


业务支撑软件网络优化 解决方案

 深圳市惠尔顿信息技术有限公司

地址: 深圳市南山区高新技术产业园区虚拟大学园

电话: (0755) 26546529 • 传真 (0755) 26553507

公司主页: <http://www.wholeton.com>

E-mail: wholeton@wholeton.com

● 声明

Copyright©2004-2011 深圳市惠尔顿信息技术有限公司 版权所有。

由深圳市惠尔顿信息技术有限公司提供的本方案中包含的所有信息，都将被视为机密信息，本方案仅供各地财政单位网络异地互联解决方案时用。

惠尔顿公司本着“凸显带宽潜能、增值网络应用”的经营理念，利用当今网络中最前沿的技术促使应用软件在网络的运行的更安全、更快速、更稳定、更容易管理。

● 文档说明

2010年11月在财政局需求调研，我们所接触到的财政局所有领导与工作人员的敬业态度和工作热情令人敬佩，使得我们能准确了解到乡财国库业务信息系统对网络的要求，为此，我们要特别感谢所有财政工作人员的帮助！

目 录

序言	4
一、应用现状.....	4
1、应用数据库在内网的安全问题.....	4
2、应用在广域网/专网访问速度慢.....	5
3、管理软件管理与维护的不便.....	5
二、应用网络优化.....	6
1、提升应用访问速度，增强用户体验.....	6
1.1、远程应用的虚拟化.....	6
1.2、LZO 数据流压缩技术.....	6
2、增强应用的安全防护.....	6
2.1、服务器的安全防护.....	6
2.2、数据传输中的安全.....	8
2.3、客户端的安全.....	8
2.4、身份认证.....	9
2.5、应用级的访问控制.....	9
2.6、VPN 专线效果.....	10
3、应用集中部署，降低应用的管理开销.....	10
三、方案效果.....	12
1、提升访问速度 5-10 倍.....	12
2、保障了核心数据的安全.....	12
3、降低应用系统的 80%维护成本.....	13
4、与应用整合，使用培训费用降低 50%.....	13
四、产品部署.....	13
1、财政局网络.....	14
2、远程连接模式.....	14
3、需要访问管理软件的用户.....	15
五、方案预算.....	16
1、报价说明.....	16
2、项目报价.....	16
附录 I：所选产品技术参数.....	17
六、服务保障系统.....	20
1、售后保障.....	20
2、服务承诺.....	20
3、增值服务.....	21
七、典型案例.....	23
八、关于惠尔顿.....	25
稳步发展的惠尔顿.....	25
内部建设.....	25
技术实力.....	26
分支机构.....	26
发展历程.....	26

序言

随着中国电子政务建设的深入，日常的业务和相应的改革推动，越来越依赖于各种管理软件，随着业务的深入和对将来的应用系统的规划，同时也就存在了越来越多的用户接入数据中心，越来越多的数据中心建立，越来越多的服务需要提供。

目前，财政部门虽然建立了较为完善的专网系统，但在专网上运行的各类应用软件系统都是暴露在整個专网上的，假如专网内的用户不存在扫描、窥探行为等非法行为，专网的安全有一定保障的。

在保障应用安全的前提下，应用系统的使用效率、维护难度与使用难度是一个很严重的问题。应用系统响应时间长、远程应用系统维护成本高。

在这样的形势下，惠尔顿公司及时推出光里软件网络优化解决方案，至今已有内蒙古、广东、福建、河北、辽宁、江苏、新疆、湖南等多个省市财政单位的多个应用软件在网络上运行的优化经验，充分保障了核心数据服务器的安全、提升应用的访问速度，同时大大降低整个系统的运行维护成本。

一、应用现状

1、应用数据库在内网的安全问题

随着国家政府专网的建设的不断完善，随着国家电子政务的深化改革，越来越多的政府单位的电脑连接入了政府专网内，越来越多的应用软件在政府专网内普及使用。目前，各个单位可能上了较为完善的专网系统，但在专网上运行的各类应用软件系统都是暴露在整個专网上的，因此安全的隐患一直存在。要解决信息畅通、工作效率问题又必须在专网上使用应用系统，这是现在新的工作模式下的两个矛盾体。在之前很多单位也只能利用防火墙和其他杀毒产品来解决应用软件在专网上的安全问题，但此类解决方案只是治标，不治本，依然存在以下问题：

- ✓ 在专网内传输的应用数据，对于机密数据无任何加密等保护措施，导致数据泄密。
- ✓ 在专网内应用软件的数据服务器群由于需要专网内的其他电脑访问，将服务器群服务端口直接暴露在专网上，导致数据服务器直接受到专网内的任一电脑的安全威胁。
- ✓ 在专网内应用软件的数据服务器群的访问权限，无法细致到特定的人特定时间段访问特定的应用软件，导致专网内的任何人都可以访问所有的数据服务器资源，给非法用户敞开了灾难的大门。

- ✓ 在专网内的电脑直接通过网络层访问应用软件数据服务器，一旦电脑由于其他原因如由于业务需要上网，或者便携存储设备等导致感染病毒、木马后，将会直接传播给服务器，造成数据丢失、泄密。
- ✓ 如果出现安全事故，安全审计能够细到每个人吗？即身份认证是否锁定到人？
- ✓ 对于重要数据库服务器端操作权限最大的系统管理员，如何将他们误操作导致的安全事故概率降到最低？

2、应用在广域网/专网访问速度慢

不在同一个办公室的各行政事业单位通过各种形式的广域网相连，他们绝大多数采用专线形式的 ADSL 连接到应用服务器，或者采用公网的 ADSL 连接到应用服务器，部分偏远地区采用无线(CDMA)的方式连接到应用服务器，如何使得这部分的用户使用起来的速度效果等同于或者接近于 10-100M 的局域网网速？

3、管理软件管理与维护的不便

- ✓ 如果应用系统是用 C/S 的话，通常的一个应用系统都有上百的用户群，安装 100 多个的客户端以及维护这些客户端的正常运行工作量将十分艰巨；
- ✓ 如果是 B/S 的话，一般是基于 JAVA 开发，运行效率相对较低，对于客户端服务器端的配置均要求比较高，数据对传输的带宽要求也比较大；同时因为 B/S 软件是基于 IE 浏览器来访问的，对于客户端的 IE 浏览器的标准程度要求比较高，对非标准的一些东西敏感性比较强，导致客户端需要人工安装和维护的工作量和难度还是有的。

二、应用网络优化

1、提升应用访问速度，增强用户体验

1.1、远程应用的虚拟化

将原来在 10M 或 100M 局域网的业务搬到广域网上跑，速度会变慢的原因主要是传输通道变窄，广域网上很少有像局域网同样的带宽。传输速率类似于“木桶原理”，整个传输速率取决于传输通道中的瓶颈，为了解决这个问题，我们通过牺牲服务器端的资源来弥补传输带宽的短板。

通过 e 地通的远程集中接入功能将所有应用在服务器上 100%地安装、管理、支持和执行应用程序，将应用程序的执行和显示逻辑分离开来，所有计算均在服务器上执行，而只有键盘信息、鼠标点击和屏幕更新信息在客户机和服务器之间传输，大大降低对带宽的需求，不到 28.8k 的带宽就可以流畅的使用大型应用系统。也就是说采用这种模式在广域网络传输的不是真正的业务数据，而是经过压缩和加密后的屏幕变化数据，真真的逻辑运算在服务器总部机器内部或者局域网完成了。

1.2、LZO 数据流压缩技术

在将数据通过数据发送之前，先将其通过压缩算法压缩为更少的数据，再将压缩后的数据通过网络传送到另外一端；在另一端接受到数据之后，再通过解压算法解压为原来的数据。这样在网络上传送的数据就比原来少，更加充分利用已有的带宽。对于有一些不能采用远程集中接入模式来解决速度的应用，如单笔数据量并不大，但用户数很多的应用，这种应用如果采用远程集中接入功能就会导致远程集中接入服务器的投资很大，此时采用 e 地通用压缩技术来解决，对服务器端与客户端交互的数据流进行压缩，提高带宽的利用率，压缩算法为 LZO 流压缩算法。

2、增强应用的安全防护

2.1、服务器的安全防护

作为架构在应用层的 VPN，系统有效的屏蔽了 VPN 服务器的网络结构，也屏蔽了常见的网络攻击手段，系统根据授权与认证访问授信网络。更重要的是，在系统的客户端，可以

指定特定的应用程序才能发起连接，连接到服务器，完成应用的代理过程，根据这个控制，系统可以阻止病毒程序不能通过 VPN 隧道传输到 VPN 服务器端，有效保护了服务器数据资源的病毒威胁。

由于 IPSec VPN 打通了网络低层，一旦被侵入，整个网络都将暴露，建立隧道后，远程 PC 就像物理地运行在企业局域网上一样，相当于为远程访问者敞开了访问所有资源的大门，并对全部网络可视，为企业网络带来了安全风险。所以非常容易成为黑客攻击的目标。而且一旦客户端被黑客利用，他们会通过 VPN 访问企业内部系统。这种黑客行为越来越普遍，而且后果也越来越严重。例如，如果雇员从家里的计算机通过公司 VPN 访问企业资源，在他创建隧道前后，由于个人家用电脑一般缺乏安全防护措施，安全级别很低，如果黑客侵入了这台没有保护的 PC，他就获得了经过 IPSec VPN 隧道访问公司局域网的能力，而且这台接入电脑一旦中毒也非常容易通过 VPN 在整个内网传输。

作为架构在会话层的 VPN，在 VPN 服务器端，系统有效地屏蔽了的网络结构，也屏蔽了常见的网络攻击手段，如 PING、UDP、ICMP 包等，系统根据授权与认证访问授信网络；在 VPN 的客户端，可以指定特定的应用程序才能发起连接，连接到 VPN 服务器，完成应用的代理过程，根据这个控制，不仅可以实现精细的访问控制功能，重要的是可以阻止病毒和黑客程序不能通过 VPN 隧道传输到 VPN 服务器端，有效保护了服务器端数据资源受到安全防范措施弱的异地端的威胁。

e 地通 SOCKS5 VPN 要求远程接入者必须正确地使用客户端软件或接入设备，将访问限制在特定的接入设备、客户端程序、用户认证机制和预定义的安全关系上，也不允许从公共 Internet 发起访问，从而提供了更高水平的安全性。同时提供不需用户任何干预就可以自动将客户端机器硬件信息作为用户认证机制，完美实现了易用、经济又安全的解决方案。

SSL VPN 由于完全没有客户端，使得 SSL VPN 允许用户利用不安全的计算机访问企业网络，这些计算机易于受到键盘敲击记录软件和特洛伊木马的攻击，对企业网络造成威胁。同时用户在 Internet 上发起访问时，SSL VPN 客户端为企业网络带来了风险。为了避免这个缺陷，必须启用硬件 KEY 这样的外设来做辅助认证工具，这样又会增加它的整体购买成本，同时也削弱了 SSL VPN 的便利性特性。

另外，SOCKS5 的代理机制实现了应用服务器与 internet 的逻辑隔离。在 e 地通设备中，支持端口的多个 VLAN，应用服务器只需要与 e 地通设备的其中一个 VLAN 能实现通讯则可，而应用服务器不必与其他任何第三方有网络的相关连接，除了与 e 地通设备外。如何实现两个被隔离了的区域之间的访问，即应用用户对核心区的访问？

通过代理机制：

代理服务器的工作原理就是接受用户的请求并把请求转发给用户原本要访问的目的主机，反过来，目的主机的应答通过代理服务器再转发给用户。代理服务器根据支持的协议不同而又有所区别，e 地通采用 SOCKS5 作为代理协议，可以支持所有基于应用层的通信协

议。

基于以上现有的技术，e地通（如下图），其中包含有代理客户端、代理服务器。

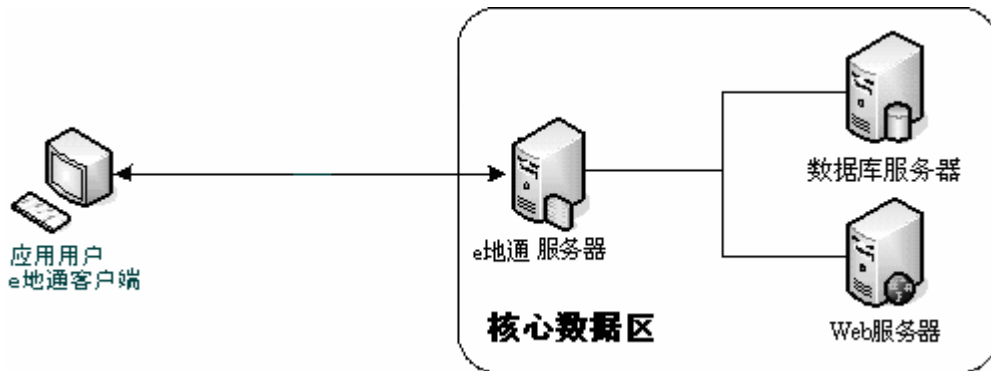


图 代理模式的应用图解

上图给出了代理模式下 e 地通客户端、e 地通服务器协同工作的流程，这个流程可以简单概括如下：

- 1) e 地通客户端监听用户对核心数据区的访问请求，并将该访问请求以 SOCKS5 协议的方式封装并加密起来发送给 e 地通服务器；
- 2) e 地通服务器执行相关的身份认证及访问控制策略，决定是否将该请求转发到目的应用服务器上。

以上步骤简要的概括了代理模式下如何完成应用用户对核心区的访问。

2.2、数据传输中的安全

采用 AES 128 位对称加密算法实现数据传输的加密的；基于 AES 128 加密算法，在 Internet 上建立安全可信的隧道，客户端与服务器之间的数据都是通过安全隧道传递。该加密算法的加密效率比同等级别的 3DES 的加密效率快 3 倍，而加密的密级与 3DES 相当。同时支持第三方算法或硬件加密卡；采用 SHA1 的数据完整性认证保证传输数据的完整性；

2.3、客户端的安全

客户端的安全主要在于环境检测，检测客户端是否安装了防火墙、杀毒软件、系统漏洞扫描存在已经的重大漏洞。在一个全网的安全环境下，在服务器端设置客户端的安全环境要求，只有符合安全环境检查的客户端才能接入到应用服务器，否则，需要提示用户升级处理或者进行客户端的漏洞补丁。

同时支持客户端设备控制：禁止 U 盘、禁止无线网络、禁止红外等，这些都是容易被黑客利用带入病毒的方式与工具，禁止可以降低客户端环境的安全风险。

支持 windows 计算机登陆，拔出 Key 计算机锁屏，确保客户端的计算机上专人专用，不至于在外出的时候或者临时离开的时候被第三方使用，植入病毒、木马类程序。

2.4、身份认证

身份认证模块可以有效地鉴别来访应用用户的身份信息，以及确定其是否具有访问核心区受控资源的权限。传统的身份认证机制往往采用的是简单的用户名和密码的形式，在进行身份信息确认的过程中，通常也是采用明文方式来发送身份信息，比如不支持 HTTPS 的 WEB 邮件系统就是一个典型的例子。这种通过明文方式来进行身份信息认证的过程是非常危险的，攻击者可以很轻松的利用一些常用的嗅探工具（如 Sniffer Pro）就可以得到用户的身份信息。

支持用户名密码认证方式、支持硬件 key 智能卡认证、硬件特征码绑定，U 盘认证、e 地通安全存储 Key 认证、动态令牌卡认证，同时支持新增的第三方认证方式，如 CA 证书认证、RADIUS 认证、LDAP 认证、Windows Active Directory 认证。另外，系统采用模块化设计，支持模块化插入其他加密算法以及硬件加密卡，同时支持模块化新增的认证方式。

支持的认证方式参考《设备性能参数表》。

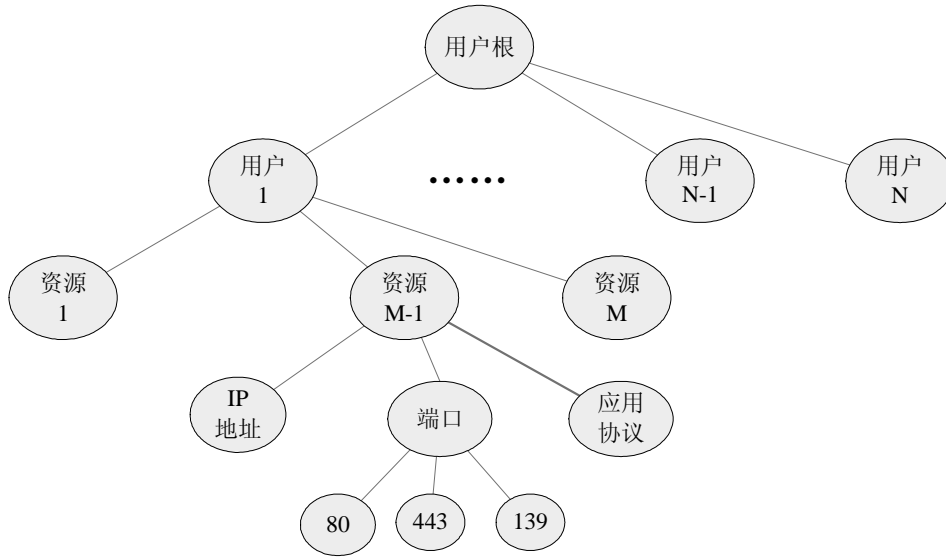


2.5、应用级的访问控制

访问控制可以保护应用用户非法操作对核心区的安全侵袭，切断应用用户对核心数据区指定机器指定应用以外数据的非法访问。评价一个系统是否具有比较高的安全性能指标，一个重要因素就是看该系统提供的访问控制粒度。作为一个好的安全系统，细粒度的访问控制是至关重要的。

e 地通支持基于 IP 地址、端口和应用的访问控制策略，从而方便网络管理员对应用用户访问核心区应用资源进行更为准确和细致的定位。在访问控制的具体实现上，访问控制模块维护了一个全局的访问控制列表，列表中定义了每一个用户的访问权限，包括被访问资源

的 IP 地址、端口号及可以被 RDP 执行的应用程序。可以用一棵资源树型图简单的表示其结构：



用户权限树型图

每一项网络资源都拥有若干种访问权限属性，上图简单列出了最基本的访问权限属性，包括 IP 地址、端口、用户身份、应用程序路径等属性信息。当远程用户发出应用资源访问请求时，访问控制模块可以根据该请求所包含的如下信息：IP 地址、端口号、用户身份、应用协议（协议分析模块分析而得）判定用户的请求是否合法，从而决定是否允许用户进行远程访问网络资源。

根据以往经验，为了充分保证该功能的充分实现，最好不要在核心数据区开放过大过粗的访问权限（如大到整个核心区网段的机器；粗到所有的端口，尤其是文件拷贝和粘贴的功能）。

2.6、VPN 专线效果

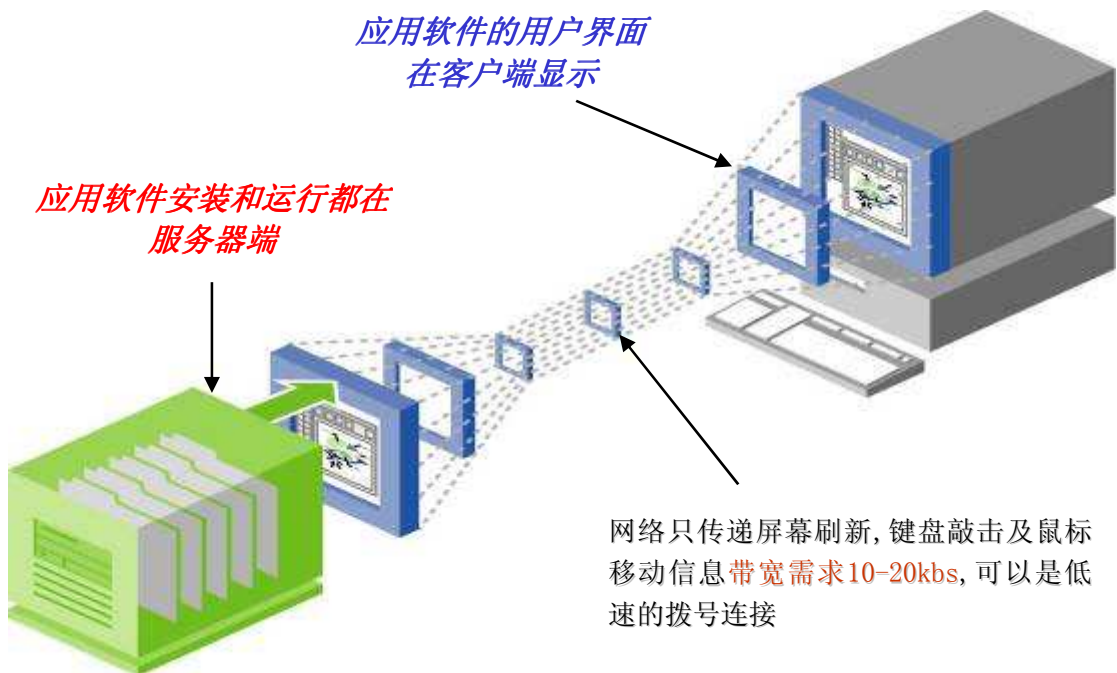
我们的网络控制客户端，在点击运行后，客户端自动断开外网，客户只能通过我们的 e 地通客户端接入到 e 地通服务器以及应用服务器，所有的一切上网操作都进行中断。这样就非常有效的保证了客户端在接入服务器的时候，避免正在上网的客户端威胁到核心数据库的安全！

3、应用集中部署，降低应用的管理开销

e 地通的远程集中接入功能将金财各种业务应用软件集中部署在应用服务器端局域网

中的某台 SERVER 上，集中管理，无需在客户机上安装业务软件，用户也不再受客户端和网络低带宽的限制，让用户在任何时间、任何地点、使用任何设备、采用任何网络连接，都可以高效、安全的访问服务器上的各种应用软件。

- ✓ 对于 C/S 软件的话，可以免去客户端的安装和维护工作。
- ✓ 对于 B/S 软件，因为 B/S 软件是基于 IE 浏览器来访问的，对于客户端的 IE 浏览器的标准程度要求比较高，对非标准的一些东西敏感性比较强，对于客户端的软件环境纯度要求比较高，一旦感染上一些病毒程序，就可能影响 IE 运行该管理软件。所以需要管理软件网络优化设备配套的安全智能存储客户端，把客户端需要下载的一些程序、对 IE 浏览器的修改、对注册表的修改等配置方式全部在后端完成，并存储在该 KEY 里，尽量做到与客户端电脑软件环境无关性，这样可以最大程度的实现客户端免安装、免培训、免服务。
- ✓ 对 C/S 和 B/S 软件均可以降低客户端机器硬件配置和一些常规操作系统的投资成本、以及维护成本。
- ✓ 整个应用软件的维护点只要聚焦在服务器端，这样对于整个系统的稳定运行提供了最小的事故发生点，保证了系统最高概率的稳定运行保障。



三、方案效果

1、提升访问速度 5-10 倍

远程集中接入功能具有强大的应用程序发布能力,它能动态的将应用程序输入输出逻辑与计算逻辑分离,省去 C/S 应用的异地客户端安装和维护工作,实现单笔数据量大,用户数少的应用在 28.8K 的互联网上快速运行.

速度对比表:

不用 e 地通通过映射应用软件端口到公网访问速度(简称访问方式 A)和通过 e 地通远程集中接入(简称访问方式 B)速度对比:

	公网直接访问	e 地通远程集中接入
从页面加载开始到完成进登入界面	05:344S	02:375S
输入用户名密码单击确定后到进入操作页面	2:000S	01:531S
软件内部模块数据处理:总预算会计系统)系 统级基础资料)会计期间模板	05:250S	00:563S

使用 e 地通远程集中接入方式速度的提高在加载新的页面,加载服务器数据时,对比传统访问得到充分体现。加载的数据量越大,效果愈加明显!

对于有一些不能采用远程集中接入模式来解决速度的应用,如单笔数据量并不大,但用户数很多的应用,这种应用如果采用远程集中接入功能就会导致远程集中接入服务器的投资很大,此时采用 e 地通用压缩技术来解决,对服务器端与客户端交互的数据流进行压缩,提高带宽的利用率,压缩算法为 LZO 流压缩算法。以下是一张对比表,用公网传输和 e 地通传输的对比表,来体现压缩的效能。

文件大小(M)	通过e地通使用FTP传输 时间(S)	直连FTP传输时间(S)
11.5M (SQL备份文件)	0:01:10.65	0:04:59.48
6.68M(WORD文件)	0:01:59.61	0:03:06.01
1.61M(Winrar压缩文件)	0:00:30.98	0:00:56.77
6.65M(JPG图象文件)	0:02:20.83	0:03:05.76

2、保障了核心数据的安全

从客户端的应用环境、客户端的身份识别、数据传输的安全、防火墙的边界安全、应用的访问权限到应用服务器的隔离与隐藏,实现了全面的全网络的安全防护体系。

接入的客户端的网络环境是安全的是可以信任的，用户的身份是确定的，应用的访问权限是明确的可以管理的，整个应用服务器（服务器群）是隐藏与隔离的，只留下 e 地通的端口对外服务，所有的风险在设备上，不能透过设备攻击应用服务器群。

3、降低应用系统的 80%维护成本

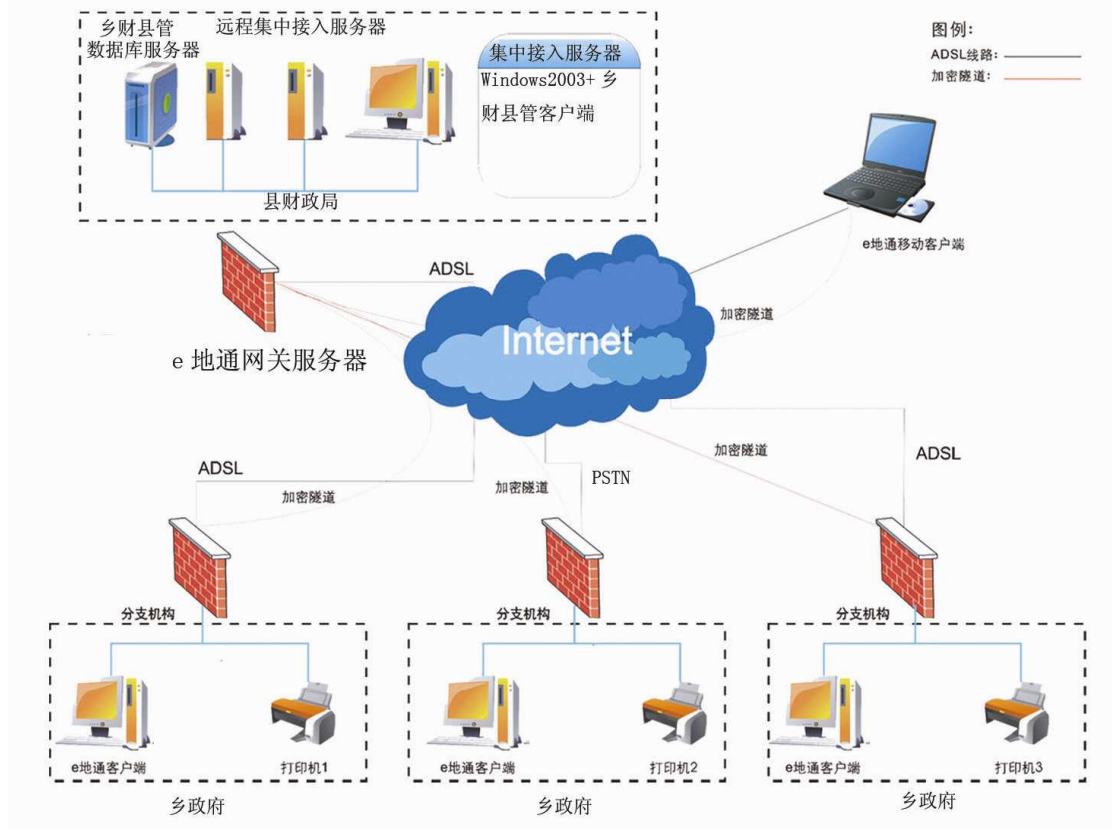
软件升级、维护、故障处理，维护工作就由“面”缩小到“点”，尤其是地域分布较广的用户，将深深体会到原来繁重的维护工作量变得简单轻松。客户端软件对硬件要求低，即使一台 PII 电脑也能运行大型的 ERP 系统，客户端的使用周期延长了 2~3 倍。

由于传统 VPN 多为采用第三方动态域名解析技术来解决 ERP 服务器端 IP 寻址问题，如花生壳、3322 等，但此类解决办法不是正规解决之道，容易出现掉线、不稳定。而且企业信息化系统的成本计算应该与周期挂钩，因为很多费用往往发生在后期的维护与追加投入上，经过验证，采用“e 地通管理软件网络优化解决方案”的系统，在一年的时间里能够比传统解决方案的系统节省 10%~20%，随着时间的延续，这种比例将会越来越大。

4、与应用整合，使用培训费用降低 50%

系统部署后，系统的培训使用成本就是绿色客户端的使用，即插即用的 U 盘使用或者 e 地通安全存储 Key 的使用。即使只有基本的计算机使用人员也会使用整个系统。系统的培训主要关注于应用系统的培训，而不必关注连接、安全、优化类产品

四、产品部署



1、财政局网络

政府内外网用户，通过 e 地通的 WAN 口，该 WAN 口的 IP 与防火墙和其他普通用户在同一个网段，同时在防火墙上把 e 地通的 WAN 口 IP 及 e 地通的应用端口 1111 做个端口映射。管理软件服务器和其他关键应用形成的核心数据区接在 e 地通设备的 LAN 口上，该 LAN 口与管理软件服务器的 IP 地址在同一个网段，要与 WAN 口和其他用户的 IP 网段做成不一样，以屏蔽局域网的普通用户对核心数据区的网络潜在攻击和安全侵袭；核心数据区的服务器无须设网关，同时在 e 地通设备上将这些服务器的内网-外网的所有端口关掉，将服务器主动往外可能产生的安全隐患也全部屏蔽掉。把 e 地通架设在防火墙后面，将管理软件服务器和其他数据库和应用服务器接在 e 地通设备上，做成一个独立的子网——核心数据区，通过 e 地通的防火墙设置，将这些服务器的所有端口关闭。在 e 地通设备上对要来访问的用户进行授权，授权访问细到 IP 及端口。如果外网用户需要访问 C/S 应用的话，需要添置一台集中接入服务器，装上 C/S 应用的客户端程序，做集中发布，其他的用户不用再装 C/S 软件的客户端。在总部需要访问管理软件系统和核心数据区其他应用的用户装上 e 地通的客户端，让他们能且仅能访问指定的应用，屏蔽了内部局域网用户访问管理软件系统可能带来的对服务器的安全侵袭。

2、远程连接模式

在核心数据区前安装 e 地通服务器，在需要访问核心数据区的用户机器上运行 e 地通客

户端或通过指定的 WEB 地址登陆 e 地通服务器，e 地通服务器在代理合法用户去访问指定机器的指定应用。

异地的乡镇，如果要到每个乡镇去安装乡镇的客户端，这是一个很大的工作量，以后的维护工作也会很大。e 地通能够切实的实现把这个维护量减少到最小，节约以后的维护成本。具体的实施方案如下：

在各个县财政局的内网的原有数据库服务器装上应用管理软件的 SERVER 端；并再购置一台服务器装上 Microsoft 2003 Server 操作系统并配置终端服务，并在上面装上应用管理软件的客户端；在乡财政局的网关处配置一台 e 地通硬件设备，在下属的乡政府安装上 e 地通的客户端，无须安装应用管理软件的客户端，通过 e 地通，从乡里面来访问县财政局的应用服务器，实现信息同步共享。

这样一来，应用管理软件以后可能遇到的故障就集中在县里面进行解决，完全不必要安排人到每个乡镇去实地解决，维护工作量大大减少。同时因为 e 地通是一台硬件设备，无须安装，所有配置工作可以在给到客户应用环境前完成，由该公司通过惠尔顿专业认证技术工程师组织一次性配置完毕，该设备随同管理软件安装团队到达每个县，无须再增加 e 地通上门安装调试人员。乡镇人员的机器无须拿到县里安装客户端，惠尔顿专业认证技术工程师将相关个性化信息配置完毕后通过邮件给乡镇人员一个自解压包，乡镇人员双击该自解压包，e 地通客户端就到了乡镇人员的 PC 上，这些操作者点右下脚的 e 地通图标，点远程桌面就进入到乡财县管应用管理软件的登陆界面。

3、需要访问管理软件的用户

需要访问管理软件系统的内外网用户，通过硬件 Key 双因素认证或通过 e 地通绿色客户端的 Key 来实现对管理软件的访问。

也可以采用 4G 的 U 盘或者 e 地通安全存储 Key 实现即插即用的安全连接，在实现客户安全身份认证的同时，将使用者的配置降低到“零”，大大地降低整个系统的培训费用与维护费用。

五、方案预算

1、报价说明

项目的总体报价=产品报价+安装调试费+升级服务费

其中：

产品报价=全国统一报价

安装调试费=项目金额的 10%

2、项目报价

序号	类别	明细	数目	单价 (RMB)	费用 (RMB)	备注
1	根据网络规划，推荐使用 e 地通核心数据的安全防护类产品	W1000SP	1			可以采用两台实现热备份
		客户端授权	m			m=单位的个数
		双因素认证 Key	n			n=Key 的数量
2	服务费	升级服务费	1			三年的软件升级和不限次数上门服务，以及远程和电话维护
		安装调试费	1			产品安装调试和培训，项目金额的 10%
4	合计：					
相关配套环境准备：至少要有 1 台（从备份的角度可以配备 2 台）服务器来做远程集中接入使用，如果没有专用服务器，从安全的角度出发也最好不要与数据库服务器共用，可以与中间层或应用服务器同用一台；该服务器要求：CPU 2*XEON 2.8G ,MEM 6G,操作系统为 windows 2003 Enterprise version，终端授权 100 个。注：该服务器的内存一般按照每增加 1 个用户占用 40M 内存来计算。						

附录 I：所选产品技术参数

分类	性能指标	W1000PG
技术参数	防火墙性能	800*3Mbps
	AES 性能	350M, 200M (3DES)
	并发会话	650000, 新建会话: 90000/S
	接口数量	5*1000M
	internet 捆绑数	4*1000M
	internet 接入	支持 ADSL、LAN、DDN、DHCP 等接入
	智能选路	客户端支持不同运行商网络的智能路由选择
	支持 VLAN	支持内网多个 VLAN, 禁止启动 VLAN 间通讯
远程集中接入特性	速度	将 WAN 的速度变成 LAN 的速度, 提升 5-10 倍以上
	易用性	C/S 变 B/S, 远程无须安全 ERP 客户端
	实施维护	降低实施维护成本 80%以上
	终端安全控制	终端安全管理工具, 文件目录访问控制、注册表、脚本安全
	打印驱动	统一的 vpdf 打印驱动
	输入法	本地输入法, 支持简体、繁体、鼠标滚轮、光标跟随
身份认证支持	用户名/密码	支持最短密码长度 6 位, 要求密码的复杂度
	硬件 Key 认证	双因素认证, 只有拥有 Key 并且知道 Key 的 PIN 码才能认证通过
	计算机硬件绑定	通过绑定计算机 CPU、硬盘、网卡三位一体的 ID HASH 值认证
	U 盘认证	通过 U 盘的硬件属性认证, 支持控制使用天数, 控制使用次数
	e 地通安全存储 Key	硬件 Key 认证与 U 盘认证的完美结合

	动态令牌认证	支持动态的密码口令认证
	CA 证书认证	支持与第三方 CA 证书的导入与认证
	RADIUS 认证	支持标准的 RADIUS 认证服务器，如 FreeRadius
	LDAP 认证	支持标准的 LDAP 认证服务器，如 OpenLDAP
	AD 认证	支持 Windows 的 Active Directory 认证服务器
服务器安全特性	传输协议	SOCKS5 RFC1928, TCP
	服务器隔离	服务器设置与设备相同的 VLAN，不设置网关，逻辑隔离 internet
	加密压缩	AES128 位加密算法，LZO 流压缩算法
	密钥协商	IKE (DH 算法)
	用户权限	移动用户的权限控制，针对服务的权限控制
客户端安全特性	防火墙检查	支持客户端防火墙的安全检测
	防病毒检查	支持客户端防病毒的安全检测
	操作系统漏洞扫描	支持客户端操作系统的漏洞扫描
	WINDOWS 登录	绑定用户登录计算机，拔出 Key 自动锁屏
	VPN 专线效果	客户端连接到应用服务器后自动断开与 internet 的连接
	禁止外设	支持禁止 USB、光驱、软驱、红外、无线网络、CF 卡等
	进程黑白名单	支持（定制支持）
QoS 与路由	QoS 级别	分带宽、分级别的 9 级 QoS 控制
	QoS 控制	支持对 IP 组、时间段、P2P 协议、内容、服务类型的 QoS 控制
	智能路由	支持不同运营商的策略路由，内网用户访问网通的 WEB 选择网通的线路，访问铁通的 WEB 选择铁通的线路
	静态路由	支持静态路由，RIP v2
	多条 INTERNET 线路接入	带宽叠加，负载均衡

	NAT	代理上网功能
	支持 DHCP	支持 DHCP 服务，对内网进行动态 IP 地址管理
	IP 地址映射	将公网 IP 地址，映射到内网的一个或多个服务器，负载均衡
状态检测 防火墙	状态检测	优秀的状态检测引擎为每个访问策略进行状态检测
	包过滤	支持 TCP/UDP/ICMP 的所有包过滤功能
	防火墙模式	支持透明桥模式、NAT 模式、router 模式
	虚拟服务/DMZ	独立 DMZ 分区，并支持（多）端口映射
	阻止攻击种类	支持抵抗 DOS、DDOS、扫描、嗅探、同步等攻击
	Flood 攻击	抵制 TCP/UDP/ICMP 的 flood 攻击检测策略
	过滤规则	支持对 IP 组、时间段、P2P 协议、内容、服务类型的控制
	URL 地址过滤	过滤特殊网站，如：sina.com，过滤所有*.sina.com
	文件类型过滤	过滤特殊类型的文件，如*.exe *.js *.gif，抵制恶意脚本的攻击
	关键字过滤	过滤关键字，如：sex, 法轮功
系统管理	系统管理	全中文 WEB 管理界面，采用 HTTPS 安全连接管理服务器
	日志	本地日志服务器，系统日志、告警日志、错误日志、调试日志、访问控制记录，支持日志的定制
	备份恢复	支持配置数据的备份与恢复

六、服务保障系统

服务是为保证整个系统安全、可靠、高效的运作的重要环节之一，这也是我们公司实现“凸显带宽潜能，增值网络应用”诺言的竞争优势。公司将派专人到现场进行安装、实施与使用培训。各子系统安装完毕后，将把整个系统交给用户，使用户人员能够独立使用，并进行简单的故障诊断排除。

1、售后保障

- ✓ 覆盖全国的服务体系、高素质的服务人员、完善的培训体系是惠尔顿提供高品质服务的有力保障。
- ✓ 服务范围遍及全国各地；
- ✓ 服务领域涵盖金融、电信、邮电、交通、能源、制造、政府、教育等各大行业；
- ✓ 服务时间 7*24 小时，电话热线咨询服务，6*12 小时，远程调试服务；
- ✓ 严格的服务人员要求，对服务人员进行严格制度管理，建立客户投诉电话：0755-26635560
- ✓ 一年多次的服务工程师培训，不定期在视频会议平台或者现场举办客户产品使用培训，加大对客户的培训和支持力度。

2、服务承诺

服务响应时间不超过二小时，现场响应时间不超过四十八小时，硬件故障解决时间不超过二十四小时，软件问题解决时间不超过二个工作日；硬件发生故障四十八小时内无法恢复，三十六小时内须提供不低于中标设备档次的备用设备；硬件返修后七个工作日内无法修复，即予免费更换。（不包括用户违反操作规定、人为损坏的情况）

- ✓ 对于开箱就发现有问题的产品，立即更换；
- ✓ 对于销售不到 30 天发现硬件故障的产品，以新货更换；
- ✓ 三年的硬件免费维护与维修

以下为惠尔顿公司对故障的分级参考标准和规定的响应时间：

故障级别	定义	惠尔顿公司故障响应时间和故障上报时间
一级故障	主要指产品在运行中出现系统瘫痪或服务中断，导致产品的基本	10 分钟内通过 QQ、远程协助工具远程呼入分析问题并解决问题，如需现场解

	功能不能实现或全面退化的故障。	决 4 小时内响应。
二级故障	主要指产品在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能产品的基本功能不能实现或全面退化。	10 分钟内通过 QQ、远程协助工具远程呼入分析问题并解决问题，如需现场解决 12 小时内响应，通过乘坐当地最快的交通工具抵达现场。
三级故障	主要指产品在运行中出现的直接影响服务，导致系统性能或服务部分退化的故障	10 分钟内通过 QQ、远程协助工具远程呼入分析问题并解决问题，如需现场解决 24 小时内响应。
四级故障	主要指产品在运行中出现的，断续或间接地影响系统功能和服务的故障	10 分钟内通过 QQ、远程协助工具远程呼入分析问题并解决问题，如需现场解决 48 小时内响应。

故障响应时间是指公司在接到故障申报后，对该故障提出初步处理意见的时间。

不属于保修范围的情况：

- ✓ 因不正常操作及人为或自然灾害所造成的损坏或故障。
- ✓ 故障产品或部件在未经授权的情况下被拆卸、改装或维修过。故障产品机壳或部件上的产品标识和序列号不清、破损或被涂改过。
- ✓ 有过严重碰撞痕迹、严重腐蚀、缺元器件、主板击穿。
- ✓ 对于以上人为因素或不可抗拒因素造成硬件损坏，公司提供有偿服务。

3、增值服务

免费服务期满后，公司仍为用户提供终身远程服务，但须收取服务费，我们采用合约服务的方式收取服务费用。

(1)、收费标准：根据软硬件设备公开报价的 10% 签订一年期限的服务合同

(2)、服务内容

A. 受理电话、EMAIL、即时通讯(QQ、MSN、视频会议系统)等方式的售后技术服务要求。

B. 7*24 小时，电话热线咨询服务，7*8 小时，远程调试服务。

C. 对于需现场进行的服务，对本市区的硬件可选择性的购买现场服务提供 5 次/年的现场服务；软件一般情况下不提供上门服务。

并由用户按照公司出差标准支付差旅费用。

D. 提供对产品的软件版本升级服务（仅限于服务期内）。

E. 提供服务期内硬件产品的维修服务。

F. 提供服务期内的硬件产品备机服务。

G. 提供服务期内定期回访服务（例行 6 个月一次）。

H. 提供服务期内定期设备检修服务（例行 6 个月一次）。

七、典型案例

- ◇广东清新县财政局
- ◇广东郁南县财政局
- ◇广东清远市清城区财政局
- ◇广东韶关市武江区财政局
- ◇广东省清远市英德市财政局
- ◇广西防城港财政局
- ◇广西上林财政局
- ◇广西田阳财政局
- ◇广西阳朔县财政局
- ◇广西博白县财政局
- ◇广西桂林市全州财政局
- ◇广西柳州财政局
- ◇广西陆川财政局
- ◇广西祈城财政局
- ◇广西田林县财政局
- ◇广西浦北县财政局
- ◇广西兴安县财政局
- ◇广西北海市铁山港区财政局
- ◇广西西林县财政局
- ◇贵州长顺县财政局
- ◇贵州贵定财政局
- ◇贵州紫云县财政局
- ◇贵州荔波县财政局
- ◇福建福州鼓楼区财政局
- ◇福建仙游县财政局
- ◇福州莆田市财政局
- ◇河北沧州财政局
- ◇河北藁城财政局
- ◇河北承德围场县劳动局
- ◇吉林白山县财政局
- ◇吉林农安县财政局
- ◇吉林永吉县财政局
- 广东徐闻县财政局
- 广东乐昌市财政局
- 广东南雄市财政局
- 广东韶关市浚江区财政局
- 广西宾阳县财政局
- 广西百色市财政局
- 广西藤县财政局
- 广西武宣财政局
- 广西宜州市财政局
- 广西大新县财政局
- 广西金秀县财政局
- 广西龙胜财政局
- 广西鹿寨财政局
- 广西岑溪财政局
- 广西灵山县财政局
- 广西省合浦县财政局
- 广西隆林县财政局
- 广西荔浦县财政局
- 广西北海市银海区财政局
- 贵州龙里县财政局
- 贵州瓮安财政局
- 贵州安顺普定财政局
- 贵州从江县财政局
- 福建涵江区财政局
- 福建秀屿区财政局
- 福州三明市财政局
- 河北献县财政局
- 河北省沧州监狱
- 甘肃庆阳财政局
- 吉林延边龙井市财政局
- 吉林汪清县财政局
- 吉林长春市双阳区财政局
- 广东阳山县财政局
- 广东罗定市财政局
- 广东新丰县财政局
- 广东省始兴县财政局
- 广西北流市财政局
- 广西玉州财政局
- 广西天峨财政局
- 广西象州财政局
- 玉林市福绵管理区县财政局
- 广西扶绥县财政局
- 广西灵川财政局
- 广西龙州财政局
- 广西南宁财政局
- 广西容县财政局
- 广西靖西县财政局
- 广西来宾市兴宾区财政局
- 广西融安县财政局
- 广西钦州市钦南区财政局
- 内蒙古全省全区财政局
- 贵州罗甸县财政局
- 贵州兴仁县财政局
- 贵州福泉市财政局
- 湖北恩施地方税务局
- 福建荔城区财政局
- 福州南平市财政局
- 河北平山县财政局
- 河北丰宁财政局
- 河北省塞罕坝林场
- 甘肃省天水市麦积财政局
- 吉林桦甸财政局
- 吉林磐石市财政局
- 吉林舒兰市财政局

◇吉林通榆县财政局	吉林省敦化市财政局	吉林省蛟河市财政局
◇辽宁鞍山财政局	辽宁建昌财政局	辽宁北票市财政局
◇辽宁朝阳市财政局	辽宁辽阳市宏伟区财政局	辽宁辽中县财政局
◇辽宁铁岭市财政局	辽宁辽阳市太子河财政局	辽宁辽阳市弓长岭财政局
◇辽宁沈阳市东陵区财政局	辽宁沈阳振安区财政局	辽宁丹东市地税局
◇辽宁大连庄河市财政局	辽宁沈阳市皇姑区财政局	黑龙江北安市财政局
◇黑龙江黑河市财政信息站	黑龙江呼兰财政局	湖南邵阳市隆回县财政局
◇湖南桂东县财政局	湖南冷水江财政局	湖南湘潭市财政局
◇湖南永顺财政局	湖南长沙芙蓉区财政局	湖南长沙民政厅
◇湖南祁东财政局	湖南武山财政局	北京市石景山市政所
◇江苏贾汪区财政局	江苏徐州市容管理局	江苏宿迁广电局
◇江苏无锡锡山区财政局	江苏无锡滨湖区财政局	江苏徐州铜山财政局
◇江苏南通海安县财政局	江苏南京市财政局	江苏省宿阳县财政局
◇上海社会保障局	上海浦兴街道社区	四川仁川财政局
◇四川北川财政局	四川古蔺财政局	四川江油市财政局
◇四川乐至财政局	四川沐川财政局	云南玉溪易门县财政局
◇云南新平县财政局	云南玉溪市红塔区财政局	云南普洱市景东县财政局
◇新疆阿克苏财政局	新疆乌恰县财政局	乌鲁木齐质量监督局
◇新疆沙雅县财政局	新疆新源县政府	河南郑州市管城区财政局
◇河南驻马店驿城区财政局	河南驻马店新蔡县财政局	河南驻马店确山县财政局
◇河南周口项城财政局	河南驻马店西平区财政局	河南驻马店正阳县财政局
◇河南焦作市审计局	河南新乡市牧野区财政局	河南驻马店遂平县财政局
◇河南驻马店汝南县财政局	河南驻马店平舆县财政局	河南驻马店泌阳县财政局
◇河南驻马店上蔡县财政局	山西长治村务公开	山西省长子县农经局
◇天津滨海新区	天津市和平区财政局	天津市河西区财政局
◇天津南开区财政局	山东德州市安监局	山东青岛市李沧区财政局
◇山东淄博农村养老保险	安徽太和县财政局	广东韶关粤北开发区财政局
◇内蒙古赤峰克旗财政局	内蒙古赤峰市敖汉财政局	内蒙古赤峰市右旗财政局
◇内蒙古赤峰市翁牛特旗财政局	内蒙古赤峰市宁城财政局	内蒙古赤峰市松山财政局
◇内蒙古赤峰市元宝山财政局	内蒙古赤峰市左旗财政局	内蒙古赤峰市巴旗财政局
◇内蒙古赤峰市红山财政局	江苏省工商行政管理局	上海市浦东新区运政管理署
◇贵州贵定县财政局	厦门市政工程	

八、关于惠尔顿

稳步发展的惠尔顿

深圳市惠尔顿信息技术有限公司（简称惠尔顿）自成立始，即本着“凸显宽带潜能，增值网络应用”的经营理念，作为“管理软件网络优化”解决方案的提出者，全心致力于为全球范围内网络通讯运营商及企事业用户提供全面的网络优化解决方案。为管理软件在网络上的更安全、更快速、更稳定、容易管理运行做持续的毕生的努力。

公司位于深圳市南山区高科技园区内，由资深管理人员和精通网络技术的专业人员组成，其中博士、硕士多名，本科以上学历占公司总人数的 85%。经过数年的沉淀与积累，公司拥有庞大的精通 VPN 技术的专业化网络安全研发队伍，在底层网络协议、数字签名认证、安全控制等方面拥有丰富经验，在 WAN 优化(即公司的加速 VPN)、特定协议优化(如 HTTP、POP3、SMTP、IMAP、数据库)、流量管理、协议分析，更是有不俗的表现。

前几年，凭借对现实中 2 万多个异地互联方案的专业考察，在国家 863 研究成果的基础上，相继推出两大系列、三十余个核心产品。凭借着我们实力雄厚、技术领先的研发队伍开发出全球首家 SOCKS V5 VPN。我司产品具备安全稳定、操作简单、投资成本低等特点。

在公司全体员工及合作伙伴精诚协作和不懈努力下，惠尔顿规模不断发展壮大，业务范围不断拓展，社会影响力不断提升，e 地通系列 VPN 产品在连锁、房产、电力、气象、医药制药、医保社保、民航售票、政府部门、建筑业、制造业等行业已经得到广泛应用。

随着公司业务的发展，新产品线的加入，公司的服务对象层次不断提升，从 2007 年起，公司在政府的财政、新农村合作医疗、医保、税务等都取得了长足的进步。

面对网络通信市场的机遇和挑战，无论是过去、现在、还是将来，我们都深刻理解用户的真正所需，为用户提供卓越的网络信息化产品和服务，这是惠尔顿的永恒动力。惠尔顿深知只有技术不断创新、售后服务更为完善，以过硬的产品和人性化的服务才能赢得客户、赢得未来。因此，惠尔顿将以技术创新为依托、以一流的服务为保障、以高效的管理为手段，不断推出更新、更好的产品，与广大的客户共迎信息革命的挑战！

内部建设

公司员工 100 多人，40%的员工持股，其中研发人员 30 多人，公司内部有基本法。

公司的高层由三个部分组成：员工代表委员会、审计部、总经理

总经理下属的主要智能部门有：研发部（含开发部、前沿技术实验室）、客户服务部、市场企划部、市场渠道部、行政财务部。

技术实力

惠尔顿拥有一支 30 多人的研究和开发队伍，其中 10% 是博士，20% 是硕士，80% 以上为大学本科学历，大部分成员在网络和信息安全领域有丰富的研究经验，并在网络和信息安全体系结构包括网络通信和管理、安全操作系统、PKI 技术、入侵检测、人工智能、数据挖掘和分析、以及密码学等方面已经取得了一定的成果。北京研发中心目前正在应用层安全体系结构、IP 层安全体系结构、操作系统安全、PKI、安全日志服务器等方面开展深入的研究。

惠尔顿的科研合作单位北京交通大学信息安全体系结构研究中心得到了国家 973 项目“信息与网络安全体系结构研究”和 863 项目“计算机信息系统安全体系结构研究”支持，为与惠尔顿的合作做好了充分的前期基础研究准备工作。该中心学科带头人沈昌祥院士是我国信息系统工程、信息安全专家。在信息工程与计算机网络安全领域中，研制成功海陆兼容的信息处理系统、保密通信电报网络系统，并主持研究计算机安全操作系统等，取得了突破性的进展。曾获国家科技进步奖一等奖 2 项；国家科技进步奖二等奖 2 项。

同时，美国密苏里大学作为惠尔顿的合作单位，为惠尔顿了解国际前沿技术、基础研究的最新动态提供了窗口，为我们研制的产品具有国际技术领先性提供了保障。

分支机构

公司总部位于深圳，同时，在广州、上海、北京设立直属分支机构，在成都、杭州、江苏、西安等地建有办事处。

发展历程

“凸显宽带潜能，增值企业应用”是我们的使命。

我们全心致力于为中国用户提供基于中国国情，富有中国特色的“增值企业应用”贴身解决方案。

成立于 2000 年 6 月。刚成立与长城宽带合作开发宽带社区，在几十家合作伙伴中脱颖而出成为长宽签约量最多，样板工程最多的公司，也被纳入最早与其合作宽带运营的公司之一；

2001 年至 2002 年，逐步关注网络安全领域，对诸多信息化建设项目进行专业考察；

2003 年涉及 VPN 领域，横跨多个行业，为客户提供 VPN 远程互联咨询、设计及产品服务；

2004 年，凭借对现实中 2 万多个异地互联方案的专业考察，在国家 863 研究成果的基

基础上，我们实力雄厚，技术领先的研发队伍开发出了中国首家 SOCKS V5 VPN；借助第六届深圳中国国际高新成果交易会的平台，正式向外推出拥有自主知识产权的“e 地通”VPN 系列产品。技术领先于中国乃至全球，同时我们立足于“将中国国情转变为中国特色”，所以产品非常适合我们的广大客户。

2005 年，研发出 SOCKS V5 + 集中接入平台，推出集成防火墙、高速路由、远程集中接入、VPN 等功能的全系列硬件产品。由北京交通大学与惠尔顿共同成立<交大惠尔顿安全实验室>；同年，通过深圳市软件企业和软件产品认证，并被深圳市软件行业协会评为“深圳市年度优秀软件产品”，

2006 年，SOCKS V5 ， IPSec 硬件产品，集合多功能防火墙、高速路由、VLAN 等，同年，惠尔顿公司 Socks5 VPN 项目被国家科技部列为“2006 年度国家重点新产品计划项目”，并获取了经费鼓励，并成功进入政府行业，被广泛应用于新疆、内蒙古、江西、广西、福建等地区的乡财县管和财政集中支付项目。

2007 年，率先提出“管理软件网络优化专家”解决方案，为管理软件网络运行护航，整合公司的产品线为远程集中接入、SOCKS V5 VPN、IPSec VPN/防火墙的“三合一”产品线、SOCKS V5 VPN、IPSec VPN/防火墙的“二合一”产品线；

2008 年 6 月，推出“应用加速”系列产品(公司命名为“加速 VPN”，国外厂商命名为 WAN 优化产品)，使得管理软件运行速度得到显著的提高，同年，推出 e 地通安全存储 Key，进一步简化了 VPN 在 internet 上的使用，该产品完整地解决了 VPN 终端可信的短板。

2009 年 10 月，我们推出了“流量管理”与“上网行为管理”产品线，力促管理软件在网络上运行的更平稳，提升了企业运行的效率，同时规范了企业网络的法律法规风险；

2010 年，我们将沿着“凸显带宽潜能、增值网络应用”的远景，完善现有的的产品线，实现管理软件网络优化的目标，保障网络应用更安全、更快速、更稳定、可管理可视化运行。

主要业务领域

惠尔顿公司本着“凸显带宽潜能、增值网络应用”的经营理念，利用当今网络中最前沿的技术促使应用软件在网络的运行的更安全、更快速、更稳定、更容易管理。在此理念的带领下，我们开发了保障应用安全的核心数据安全解决方案、管理软件网络优化解决方案，保障应用稳定运行的流量管理解决方案，逐渐形成以流量管理为核心的支撑整个应用交付的应用安全、WAN 优化、负载均衡一揽子解决方案。

为最终用户将管理软件使用好的网络优化平台——优化速度、保证安全、便于应用、利

于维护。我们与国内几大管理软件厂商捆绑销售，最终用户是通过为应用软件运行效果好来检验我们的产品。目前的最终用户主要集中在大企业和政府。

特点优势

惠尔顿不会对最终用户说：“这不是我们的事情”，造就了我们爱负责任，比人家多走一步的特点和优势。我们在公司内部建立了“立刻相应”的客户系统，将客户的服务作为公司的立身之本。

一、