于：

1. 操作方便。所有的分销点只需要一台可以连接 Internet 的电脑就可以进行联通用户全业务的话费预缴工作。
2. 无需事先压货。代理商不需要事先到联通公司购买充值卡，系统可以自动记录每个代理点的销售情况，月底统一结算。
3. 联通公司不再需要进行烦琐的有关介质卡的配送、管理工作。
4. 销售信息反馈及时。通过在线系统可以随时统计当时的话费预缴情况，不必再等每个代理点上报销售数据。

因此，绍兴联通着手大力推广在这种销售方式。他们采用了杭州康林克信息技术有限公司开发的代理商现金缴费系统来进行在线销售。这套软件使用 Browse/Server 结构，所有销售点客户端无需安装任何软件，只要能通过 IE 浏览器上网，就可以使用这套系统。这种方式大大加快了绍兴联通公司代理销售网点的建设工作，从而使市场迅速扩展。

但是，随着业务量的扩大，其中的一些问题也暴露出来。最主要的就是整个销售系统的安全使用问题，其中包括：

1. 客户端认证——系统软件中虽然设置了用户名+密码的认证方式，但是用户名和密码往往比较容易被盗用和破译。尤其是密码的强度问题，使用短小易记的密码，很容易被破解；如果使用复杂的长密码，对于使用者又难以记忆，往往会把它随手记录在记事本甚至贴在电脑旁边，使得盗窃者更加方便。
2. 网络传输——由于这套业务受理系统通过 Internet 来连接代理网点和绍兴联通公司的数据中心，所有内容都会在 Internet 上传输。而这种基于标准 Http 协议的明文传输很容易被截获。
3. 服务器被攻击——为了能让最终用户可以访问数据中心的服务器，绍兴联通需要把服务器的访问权限公布在 Internet 上。尽管使用防火墙保护，NAT 技术等对安全性有所提高。但是从 Internet 上可以使用 80 端口连接到应用服务器，这就给黑客留下了很大的空间进行攻击和侵入，进而威胁整个数据中心的安全。

由于这套业务受理系统中传输的有各类用户信息和缴费信息，一旦泄露，将直接造成经济损失。为此，绍兴联通急需一套能够保护在线系统，解决上述问题的解决方案。

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. 构建专网——通过专网，使得所有销售点和绍兴联通数据中心直接相连，所有通讯不再经过 Internet，极大地保证了网络传输的安全性。而且，由于不连接 Internet，服务器受到攻击的可能性大大降低。但是，这对于客户端的认证，仍然无法增加任何强度，一旦入侵者得到用户名密码、使用销售点的电脑进入销售系统，仍然可以进行破坏性的操作。再有，这样的连接方式相当于把所有销售点的电脑直接接入数据中心服务器的内网，那么，在这些机器上的病毒、蠕虫等威胁就都有可能由此进入服务器而造成更严重的危害。另外一个问题是，如果对每一个销售点都铺设专网，其费用极其昂贵，计算下来很可能得不偿失。
2. 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，而代理点操作人员往往不具备这样的知识，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，尤其是各个销售点的上网方式不同，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，就是和使用专网一样，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。

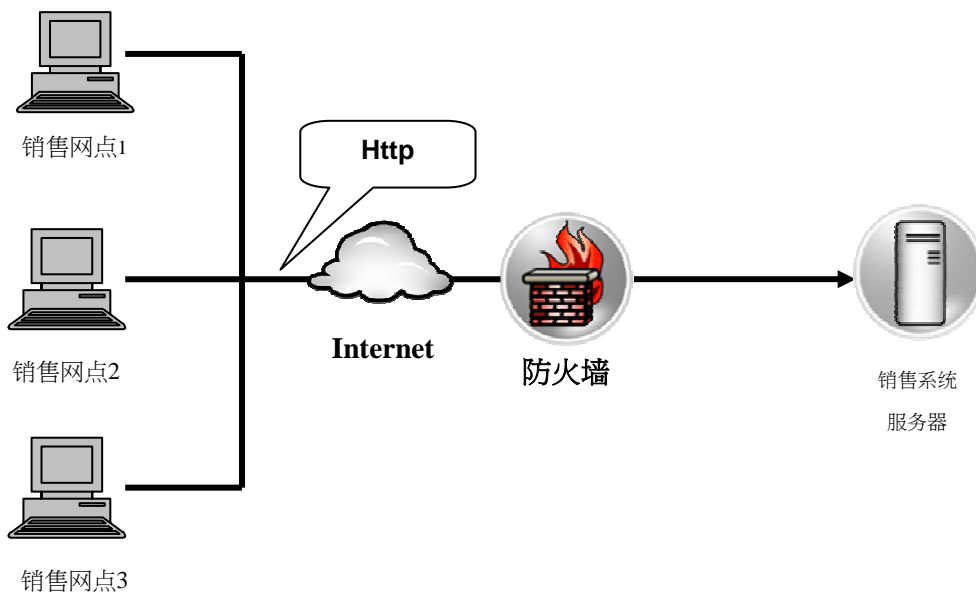
3. 使用 SSL VPN——这是一种新兴的 VPN 技术，其核心技术是利用在 Web 上广泛使用的 SSL 技术在应用层构建针对应用程序的 VPN 通道，部署成本更低。与传统的 IPSec VPN 不同，SSL VPN 无需在客户端安装和设置任何软件，只要会使用浏览器上网浏览就可以毫无障碍的使用 SSL VPN。在网络传输中，使用标准的 Https 协议，能够提供极其安全的网络隧道，保证数据不回被截获和破解；同时，也不会受 NAT 和穿越防火墙问题的困扰，任何能连接 Internet 的方式都可以构建 SSL VPN 通道。同时，在应用层建立的通道可以防止病毒、蠕虫等经由网络层传输的威胁。另外，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，绍兴联通认为 SSL VPN 更符合他们目前这样，有众多分布式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，他们选择了 SafeNet 公司的 SafeEnterprise™ SSL iGate 产品来保护充值卡在线销售系统，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：

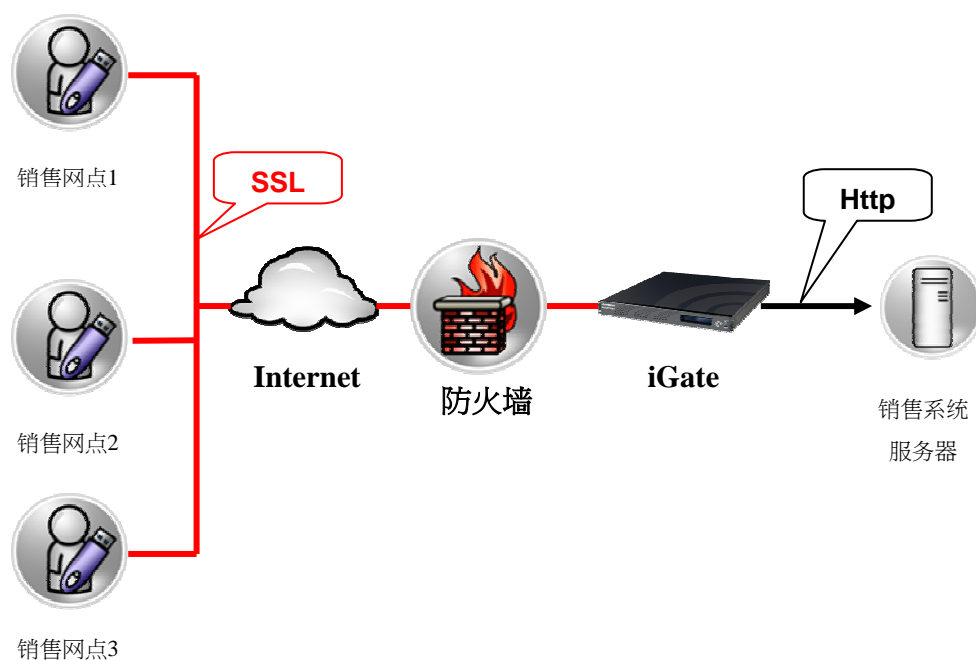
1. 客户端集成了 iKey 双因素认证令牌（需要同时提供令牌和 PIN 码进行认证）——正如我们前面所提到的，使用用户名+密码的认证方式存在着种种缺陷。而 SafeNet 公司的 iGate 是目前市场上唯一直接集成了客户端双因素认证令牌的 SSL VPN。用户需要同时知道 iKey 的 PIN 码，并且拥有 iKey 硬件才能通过认证，仅持有其中一个因素是无法通过访问验证的。这和我们使用银行卡在 ATM 取款机上取款时同样的道理。用户在连接 VPN 通道时，需要把 iKey 插入电脑的 USB 接口，然后输入只有他自己知道的 PIN 码才能通过认证。而且 PIN 码只是由数字组成，容易记忆；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——SafeEnterprise™ SSL iGate 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。这对于绍兴联通的代理商在线业务受理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，绍兴联通开始进入实施测试阶段。在没有使用 SafeEnterprise™ SSL iGate 之前，该销售系统的网络构架如下：



而将SafeEnterprise™ SSL iGate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，所有的访问都会使用 SSL 加密协议传递到 iGate 之后，由 iGate 再与服务器通信。而 iGate 的接入之需要使用一根网线连接到服务器所在内部网络的交换机即可，所有网络配置中的更改只是在防火墙上将原来解析到服务器内部网络地址的访问转向 iGate。所有的安装、配置在几个小时就可完成。

实施效果

使用SafeEnterprise™ SSL iGate保护后的在线业务受理系统，操作员在使用过程中需要插入iKey并输入PIN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我们所提到的众多安全访问需求。

目前绍兴联通已经在其所属的所有网点使用了SafeEnterprise™ SSL iGate构建的安全远程访问系统来保护它的在线业务受理系统及现金缴费系统。