

SafeNet iGate SSL VPN 成功案例：

中国石化国际石油工程有限公司

中国石油化工集团国际石油工程有限公司（SINOPEC PETROLEUM SERVICE）是中国石油化工集团公司为开发海外石油工程服务市场而特别设立的全资子公司，负有统一管理、协调、组织集团公司上游石油工程队伍实施海外石油工程业务的职责。

目前，中国石化集团国际石油工程公司在对外石油工程承包、油田技术服务、劳务合作方面均取得了较大进展。在非洲、中东、中亚、美洲、南亚和东南亚等数十个国家和地区，通过开展合资合作、提供技术服务或以承包及分包的形式，实施了物探、钻井、测井、录井、固井、修井、油田地面建设、管道建设和水利、道路建设等石油工程及其他工程服务项目百余个。

随着业务的扩展，尤其是当前巴西、苏丹等项目的筹划进行，中国石油化工集团国际石油工程有限公司在巴西、苏丹等地设立了项目组，各项目组与国内集团总部需要进行大量而且重要的文件传输。由于地理的限制使得通过传统方式传递文件、项目资料非常困难，这样，通过多方调研，公司总部决定在北京总部搭建全球协同办公系统，构建远程信息访问架构，充分利用互联网的便利性。通过石化全球协同办公系统为巴西等项目组提供远程的信息共享，主要包括：

内部公文办理系统：提供项目组人员在国外能够办理内部业务的功能。

文件传输系统：提供文件的相互交流，集中管理，大文件的断点续传等。

电子邮件系统：提供项目组负责人和公司总部人员之间通过电子邮件形式进行快速、便捷的信息交流。

视频会议系统：提供项目组与总部之间各人员进行时实的语音和视频交流。

由于互联网的开放性，远程员工利用全球协同办公系统在与总部通信时，就面临着信息传输的安全性、有效性、保密性等种种安全问题。如果数据直接在网上传输，数据中包含了许多敏感的、保密性的信息，存在着极大地被攻击，窃取的危险，一旦被截获，将会造成重大的损失。

为此，公司总部考虑构建一个安全的远程访问解决方案以应对上述的问题。根据当前的实际状况，公司总部决定把采用 VPN 设备在 Internet 上架设虚拟专用网作为搭建全球协同办公系统的重要有机组成部分。目前市场上的 VPN 主要由两种类型：

1. 使用 IPSec VPN——这种传统 VPN 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，从而可以保证数据在网络传输中的安全性。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。这样，造成了维护成本的增加。

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，尤其是各个子公司的上网方式不同，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，数据就无法传输，如果为此设立一支维护队伍随时提供支持，又会增加成本。再有一点，就是客户端的电脑直接连入服务中心内部网络，有可能会将病毒、蠕虫等威胁带入。

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。

首先，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，保证数据不会被截获和破解；

其次，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。

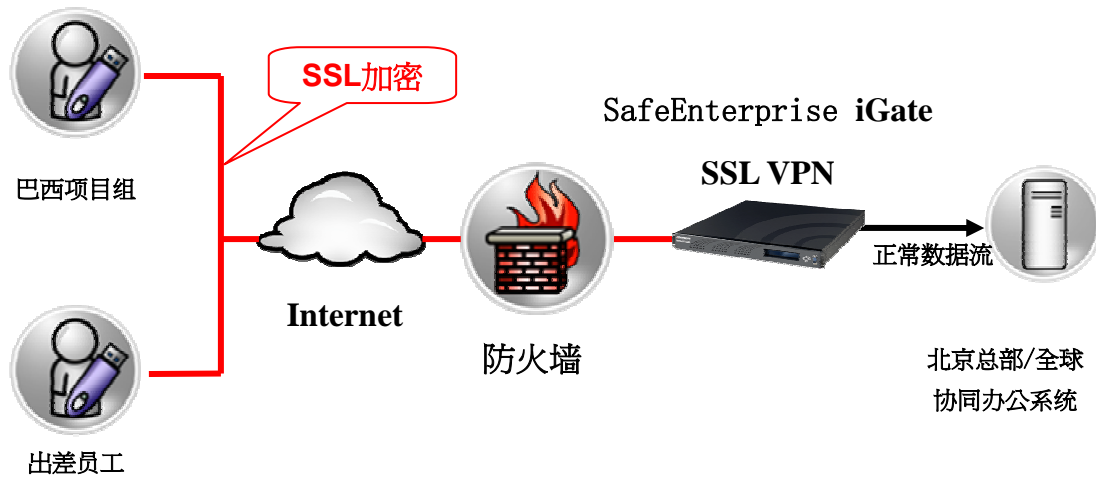
经过对两种方案对比，石化集团国际石油工程公司认为 SSL VPN 更适合于公司实际应用。经多家 VPN 设备长期测试而最终采用了 SafeNet 公司的 iGate SSL VPN 设备来构建远程访问的解决方案。这主要是因为：

1. iGate 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)，使用传统的用户名+密码的认证方式不能保证客户端验证的安全性。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. iGate 在客户端集成的 iKey 令牌本身就是一个独立的身份认证产品。这样既提高了客户端程序的安全性，也大大简化了最终用户登录的操作，从而通过整合 iGate SSL VPN 将整个系统安全性、易用性都进行了大幅提升。
3. 采用 ssl 加速功能。通过 iGate 硬件内置的 SSL 加速卡，提升了用户的认证、授权、数据传输的速度，同时，最大程度的减少了内网服务器的负担——所有加密、解密的功能均由 iGate 硬件完成。

方案实施：

使用 iGate SSL VPN 之后，网络结构如下图所示：

从图中可以看出，所有通过互联网到总部的访问都会使用 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 iGate SSL VPN 后，北京总部的全球协同办公系统实现了异地共享，同步运作，使得员工在外随时通过 INTERNET 接入网络，实现随时随地的移动办公，提高了工作效率。全公司的信息化的再次提升，提高了公司实力，为公司业务的进一步开展打下了坚实的基础。