

移动安全远程接入

iGate 远程访问系统在上海烟草集团的应用

Cast Study

[SafeNet iGate 安全远程访问解决方案帮助我们很好的提升了内部沟通和管理能力, 让分布在各地的员工更快捷、更方便的接入企业内部网。]

上海烟草信息中心主任

企业概况

上海烟草(集团)公司于1993年组建,是一个以卷烟工业为主的,多元化、集约化、现代化的大型企业。在2003年度中国纳税百强排序中,公司名列烟草行业第一、全国第二;在2003年度中国工业企业利润总额排序中,公司名列烟草行业第一、全国第十。

2004年,公司出口创汇9312万美元,其中利润7988万元。目前公司海外免税和有税目标市场超过120个,卷烟产品远销五大洲40多个国家和地区。

需求分析

随着信息化的发展,上海烟草(集团)公司为了不断提高企业的工作效率、增强企业的竞争力以及降低不必要的运营成本,考虑建设一个基于Internet网络平台的VPN远程安全接入网络,用于满足大约5000名分布在各地的员工远程办公(OA、ERP、Email、文件共享)、远程业务受理以及远程网络维护(Terminal Service)的需要。对该VPN网络的具体要求如下:

(1) 接入需求

- 满足各个远程分支机构的接入;
- 满足出差人员的接入;
- 满足合作伙伴和客户的接入。

(2) 功能性需求

- WEB应用系统的远程接入,如:OA、邮件、财务系统;
- 文件共享;
- 应用服务器的接入。

(3) 安全性需求

- 具备安全访问控制和数据加密传输能力;
- 强复合身份验证,持有硬件介质、持有密钥保护、第三方认证机构,防止:泄漏、篡改,同时实现抗抵赖,如:USB Key等。

(4) 可管理性需求

- 根据用户身份来确定用户的访问权限;访问控制的等级达到文件级;集中管理。
- 对VPN中新增加的节点的配置,快速、简单。
- 可实时监测网络应用状况,提供详细日志和审计功能。

(5) 可扩展性需求

- 可随时增加新的分支机构和临时移动用户
- 支持安全协议的增加和升级
- 能增加新的系统功能

(6) 易用性需求

- 对终端用户配置简单
- 对网络管理配置简单

需求分析及实现

针对于上海烟草提出的实际要求,首先需要实现数据在Internet上的加密传输,就要采用VPN的实施方案;其次,对远程接入的用户需进行强制认证,并能结合硬件USB Key来认证;再次要求接入的用户不能获得网络内部结构信息,只能使用自身有权限的应用;最后,由于有众多用户要访问公司内部应用系统,且客户端的网络环境千差万别,因此要尽可能的减少客户端的维护量。故此采用SSL VPN成为必然的选择。

SafeNet公司推出的SafeEnterprise SSL iGate Pro可满足用户提出了全部需求,同时结合iKey双因素的客户端认证方式,加强认证的安全性。另外,考虑到用户对网络的不间断性有较高要求,系统设计为双机热备架构,保证网络应用的不间断。具体实现方式如下:

■ 接入需求的实现

在总部部署iGate Pro服务器,就可以通过Internet实现远程分支机构的接入、出差人员的接入以及合作伙伴和客户的接入。只要他们能接入Internet网就能实现远程访问。



移动安全远程接入

iGate 远程访问系统在上海烟草集团的应用

Case Study

[SafeNet iGate 安全远程访问解决方案帮助我们很好的提升了内部沟通和管理能力, 让分布在各地的员工更快捷、更方便的接入企业内部网。]
上海烟草信息中心主任

■ 功能性需求

通过 iGate Pro 可以实现 WEB (B/S) 应用系统的远程安全接入, 如: OA、邮件、财务系统; 文件共享以及应用服务器的接入等。

■ 安全性需求

iGate Pro 可以实现端到端的数据加密, 能够针对每一个用户进行访问控制和加密数据传输。配合硬件 iKey 使用, 实现强复合身份验证, 防止: 泄漏、篡改, 同时实现抗抵赖。

■ 可管理性需求

iGate Pro 可根据用户身份来确定用户的访问权限。访问控制的细粒度达到文件级, 可集中管理, 有详细日志 (审计)。对新增加的客户端无需配置, 网管中心分配账号, 用户直接使用浏览器即可远程接入。提供报告工具, 实施反映网络情况, 并有图表统计。

■ 可扩展性需求

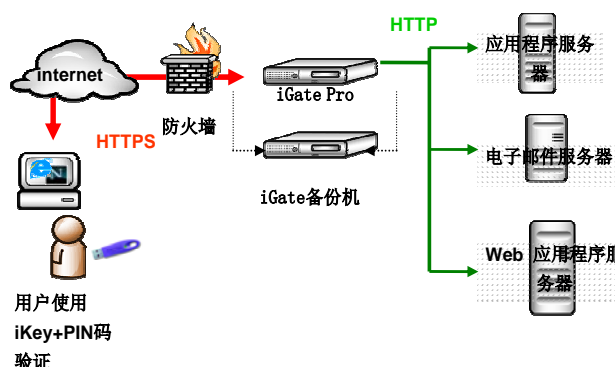
增加新的分支机构和临时移动用户时, 只需在网管中心分配账号。iGate Pro 支持多种安全协议和加密算法, 可完全满足用户的需求。用户可以通过升级 License 文件来增加并发用户数。用户可以通过软件升级来增加新的系统功能

■ 易用性需求

对终端用户基本无配置工作 (如使用 C/S 应用需安装 Java 虚拟机环境), 用户可直接通过浏览器实现远程接入。对网络管理配置简单, iGate Pro 服务器支持 Web、SSH、Console 管理, 支持 SNMP 协议, 同时配有 ACM 管理软件用于分发 iKey 和账户 (该软件可成批分配账户), 并可利用用户原有的认证系统如: LDAP、NDS、Active Directory、Radius 等

实施方案

iGate Pro 的工作位置在防火墙和后端服务器之间, 从客户端到 iGate Pro 之间的通讯都采用 SSL 协议加密, 而 iGate 与服务器的通讯则使用标准的 http 协议, 不会因为 SSL 加解密工作给服务器带来任何负担。



客户登录时使用 iKey+PIN 码的双因素认证方式, 对服务器端使用标准 SSL 验证, 对客户端使用 MD5 哈希算法的挑战-响应进行验证。双方验证结束后, 所有通讯均使用 HTTPS 协议, 保证了从客户端到 iGate 之间的通讯安全。信息传递到 iGate, 由 iGate 将其解密后以标准 HTTP 协议传递到后端的服务器, 从服务器返回的信息, 再由 iGate 加密后传递到客户端。

从 2005 年 9 月正式启用, 到目前为止, 集团总部及各分支机构应用状况良好, 大约 5000 名员工将陆续使用这套安全远程访问系统, 让它发挥更大的作用。

欲了解更多信息:

请登陆 SafeNet 公司网站察看详情:

<http://cn.safenet-inc.com>

赛孚耐 (北京) 信息技术有限公司

地址: 北京市海淀区西三环北路 100 号金玉大厦 1603 室 100037

电话: 010-88519191

传真: 010-68727342

email: security@safenet-inc.com

地区代理: 上海燃点电子科技有限公司

地址: 上海肇嘉浜路 999 弄 58 号 803 室 200030

电话: (021) 64038179*808

网址: <http://www.cn-randian.com>

Email: hb@cn-randian.com

