VA 虚拟应用解决方案

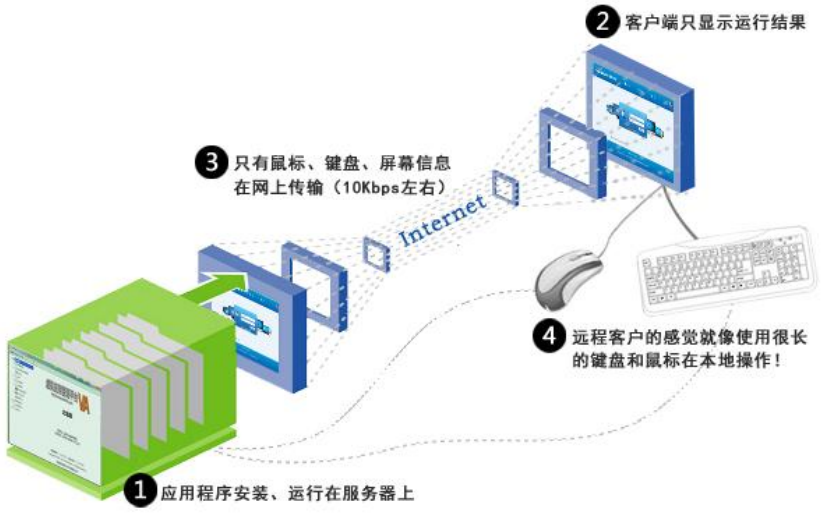
目　录

1 概述

1.1 背景概述

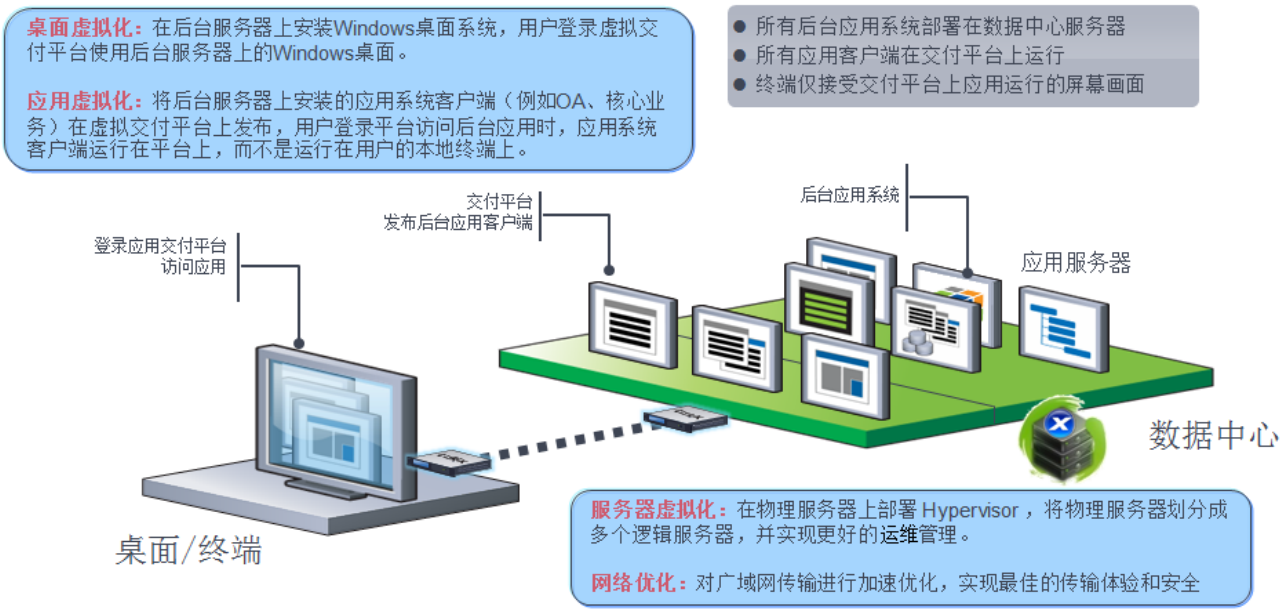
继个人计算机、互联网变革之后，2013 年，云计算作为 IT 浪潮的代表正在向我们走来。它将带来人类生活、生产方式和商业模式的根本性改变，成为当前全球关注的热点。目前，云计算的解决方案、安全问题以及接入方式的完善是云计算最为核心、最为迫切需要解决的问题。

VA 虚拟应用管理平台是基于服务器计算架构的应用接入平台。它将用户各种业务软件集中部署在 VA 服务器(群)上，通过 VA 通讯协议---VAP 协议，即可让客户端快速安全稳定的执行服务器上的应用软件，轻松建立企业自己的私有云平台，轻易实现用户在任何时间、任何地点、使用任何设备、采用任何网络连接方式，高效、安全的访问企业应用和资源。



VA 是构建在 Microsoft Windows Remote Desktop Service(RDS，原 Teminal Service)基础之上，并提供了大量扩展的增强功能，用户可以使用各种终端设备，以会话共享的方式，访问运行在 Windows 2003/2008 服务器上的应用程序或共享桌面。每个用户仅仅能够看到自己的会话，不同用户之间的会话是隔离的。应用程序在数据中心服务器上执行，显示屏幕和键盘等输入通过网络进行传输，没有真正的业务数据在网络传输。

1.2 VA 云计算



通过上图和服务器虚拟化、桌面虚拟化的比较，可以看到，应用虚拟化对原有的基于应用客户端访问后台应用系统的架构中间，进行了平滑的改善。原有的后台应用服务器及局域网访问保持原样不动，只是在前端用户和后台应用服务器之间增加了虚拟应用交付平台的部署，主要实现对各种应用客户端的集中部署和管理，这样可以大大减少 IT 维护，并能全面提升远程访问的效率，并且由于客户端软件不再扩散到整个桌面，管理得到进一步加强，系统整体安全性得到提高。

VA 云计算中的 ARS 应用服务器的核心是 VAP 协议，该协议连接了运行在平台上的应用客户端运行环境和远端终端设备，通过 VAP 的虚拟通道（分别传递各种输入输出数据如鼠标、键盘、图像、声音、端口、打印等等）运行在中心服务器上的应用运行环境的输入输出数据重新定向到远端终端设备的输入输出设备上，因此虽然应用客户端软件并没有运行在客户端设备上，但是用户使用起来和在客户端安装运行客户端软件相比，没有感觉任何操作上的改变。

VAP 协议是一种高效率的数据交换协议，采用了数据压缩、加密和连接优化技术，每一个用户的连接只占用少量的网络带宽，而实际运行的客户端软件位于后台的局域网内，因此终端用户相当于用少量的网络带宽就可以享受到局域网内的运行速度。如系统客户端和服务器之间有大量的数据交互，使用集中模式

可以有效地降低数据传输，大大提高整体性能。同时 VAP 协议可以分别针对单独的虚拟通道进行控制，这样为用户的访问和使用带来了细粒度的控制。

1.3 企业应用需求

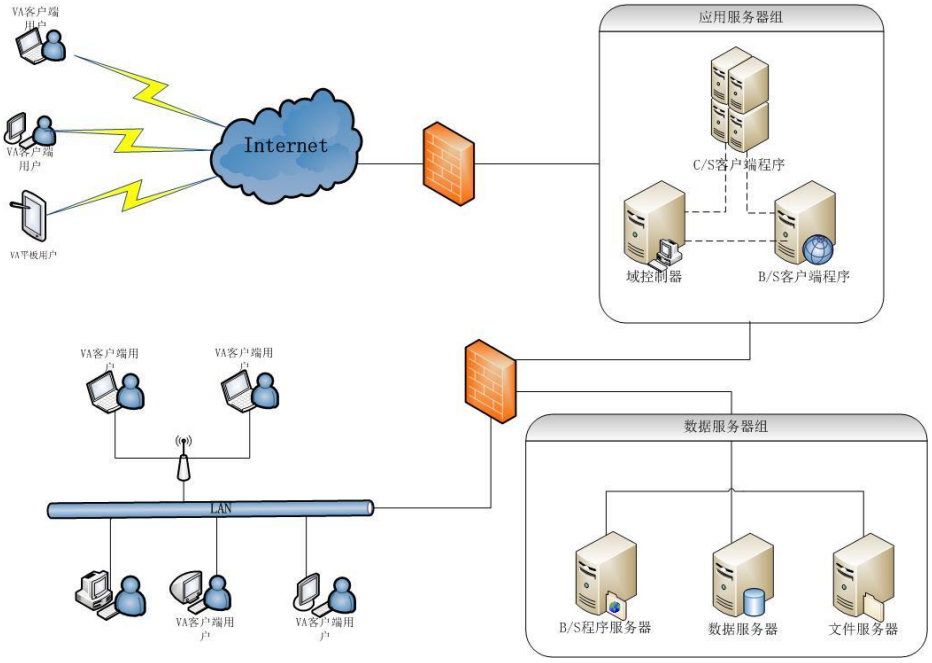
当前企业组织在存在大量应用（ERP、CAD、OA 等）信息系统及硬件设备是时，都会面临更有效率和安全的使用这些资源的问题，比如：所有客户端设备的安全上网，公司内部资源的访问、数据资源的集中管理、应用系统的安全登陆等等问题。如果分别采用不同的解决方案也能达到效果，但会导致企业资源的使用成本居高不下，同时各种解决方案的兼容性也会影响整个系统的稳定。采用 VA 云计算方案可以综合解决以上这些问题。

2 企业应用解决方案

2.1 应用集中

随着信息技术的发展，企业中大量存在着各种应用软件，如财务软件、个人应用、ERP、OA、CRM……它们分布在单位的各种服务器和个人电脑上，IT 管理部门管理和维护这些系统分身乏术，个人用户使用应用时操作繁琐、问题频发，解决这些问题的最好办法是让用户在一个环境中看到所有企业应用资源，甚至不需要原账号即可正常使用企业应用资源，

VA 云计算解决方案可以将用户各种应用软件（ERP、OA、CRM……）集中部署在 VA 集群服务器上，客户端通过统一认证快速安全地操作使用服务器上的各种应用软件 ;客户端也不再需要安装任何应用软件，应用管理软件的升级、打补丁、维护都集中在服务器上完成。



2.2 安全上网

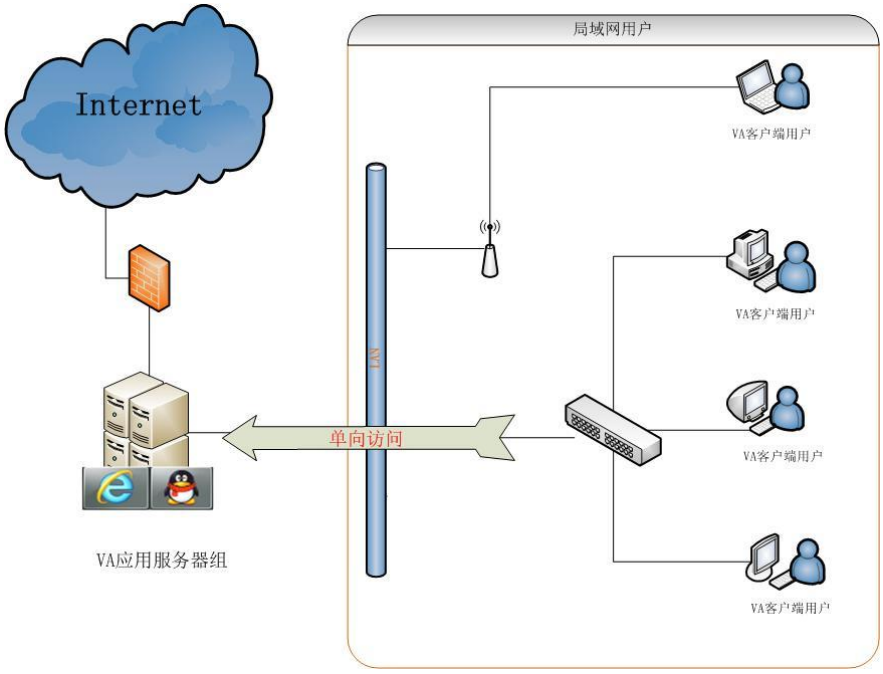
企业一般解决安全访问问题的方法是通过在网关处架设防火墙、杀毒软件等解决网络安全的访问控制

和安全漏洞，但防火墙等设备实际上仍然会有大量的安全因素穿透过去，成为安全隐患。

通常，系统安全与性能和功能是一对矛盾的关系。如果某个系统不向外界提供任何服务（断开），外界是不可能构成安全威胁的。但是，企业接入国际互连网络，提供网上商店和电子商务等服务，等于将一个内部封闭的网络建成了一个开放的网络环境，各种安全包括系统级的安全问题也随之产生。

采用这种网络结构的企业，局域网内用户一般通过路由器使用 NAT 或代理服务器访问外网，然后通过防火墙端口限制机制使用户的各种访问无法访问外网，这样导致很多对外的正常联系也不能够完成，而企业希望做到的应该是最大范围的“可控”的外网访问，采用 VA 虚拟应用系统并合理的部署可以使用户虚拟访问互联网络，能够使用任何软件（QQ、浏览器等等）间接访问互联网，用户可以“看到”所有的访问资料，但却仅仅是看到，无法直接获得数据，这样可以保证所有内网电脑既可以正常使用软件有可以保护内网所有的安全，而用户想要直接获得数据也可以通过审批的权限获得。

采用 VA 云计算的部署方式是网关处部署 VA 虚拟应用服务器，内网用户通过 AR 应用执行器运行 VA 服务器上的应用（浏览网页或运行各种网络工具），这样，内网用户能够通过这些发布的应用不受限的使用各种网络资源，同时这些网络数据并不会流入内网，保证了内网绝对的安全性。



这种部署方法的可以做到完美的内网防护作用：

a) 利用路由器几乎完善的 WAN 口的外网隔离作用保护内网

b) 内网用户只能通过映射端口后的 AR 访问 VA 应用服务器 ,再通过 VA 应用服务器上发布的应用完整、可控的使用互联网

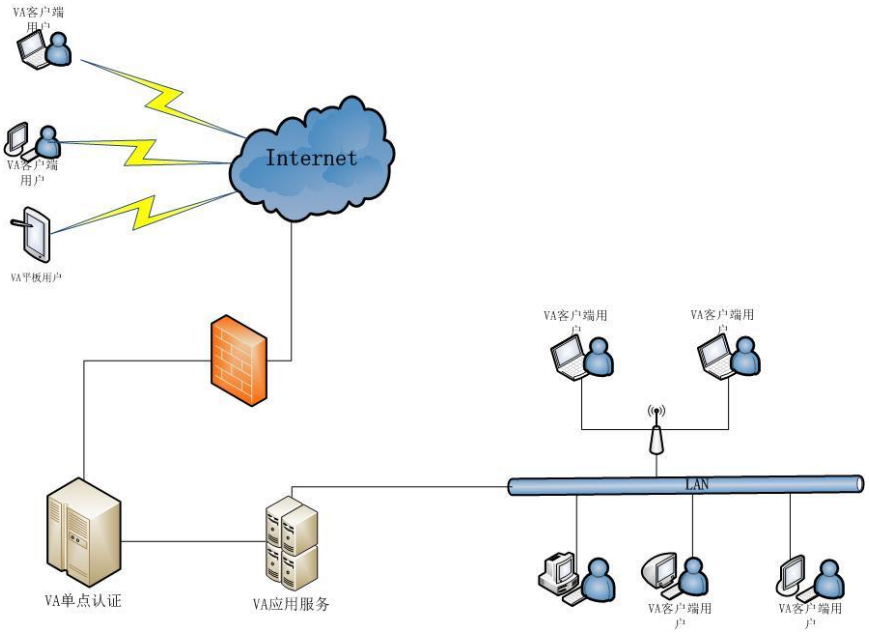
c) 双向隔离 VA 服务器：不论是 internet 还是局域网用户都无法通过其他方式访问到 VA 服务器

d) VA 服务器上的所有发布的应用操作可审核、打印可记录、使用可管理（细粒度的时间、人员等的管理）

e) 局域网用户也可以经过 VA 管理员授予获得真实数据的权限，获得的数据也可以审核。

f) 这种内网电脑管理的方式才可以真正做到隔离访问互联网。

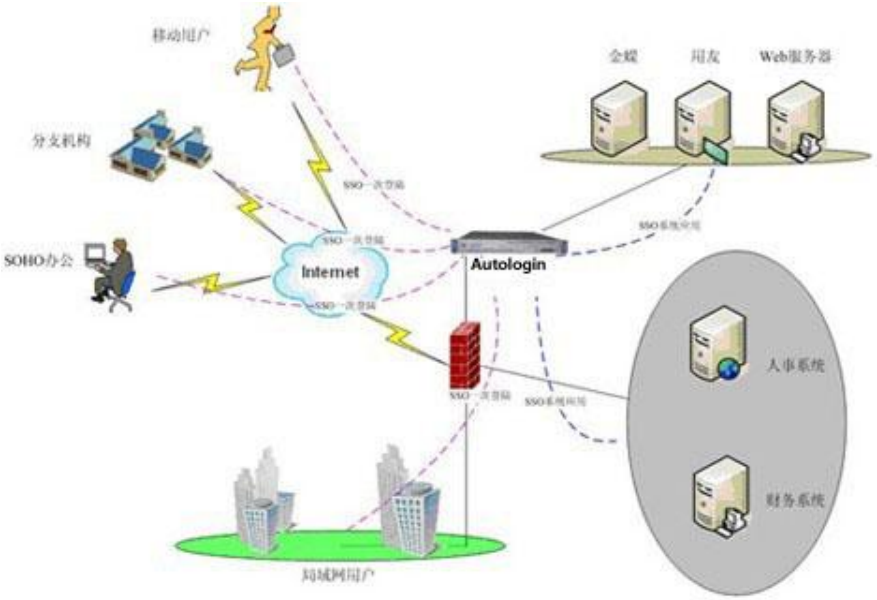
2.3 单点登录



处于信息技术高度发达的今天，众多的业务系统，用户需要在不同系统间频繁切换造成账户或密码遗忘，同时，企业需要大量的 IT 技术管理人员分别管理维护不同系统的用户信息。针对此问题，VA 单点登录功能为企业用户提供统一的信息资源认证访问入口，建立统一的、基于角色的和个性化的信息访问平台，

通过实施单点登录功能，用户只需一次身份认证，就可以对所有被授权的应用系统进行访问，无需重复输入密码；系统管理员只需要维护一套身份认证平台，提高信息系统的易用性、安全性、稳定性。

VA 单点登录功能被称为应用程序自动登录（AutoLogin），用户只需要将密码一次设置到 VA 系统中，则在 VA 系统中集中发布的应用就可以直接一次登录，同时密码被加密保存到 VA 系统中。



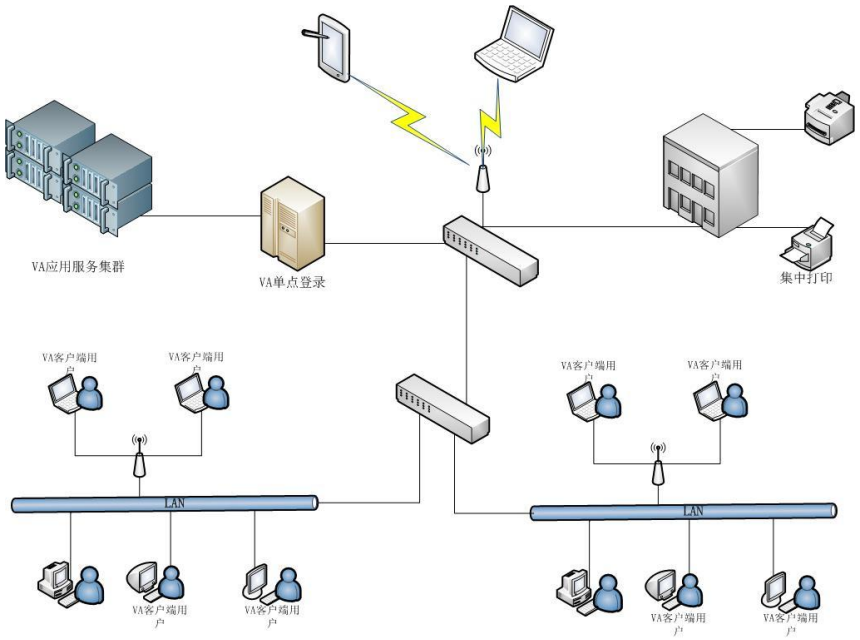
应用优势

- 单点登录：用户只需登录一次，即可通过单点登录系统（AutoLogin）访问后台的多个应用系统，二次登陆时无需重新输入用户名和密码
- 广泛适应性：业务系统可以为异构系统，其运行的操作系统平台和应用服务器可以各部不同，客户端可以适用不同的浏览器的需求
- 即装即用：现有的业务系统和应用模式无需任何修改即可实现 C/S 单点登录系统
- 基于角色访问控制：根据用户的角色和 URL 实现访问控制功能
- 全面的日志审计：精确地记录用户的日志，可按日期、地址、用户、资源等信息对日志进行查询、统计和分析
- 多种认证方式：满足用户名/密码认证，用户名/seamoon 动态密码认证，还能实现少 数用户通

过 USB KEY 等硬件认证

- 集群：通过集群功能，实现多台服务器之间的动态负载均衡
- 传输加密：支持多种对称和非对称加密算法，保证用户信息在传输过程中不被窃取和篡改
- 可扩展性：对后续的业务系统扩充和扩展有良好的兼容性

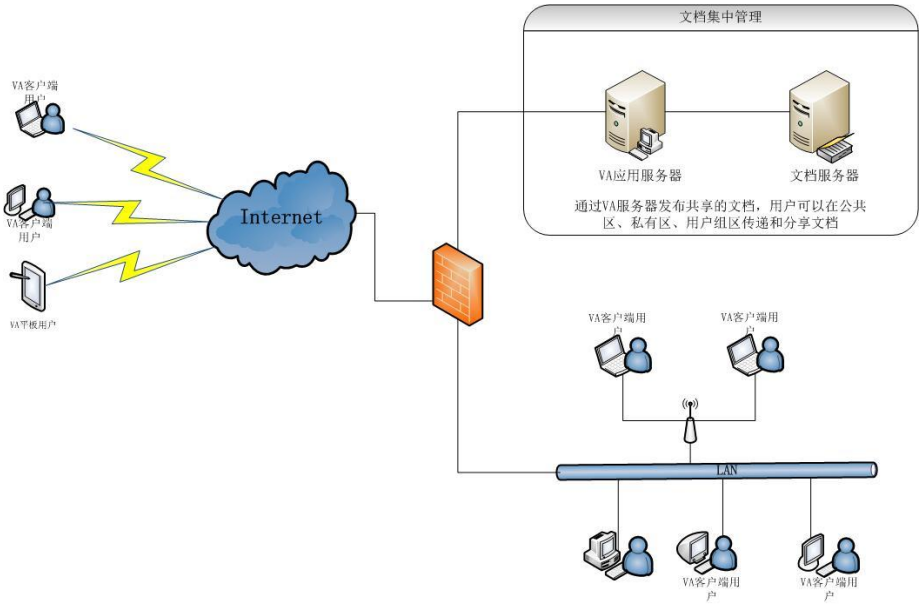
2.4 局域网应用



虚拟应用并不仅仅只能在 Internet 上部署，更多的可以在企业内部网上部署，内部网络的带宽可以保证局域网应用体验更理想，更好的实现企业集中统一资源、降低 IT 管理成本、保证数据安全等作用效果。

企业中大量存在的信息孤岛，导致整个组织的数据无法共享、无法统一管理，甚至企业的信息管理部门选择了类似“管理驾驶舱”的解决方案，希望全局把握企业各方面状况时，也往往在细微的数据集中层面无法实现。VA 虚拟应用提供了一种解决办法，用户可以在企业信息中心上集中部署各种应用，通过 VA 实现用户层面的操作，信息中心集中将数据统一管理，再进一步通过适当的开发或通用软件就可以轻松实现数据整合。

2.5 文档集中管理



不论企业大小都有大量的各种文档和资料需要管理，不同的文档对于不同的使用者有不同的权限，集中统一存放的资料就相当于企业的图书馆一样，给予用户不同权限才能保证文档资源的安全。

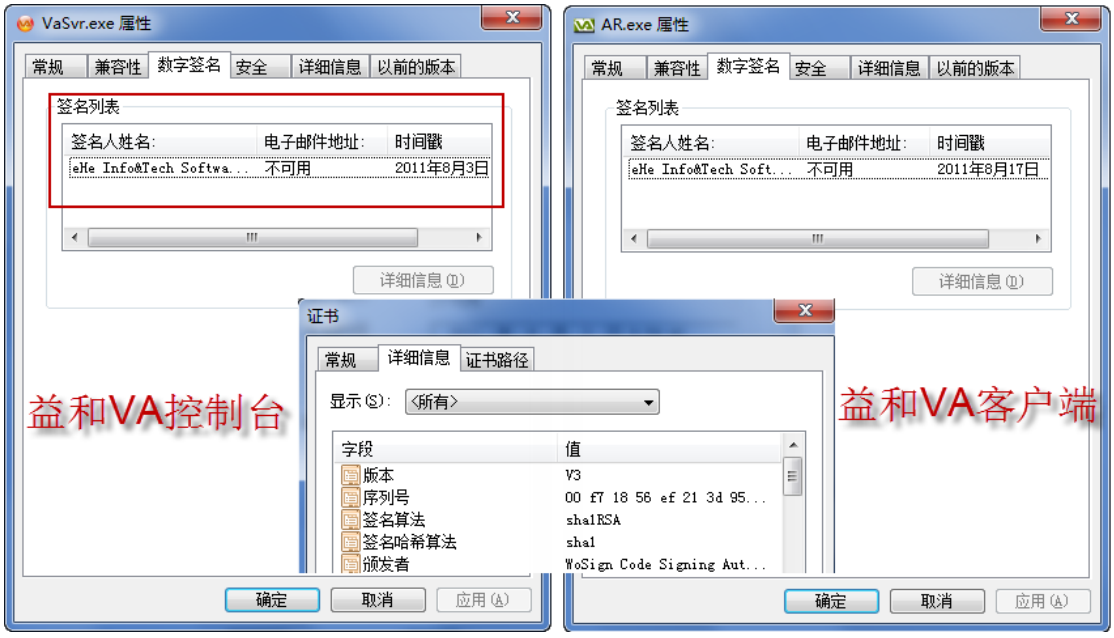
VA 虚拟应用系统提供服务器存储资源的发布，VA 文件夹发布可以提供给用户公共文件夹、私人文件夹、同组用户文件夹、互传文件四种文件夹类型，公共文件夹的文件所有用户都可以看到，企业可以通过此处发布公告文件；私人文件夹只有自己能够看到，用户可以保存自己的私人文件资料；同组文件夹可以看到在同一个组中共享的文件；用户之间也可以互传文件资料。整个过程用户不需要知道文档资源在服务器存储的具体位置，同时设定不同的用户权限可以方便、细致的管理用户对你每个文件夹的读写传权限。

3 VA 系统设计

3.1 多重技术保障

3.1.1 数字证书认证

益和 VA 服务器端和客户端程序分别封装了网络数字证书，通过权威的 CA 机构，即证书授证（CertifVAPte Authority）机构颁发数字证书，让控制台和客户端程序在任何系统环境下均能通过各类程序验证，保障程序运行的稳定性以及排除被意外查杀的可能性。



3.1.2 服务器负载管理

益和 VA 对所依赖的操作系统精心呵护，对资源采用了动态分配和轮询式的负载均衡管理办法，并可以根据每一台服务器的负载能力进行个性化权重设置，保障服务器集群整体性能的发挥，避免在多服务器情况下由于资源分配不均而影响性能甚至导致宕机。

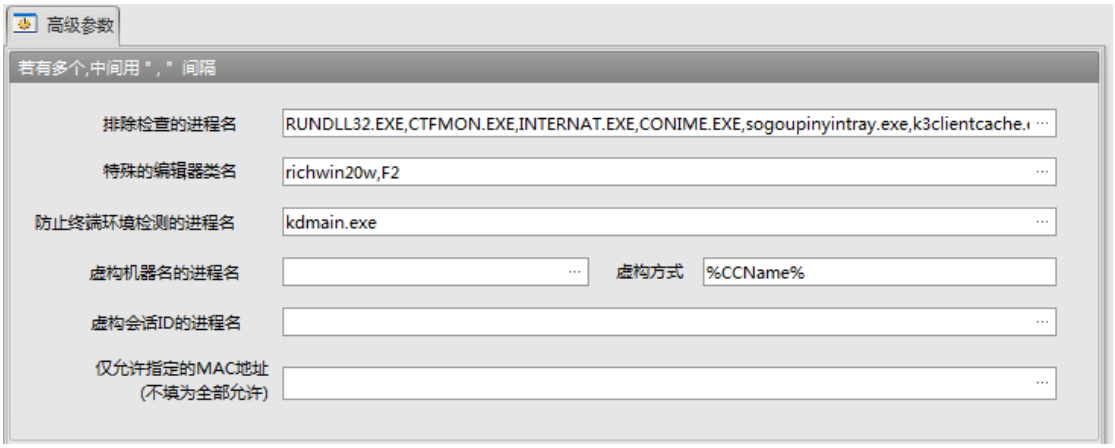
3.1.3 服务器硬件管理

对服务器核心硬件监控并管理，对超负荷运行的硬件及连接异常直接进行报警。通过对单项硬件资源的管理，可以在超负荷或者意外情况出现时人为介入，保障服务器流畅运行。

3.1.4 高级参数设置

对于特殊应用程序，如特殊部署方法、特殊进程的关联性导致无法正常退出、特殊应用程序不允许打

开多份等情况，益和 VA 提供了高级参数设置，通过相关参数的设置，保障稳定应用诸多个性化特殊环境的程序。



3.1.5 多动态域名容错

更多中小企业都是使用的 xDSL 方式上网 ，在没有固定 IP 连接时，需要安装域名进行 IP 解析，存在三种可能出现的问题： 一是需要安装域名客户端软件，二是某个域名解析错误时或者故障则无法访问，三是申请多个域名就需要记住多个域名。

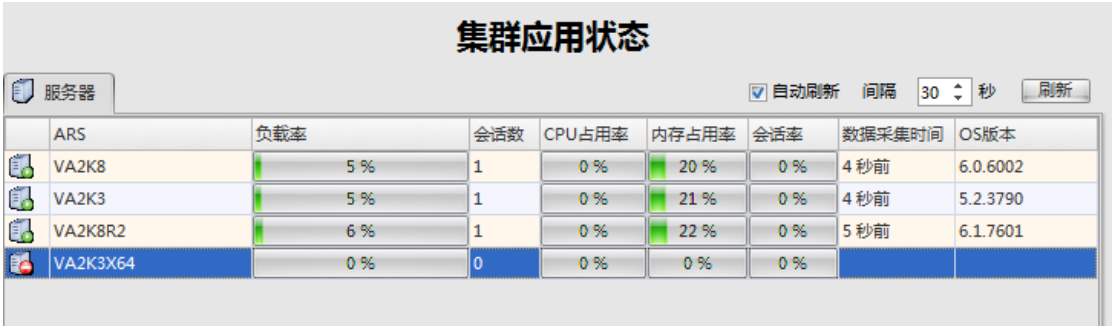
为解决此类问题，益和 VA 内置多动态域名引擎，直接在控制台-〉动态域名 栏目下 输入域名相关登录信息，AR 客户端软件自动寻址，实现域名解析，无需安装动态域名客户端软件；同时提供域名容错功能，在某个域名故障时，客户端软件 AR 选择备用的可以正常使用的域名进行登陆，彻底解决了用户申请免费动态域名、域名解析有时不稳定的问题。用户从此不用担心连接不上 。

3.1.6 控制台自动修复

益和 VA 服务器端核心服务 VaSvr.exe 采用“看门狗”机制，在该服务遭遇意外被查杀时、意外终止时，只需 1 秒的时间则能自动重新启动，恢复该服务，保障服务器益和 VA 控制台稳固运行。可以尝试在任务管理器中将 VaSvr.exe 强行停止，会看到瞬间该服务又自动启动恢复。

3.1.7 服务器集群管理

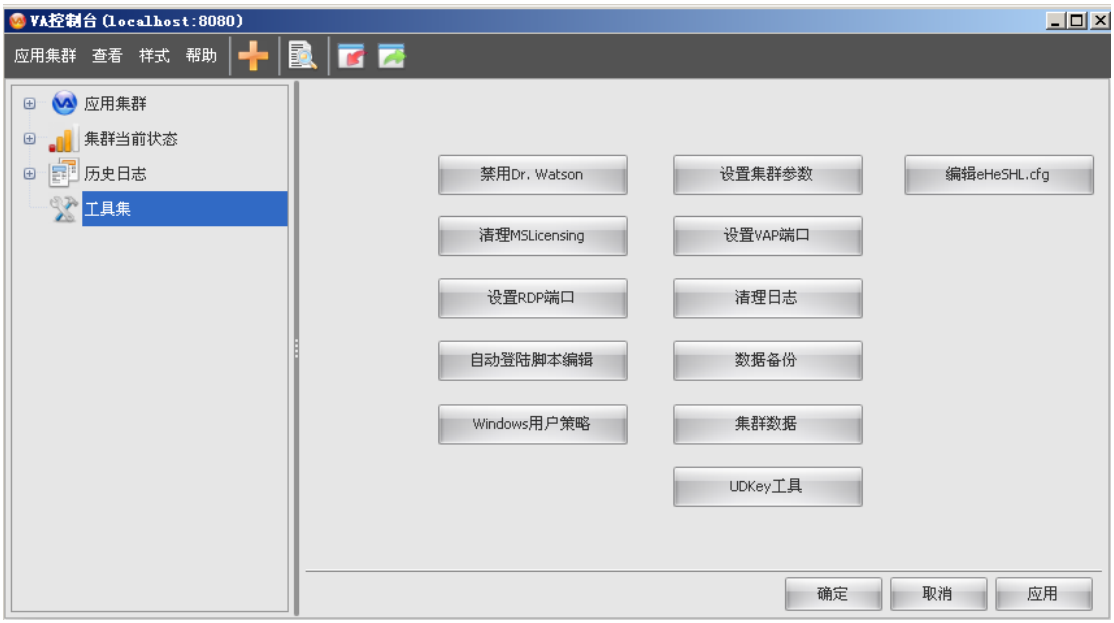
益和 VA 集群状态管理，可以实时监控当前多服务器集群情况，红色表示服务器有问题，同时也可以对负载率过高的服务器直接右键注销，经过实测，被注销的服务器，用户会自动迁移到正常的服务器上，同时，新访问的用户，按照设置好的负载均衡管理办法，也会自动的连接到正常的服务器上。集群状态下，只要资源的部署有适当富余量，就不会因为个别服务器宕机而影响整个 IT 系统的运行。



3.1.8 辅助工具集

益和 VA 提供了辅助工具集，管理员可以用简单的命令即可调出，在辅助工具集里可以对当前系统和 VA 程序进行各种设置和数据备份，在某些特殊情况下（如遗失控制台密码、端口冲突等），可以直接使用

此工具进行设置，既便捷又为保障了系统有效运行。



3.2 注重用户体验

3.2.1 智能虚拟打印

【VA 虚拟应用管理平台】支持本地智能虚拟化打印，虚拟打印也是此种信息化模式最关键的技术指标，VA 本地打印拥有核心引擎技术，打印功能考虑多种用户环境，功能卓越。

使用通用打印（也称虚拟打印）不需要在服务器上安装任何打印驱动，通过简单的打印机选择，将服务器上打印内容传送到本地物理打印机进行输出，虚拟打印是打印技术发展的趋势。

虚拟打印支持打印后台进程转换优先级，打印进程可管理，提高打印速度；

虚拟打印支持本地各类型打印（本地直连式打印机、局域网打印机、打印至文件等）；

虚拟打印支持广泛的打印机型号；

虚拟打印支持 POS 打印，即打即停；

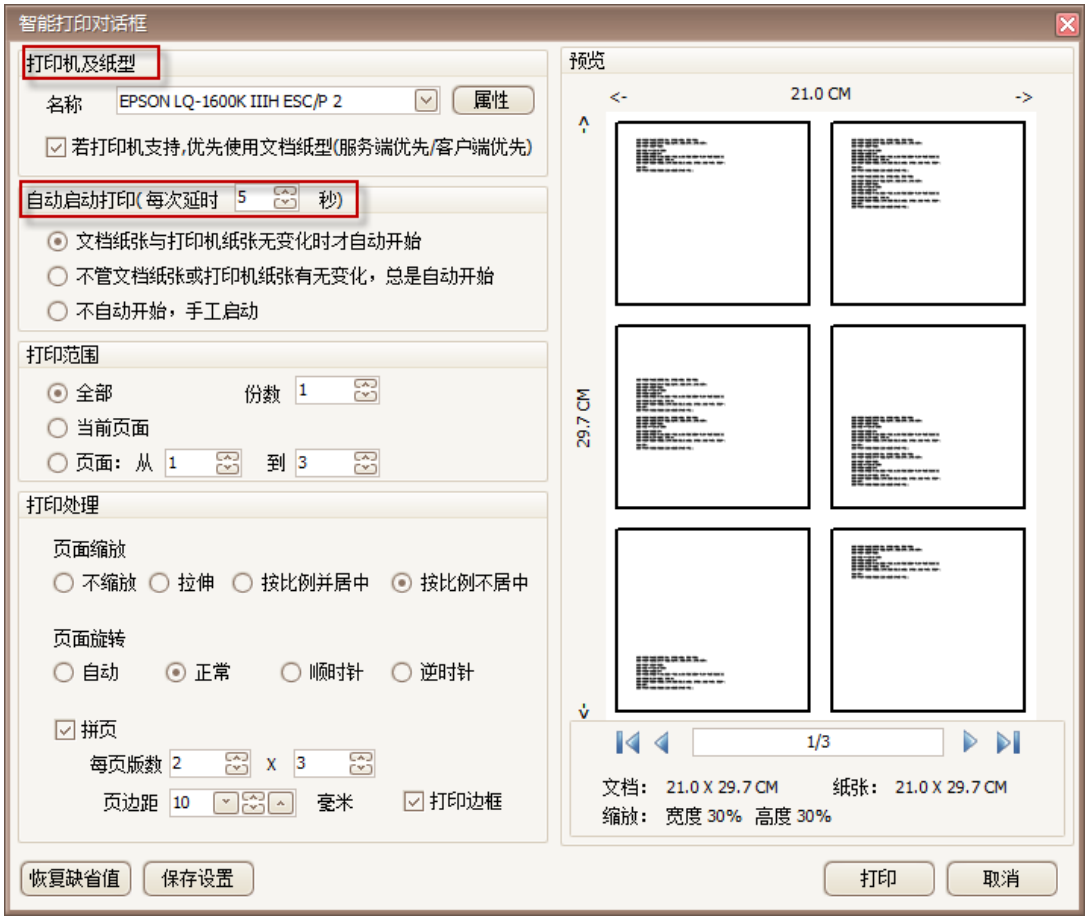
虚拟打印支持弹出式钱箱打印；

虚拟打印支持各种纸型打印，并且服务器一次定义后，自动传递纸型至客户端，客户端无需在定义纸型;

虚拟打印效率极高，打印速度快、打印准确；

虚拟打印支持本地的各种可管理性（打印页面旋转缩放、边距调整、打印范围、自动打印时间、拼页打印、动态预览等）。

虚拟打印几乎可以完美的将服务器上应用无差别的打印到客户端上。



3.2.2 本地输入法

【VA 虚拟应用管理平台】支持优异的本地输入法，根据输入法编码转换、简繁自动、环境识别等测试数百种环境，本地输入法让用户体验到录入如此简洁！

本地输入法直接用客户端本地个性化的输入法在远程应用里录入。

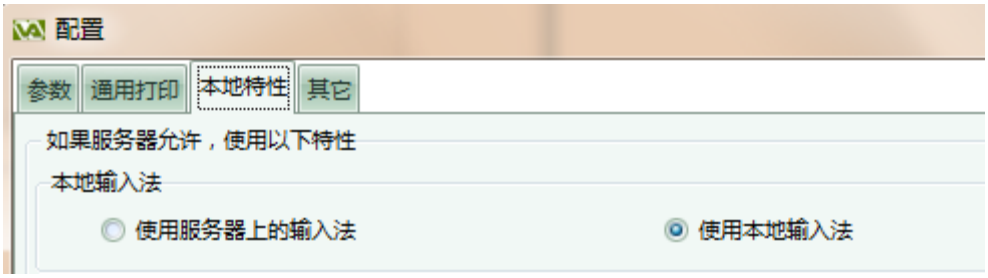
本地输入法功能强大，可以支持本地任何输入法；

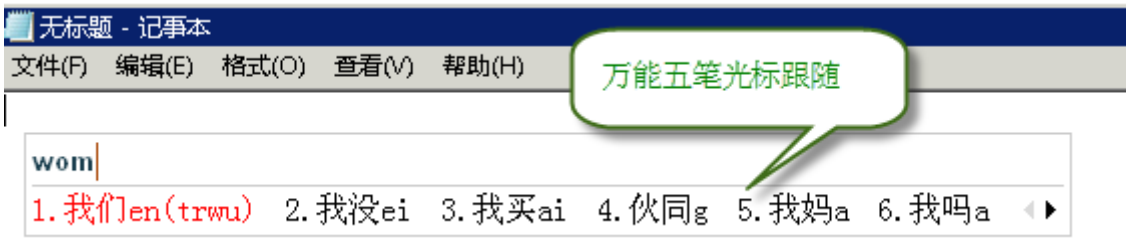
支持简繁英系统下的正确录入；

支持输入法光标跟随技术，录入方便；

支持本地输入法自动校验，录入无差错；

支持简繁体转换功能，即服务器上的应用是繁体版，客户端是简体版系统，在使用本地输入法录入时，可以直接将录入的简体字自动转换为繁体保存在服务器上。





3.2.3 无缝窗体技术

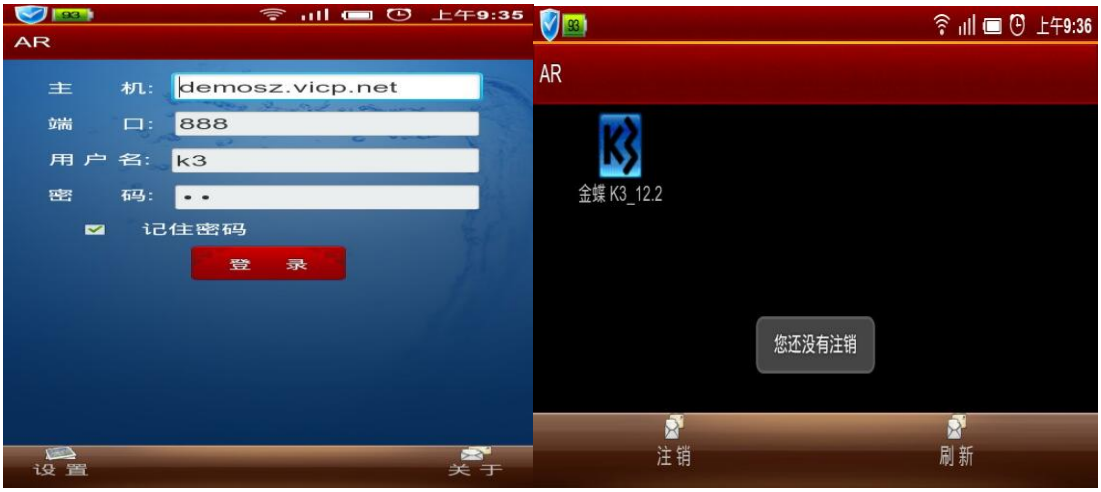
【VA 虚拟应用管理平台】具有完美的无缝窗体技术，无论是在矩形窗体还是在不规则的异型窗体均能获得极好的体验效果，使用远程应用完全如同本地应用无差别。同时在无缝窗体的基础上增加自定义模式和百分比显示模式，满足更多群体的需求。

3.2.4 扩展支持移动平台

随着移动终端设备（如安卓等）越来越普及，目前越来越多的企业将手持终端设备用于企业的信息化办公应用当中，VA 系统目前已经支持到大多数移动终端设备，在您的手机上就能浏览打开 PC 上的程序，使得移动办公成为真正的可能。

客户端支持：在安卓手机上直接安装 AR 客户端。

在安卓手机上的 VA 登陆界面：



3.3 VA 系统的安全设计

在应用服务器架构（A/S 架构）中，尤其是广域网远程应用时，安全是应用的前提，在集中式的应用模式下，网关接入安全及访问安全是极其重要的，VA 虚拟应用平台从网络边缘防护、传输过程加密、身份认证、访问控制等安全措施方面有着全面的防护设计，再加之 VA 系统平台配置的系统 AD 策略模板，可确保远程应用的网络安全及访问安全。

3.3.1 接入架构安全

由于 VA 系统是基于服务器计算架构（Application Serving 简称 A/S 架构）的应用接入平台，VA 自主设计的 VAP 协议能够动态实时对应用程序的输入输出逻辑和计算逻辑进行分离，在这种应用架构下，所

有的计算功能都是在服务器上完成的，服务器与客户机之间的网络中只传输键盘、鼠标移动变化指令和图像矢量信息，这些信息包即使被侦听和截获，也是一堆无用的信息，所以这种架构的安全性是非常高的。

3.3.2 数据传输安全

虽然在应用服务器架构下（A/S）下，客户机与服务器之间通讯不传输真实数据，只传输鼠标、键盘的点击动作及图像的矢量信息，但 VA 的 Secure VAP 协议仍然在建立客户端和服务器的专用隧道连接时对其数据包进行加密。

而且用户针对可以自由选择设置对传输过程进行 SSL（Secure Sockets Layer）和 TLS 强加密设置，加密强度可达到 128 位，最大限度的保障了传输过程的安全性。

SSL/TLS 是基于 PKI（Public Key Infrastructure）信息安全技术，是目前 Internet 上广泛采用的安全服务。可以提供通讯中的数据保密性、完整性保护；通过强制客户端证书认证的 TLS 服务，同时可以实现对客户端身份和服务器端身份的双向验证。

3.3.3 远程访问安全

用户访问身份认证

VA 系统除了自带用户名密码认证控制外，还提供用户名密码 + USBKey 身份认证接口，为用户提供高安全的访问保障。

3.3.4 VA 访问策略控制

1）应用接入防火墙

接入防火墙的主要功能是管理员用来管理用户权限。根据个人工作不同有时需要对某些用户禁止登录服务器，禁止使用某些应用程序，这些通过简单设置一下防火墙就能够使问题得到解决。（设置见附录 1）

2）访问安全策略

VA 系统可将每个会话连接做到细粒度访问控制，当客户端机器访问服务器时，可以通过设置与其绑定的应用程序可被访问的时间、安全等各种策略，对系统所发布的应用程序提供访问安全的保障，防止被恶意用户不正当的访问。此外，VA 系统还提供指定名称、指定 MAC 地址等预约式认证方式。

3）应用系统授权访问

VA 系统可针对发布的某一个应用系统或关键资源进行用户（组）权限授权，完全满足用户细致的访问权限管理。

3.3.5 服务器系统安全

VA 系统全面兼容 Windwos 系统的安全策略，它包括 3 项内容：用户策略、AD 策略、NTFS 设置（个别文件的设置、非系统盘的设置、系统盘的设置），这些安全策略可与 VA 系统紧密结合起来，用户可根据自身情况，限制用户的各种行为，如隐匿硬盘、限制打印、存储等操作行为，并可通过 VA 的安全策略，实现对接入客户端电脑的各种 USB、硬盘、串口、并口资源的使用限制，保障系统的安全、可靠、持续运行，将 Windows 操作系统 B2 级的安全管理完完全全的发挥出来。而且 VA 系统提供常见的安全策略模板，让用户快速实现系统安全策略配置。

3.3.6 VA 系统的安全措施

1）VA WEB 服务安全

由于使用标准浏览器（IE）就可以访问应用系统，因此 WEB 服务的安全性将至关重要，所以 VA 系统 WEB 服务没有选择通用的第三方 WEB 产品来作为 VA 的 WEB 服务，而是针对远程应用的 WEB 安全特点，进行了专项开发，并进行高强度的安全攻击测试，可完全摒弃用户因 WEB 服务器可能存在的安全隐患而造成对系统安全问题的担心。

2）VA 数据库服务安全

由于通用数据库的安全隐患也比较多，所以 VA 直接在系统中内置了数据库服务功能，并进行了高强度的加密处理，让用户无需担心数据库的安全，放心使用。

3）VA 安全事件管理

VA 系统可为用户提供所有用户及网络访问活动监控，可记录所有用户的全部访问与操作信息，可通过多种日志多角度去监控与管理整个应用安全状态，做到可记录、可追溯、动态报警的安全管理，从而帮助系统管理员及时发现及解决安全应用问题。

4 一般部署方案设计

4.1 方案软件结构构成

VA 云计算方案主要的软件结构组件如下表：

逻辑划分	组件名称	功能
客户端	AR	VAP 客户端
基础架构组件	应用接入防火墙	安全接入网关，实现应用和登录的访问控制功能
	Web Interface	用户访问接入站点，进行应用呈现
	虚通道	提供会话接入管理功能
	授权	用户登录授权
	数据库	存放系统和应用数据
	输入法监控	中文（简繁体）语言输入监控
	打印监控	本地打印监控，完成监控和打印数据的服务器到客户端的传输
	性能监控	监控系统性能和用户访问体验
应用发布服务器	ARS	VA 发布应用的登录
	RDP	VA 免终端或微软 RDP 协议

一套完整的 VA 部署方案可以在一个服务器上包含所有这些组件，也可以将它们部署在一个 VA 集群服务器内分别部署。

4.2 用户配置

建议配置 1：100-500 用户

- 硬件配置方案

✓ 物理服务器

（假如一台 4vCPU 8GB 内存的虚拟服务器支持 70 用户。）

服务器用途	配置	数量
基础架构服务器	2 路 4 核 CPU，4GB 内存，3*500GB 硬盘	1 台
应用发布服务器	2 路 8 核 CPU，48GB 内存，3*500GB 硬盘	1-3 台

✓ 基础架构服务器组件配置

组件名称	vCPU	内存	硬盘	所在物理服务器
基础构架组件	2	4G	30G	主服务器 1
应用发布组件	2	4G	30G	主服务器 1
应用发布组件	4	8G	30GB	ARS 服务器 1
应用发布组件	4	8G	30GB	ARS 服务器 2
应用发布组件	4	8G	30GB	ARS 服务器 3

(注：主服务器同时应用接入服务器的部分功能)

✓ 每台应用发布服务器的虚拟服务器划分（一台物理 ARS 服务器划分为 4 个虚拟 ARS 服务器）

虚机名称	vCPU	内存	硬盘
ARS01	4	8G	30GB
ARS02	4	8G	30GB
ARS03	4	8G	30GB
ARS04	4	8G	30GB

■ 软件配置方案

软件名称	数量	说明
VA 许可协议	=用户数	按照并发用户购买，选择企业版
VA 应用服务器许可	若干套	按照 ARS 服务器数量选择
Microsoft Windows Server	若干套	根据需要安装的 Windows 服务器数量购买
Microsoft RDS 许可协议	=用户数	根据 windows 版本购买（可选择）

建议配置 2：500 用户以上

- ■ 硬件配置方案

✓ 物理服务器

（假如一台 4vCPU 8GB 内存的虚拟服务器支持 70 用户。）

服务器用途	配置	数量
基础架构服务器	2 路 4 核 CPU，4GB 内存，3*500GB 硬盘	1 台
应用发布服务器	2 路 8 核 CPU，48GB 内存，3*500GB 硬盘	3 台以上，每台支持 200 以上用户

✓ 基础架构服务器组件配置

组件名称	vCPU	内存	硬盘	所在物理服务器
基础构架组件	2	4G	30G	主服务器 1
应用发布组件	2	4G	30G	主服务器 1

应用发布组件	4	8G	30GB	ARS 服务器 1
应用发布组件	4	8G	30GB	ARS 服务器 2
应用发布组件	4	8G	30GB	ARS 服务器 3

(注：主服务器同时应用接入服务器的部分功能)

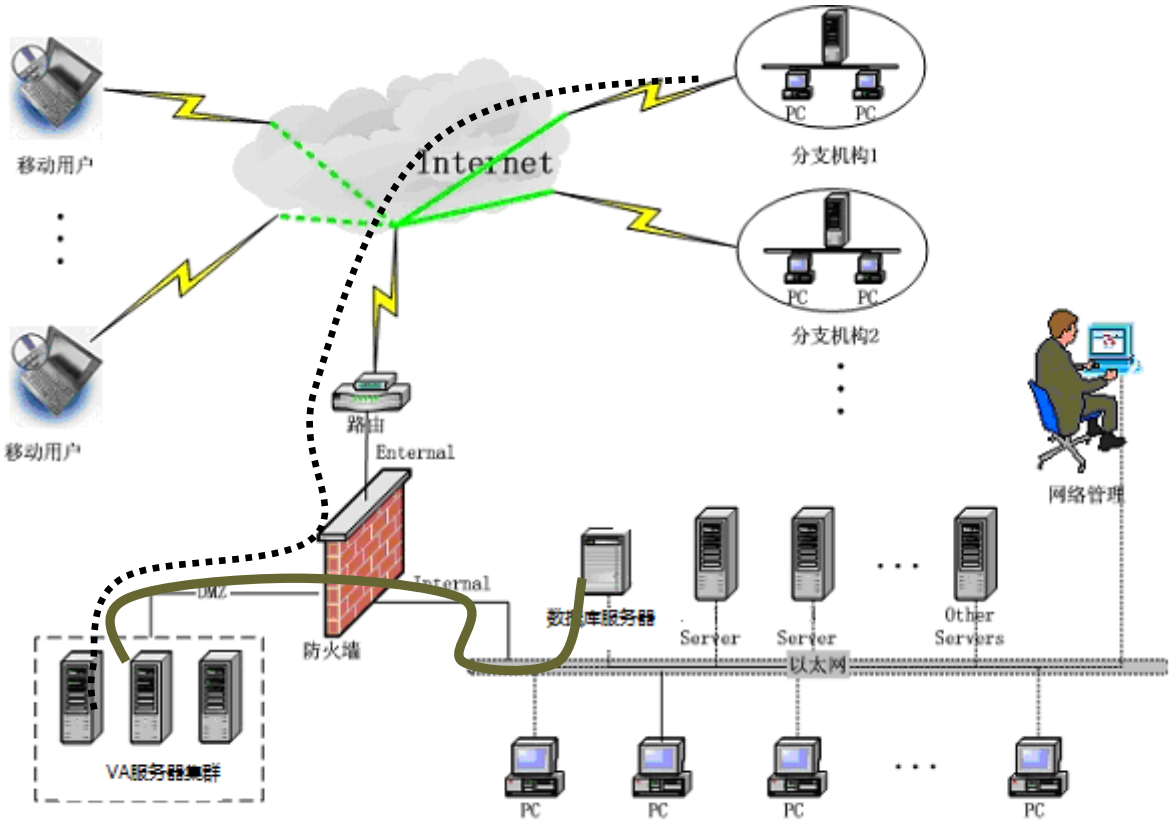
- ✓ 每台应用发布服务器的虚拟服务器划分（一台物理 ARS 服务器划分为 4 个虚拟 ARS 服务器）

虚机名称	vCPU	内存	硬盘
ARS01	4	8G	30GB
ARS02	4	8G	30GB
ARS03	4	8G	30GB
ARS04	4	8G	30GB

- ■ 软件配置方案

软件名称	数量	说明
VA 许可协议	=用户数	按照并发用户购买，选择企业版
VA 应用服务器许可	若干套	按照 ARS 服务器数量选择
Microsoft Windows Server	若干套	根据需要安装的 Windows 服务器数量购买
Microsoft RDS 许可协议	=用户数	根据 windows 版本购买（可选择）

4.3 网络拓朴图



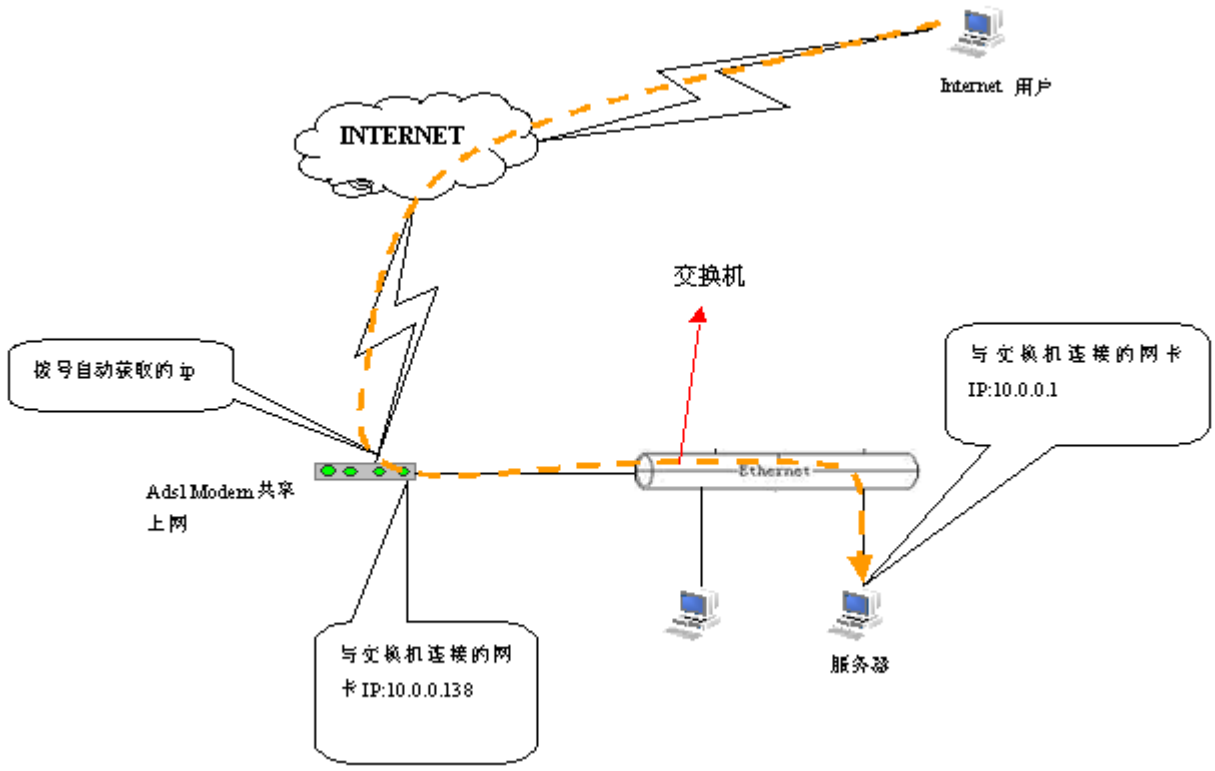
移动用户透过各种网络连接方式连接到 VA 服务器上发布的浏览器上进行访问

服务器集群上发布应用.

4.4 网关设置

安装及使用 VA 系统后局域网内没有路由及防火墙的限制可以自由使用，广域网的使用因为与内网隔离需要在公司网关（如：Adsl modem 、防火墙、路由器等）上设置端口映射将外网访问的端口映射到局域网内的服务器上才可以使用。

假设某公司网络结构如下（阿尔卡特 ADSL，更多网关路由的设置见附录 2）：



如上图所示，外网的 INTERNET 上的 VA 用户如果要登陆服务器就需要经过各个软硬件的限制，这样就需要通过设置端口映射来解决这个问题。

5 方案应用效果

5.1 应用系统大集中

集中运行和管理，已是信息化发展的必然趋势，无论从节省财力资源、人力资源的角度，还是从信息系统为企业业务服务、提高竞争力、加强风险控制手段的角度来说，集中化的信息系统模式都能提供更大的优势，VA 就是实现集中管理和远程访问的一个非常有效和快捷的平台。

在实施和应用的过程中，借助 VA 远程应用接入方案，明确各使用者的权限，系统管理员或决策者有权单点控制整个系统的进程、资源、状态等，并且通过有效的控制工具部署和督促各个环节的正常工作。

5.2 系统安全

VA 平台，将 Windows 应用服务器与互联网完全隔离，消除了这些 Windows 应用服务器的安全隐患；在网络上传输的只是客户端的键盘、鼠标动作以及显示界面的变化部分，业务数据被保护在企业总部的信息中心，避免了业务数据泄密的危险；同时，客户端的操作感觉虽然就像在本机操作，但是未经权限许可，不得擅自修改、备份、拷盘、打印等。通过应用发布的方式，员工只能使用公司规定的应用程序，如 GUI 客户端程序等，而不能打开其他的应用软件或数据信息。

5.3 系统工作稳定

应用系统由专人统一维护，稳定性好，安全性高。通过大型企业使用 VA 方案的经验，VA 远程接入方案支持 7x24 不间断的工作模式，完全满足企业对关键应用系统的要求。

5.4 降低客户端的维护量

由于下面的员工或是合作伙伴、供应商等，并没有实质性接触到软件的升级、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。

5.5 大大缩短项目实施周期

由于应用系统只需安装在服务器上，因此一系列的安装、配置、调试工作得到简化，原来需要一两个月、跑来跑去、重复进行的工作，现在只需一两个星期、甚至几天的时间就能完成。

5.6 节约网络带宽

通过 VA 应用管理平台，在网络上只传输鼠标、键盘和压缩的运行结果的屏幕信息，带宽的使用降为最低，将局域网上的应用直接延伸到了广域网，VA 系统平台即使在低带宽下也能达到满意的性能。用户通过普通的互联网接入，就能很好的实现软件系统的远程应用，节约了大量的专线成本，提高了系统处理效率。

5.7 性能保障

由于 VA 系统自动支持的对后台应用服务器的动态负载均衡能力，可以使应用系统达到最佳性能，同时保证系统维护、升级等可以在不影响生产的前提下分阶段实施，最大程度地保障了系统的性能

5.8 保护对客户端的投资

VA 系统对客户端只要求能够使用 WEB 浏览器即可，对机器的性能没有要求。从 windows

全系列都可以通过 AR 访问企业资源。充分保护了用户对现有 IT 资源的投资。而且，对于客户端，无需根据应用系统的不同，经常升级。

5.9 适应更广泛的企业远程访问需求

VA 系统平台支持 ADSL 等没有固定 IP 地址的接入方式，企业既可在其发展的不同阶段均可以享受安全的远程访问带来的好处。企业用户直接通过互联网使用任何设备访问应用系统，而不需重新编写程序代码，同时保持原有的用户感受，既承袭了 C/S 结构的软件资源和用户经验，又进一步发挥了 B/S 结构的集中控管优势。

6 附 录

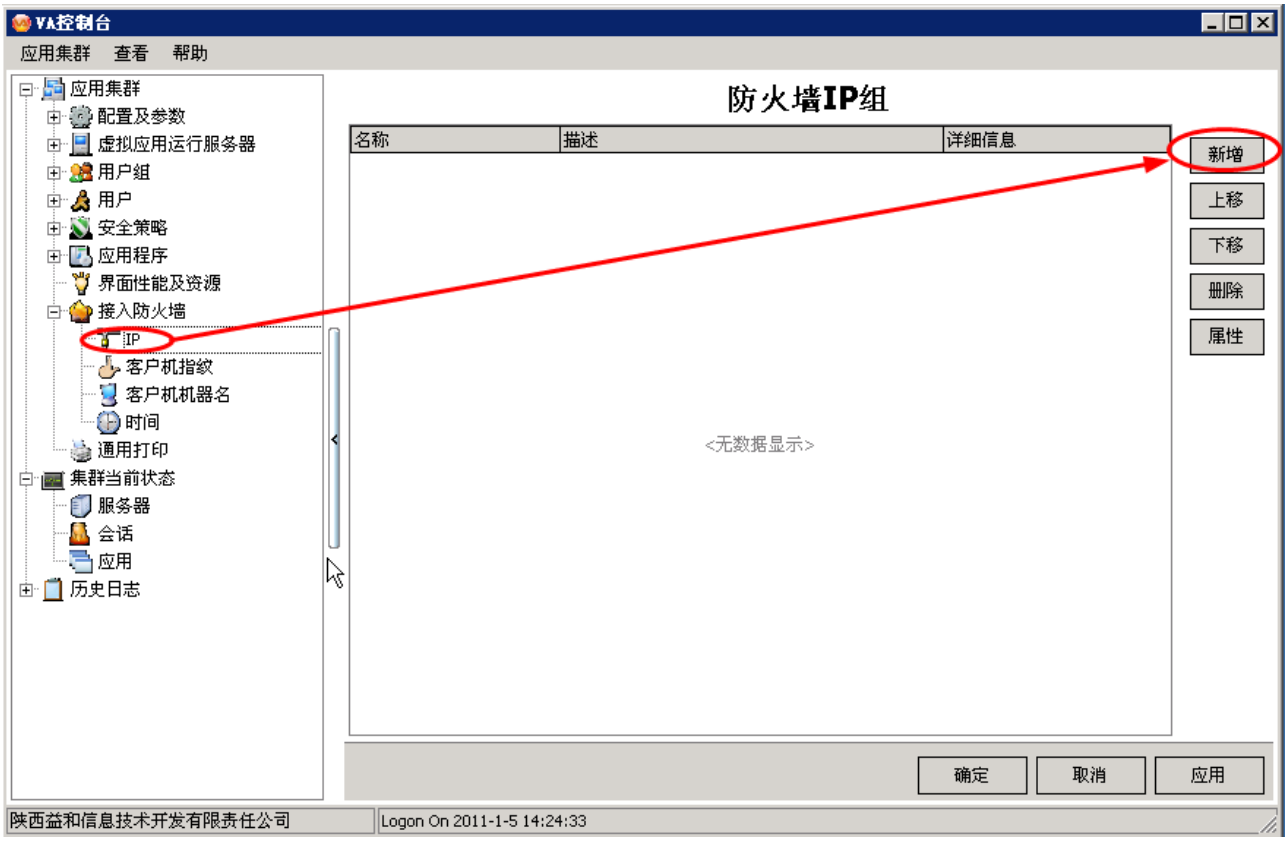
6.1 接入防火墙设置说明

接入防火墙的主要功能是管理员用来管理用户权限。根据个人工作不同有时需要对某些用户禁止登录服务器，禁止使用某些应用程序，这些通过简单设置一下防火墙就能够使问题得到解决。

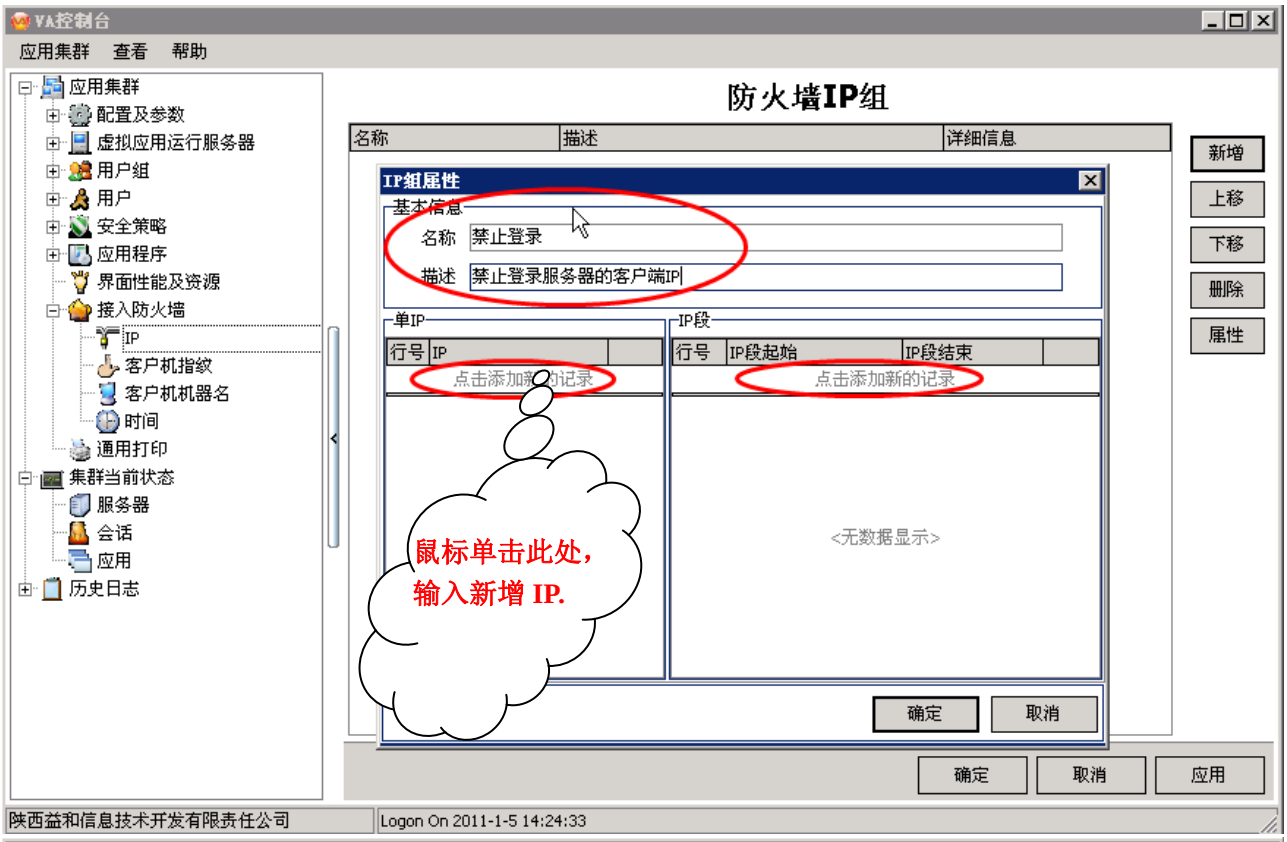
举例介绍 IP 地址：

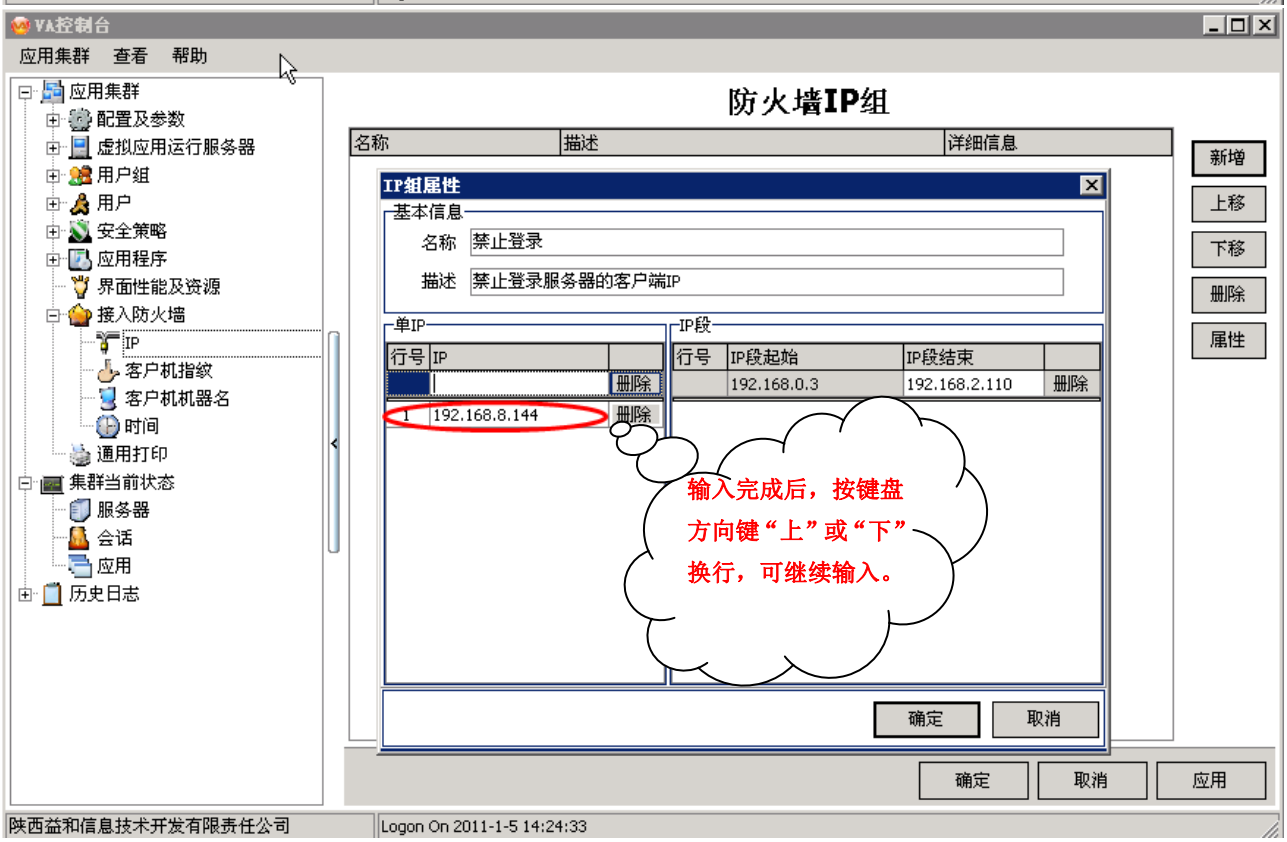
首先举例介绍一下接入防火墙“IP 地址”的设置方法，比如单个 IP：192.168.8.144；192.168.8.131 和 IP 段：192.168.0.3~~192.168.2.110 设置为禁止登录服务器。

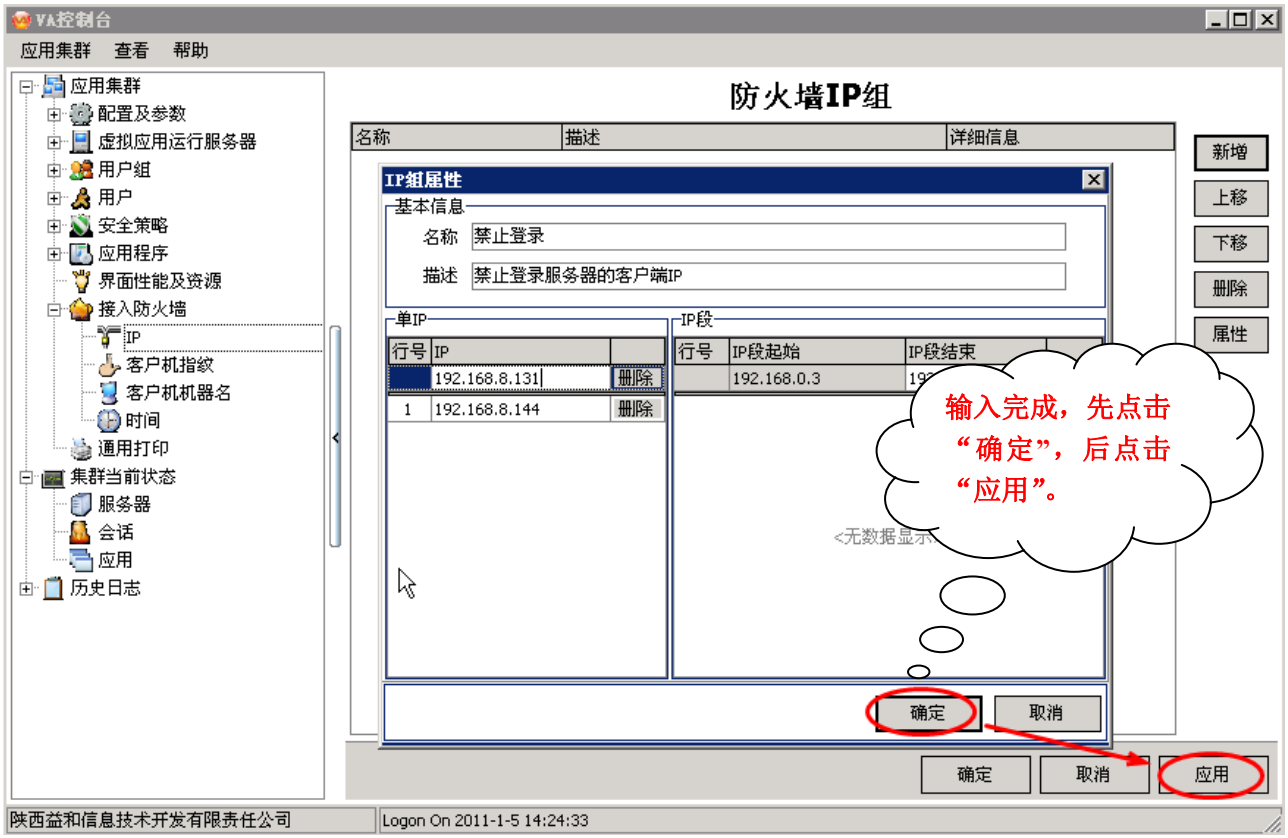
1. 打开接入防火墙，选择 IP，点击新增。



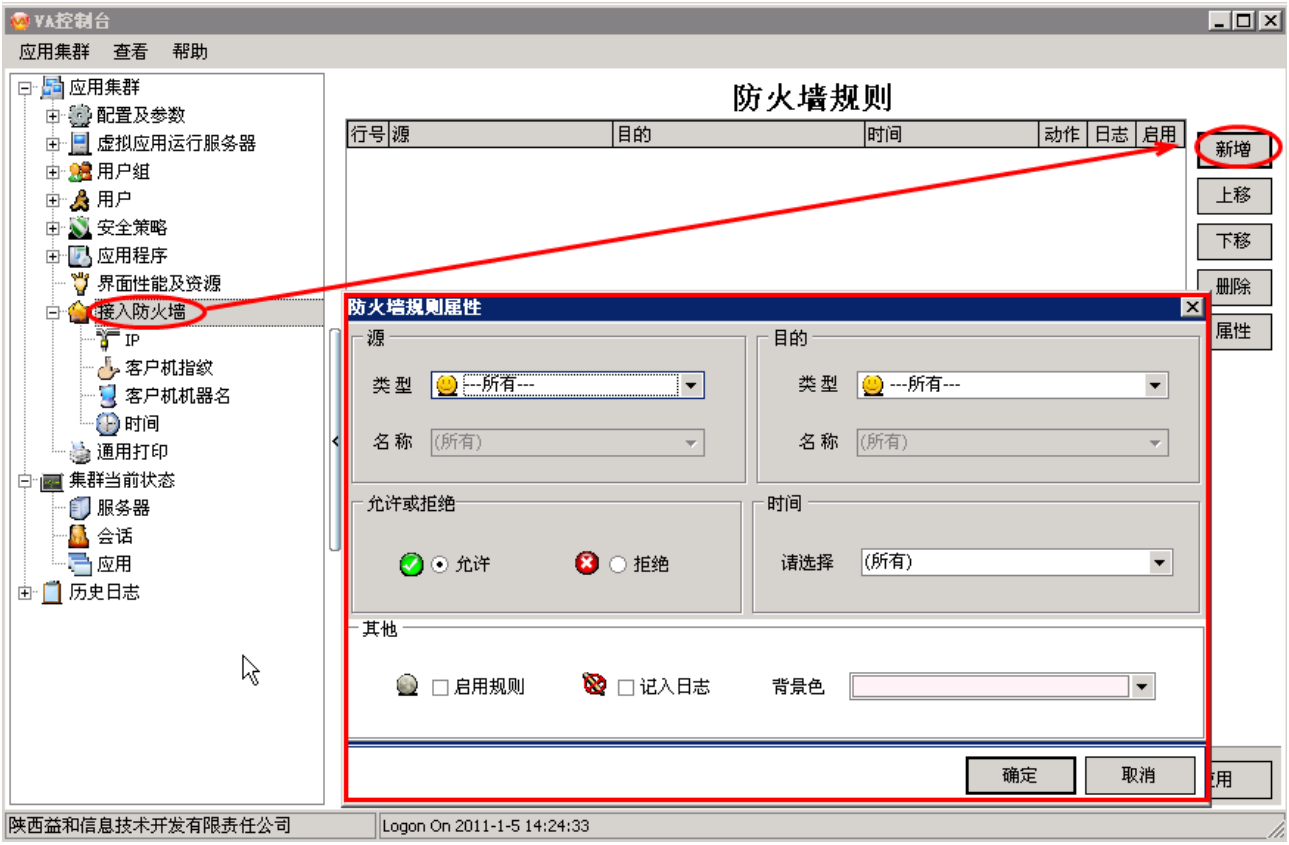
2. 名称，描述可自行填写，在这里设为名称：禁止登录，描述：禁止登录服务器的客户端 IP.输入新增 IP 及 IP 段。


VA控制台
应用集群 查看 帮助
应用集群
配置及参数
虚拟应用运行服务器
用户组
用户
安全策略
应用程序
界面性能及资源
接入防火墙
IP
客户机指纹
客户机机器名
时间
通用打印
集群当前状态
服务器
会话
应用
历史日志
防火墙IP组
名称
描述
详细信息
新增
上移
下移
删除
属性
IP组属性
基本信息
名称 禁止登录
描述 禁止登录服务器的客户端IP
单IP
行号 IP
点击添加新的记录
IP段
行号 IP段起始 IP段结束
点击添加新的记录
<无数据显示>
鼠标单击此处，
输入新增 IP.
确定
取消
确定
取消
应用
陕西益和信息技术开发有限责任公司
Logon On 2011-1-5 14:24:33


VA控制台
应用集群 查看 帮助
应用集群
配置及参数
虚拟应用运行服务器
用户组
用户
安全策略
应用程序
界面性能及资源
接入防火墙
IP
客户机指纹
客户机机器名
时间
通用打印
集群当前状态
服务器
会话
应用
历史日志
防火墙IP组
名称
描述
详细信息
新增
上移
下移
删除
属性
IP组属性
基本信息
名称 禁止登录
描述 禁止登录服务器的客户端IP
单IP
行号 IP
1 192.168.8.144
删除
IP段
行号 IP段起始 IP段结束
192.168.0.3 192.168.2.110 删除
输入完成后，按键盘
方向键“上”或“下”
换行，可继续输入。
确定
取消
确定
取消
应用
陕西益和信息技术开发有限责任公司
Logon On 2011-1-5 14:24:33

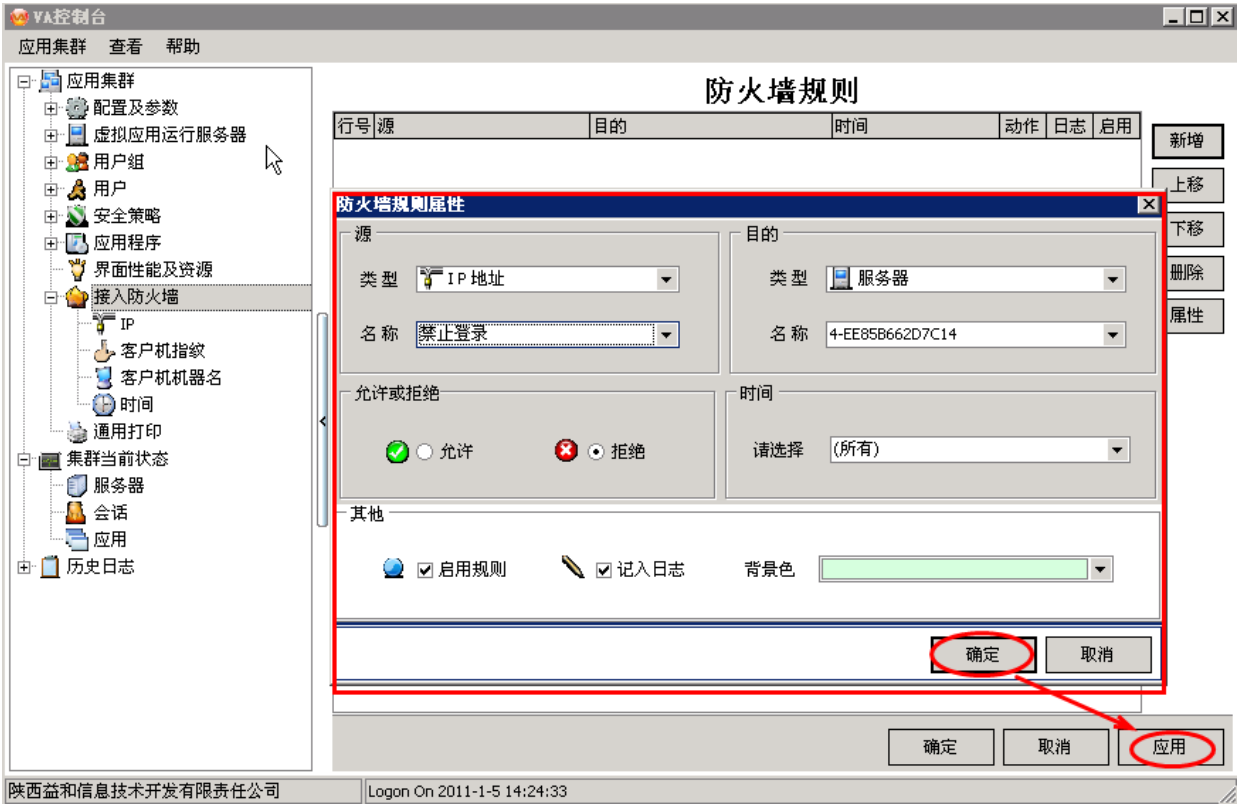


3. 防火墙规则设置，选择接入防火墙，点击新增，出现防火墙规则属性框。



4. 源类型选择:IP 地址，名称：禁止登录。勾选启用规则、记入日志。

5. 点“确定”，“应用”之后，防火墙规则生效。



这样设置后，所达到的效果就是，客户端 IP 为：192.168.8.144；192.168.8.131 和 IP 段

192.168.0.3~~192.168.2.110 之间的用户，将无权登录服务器。

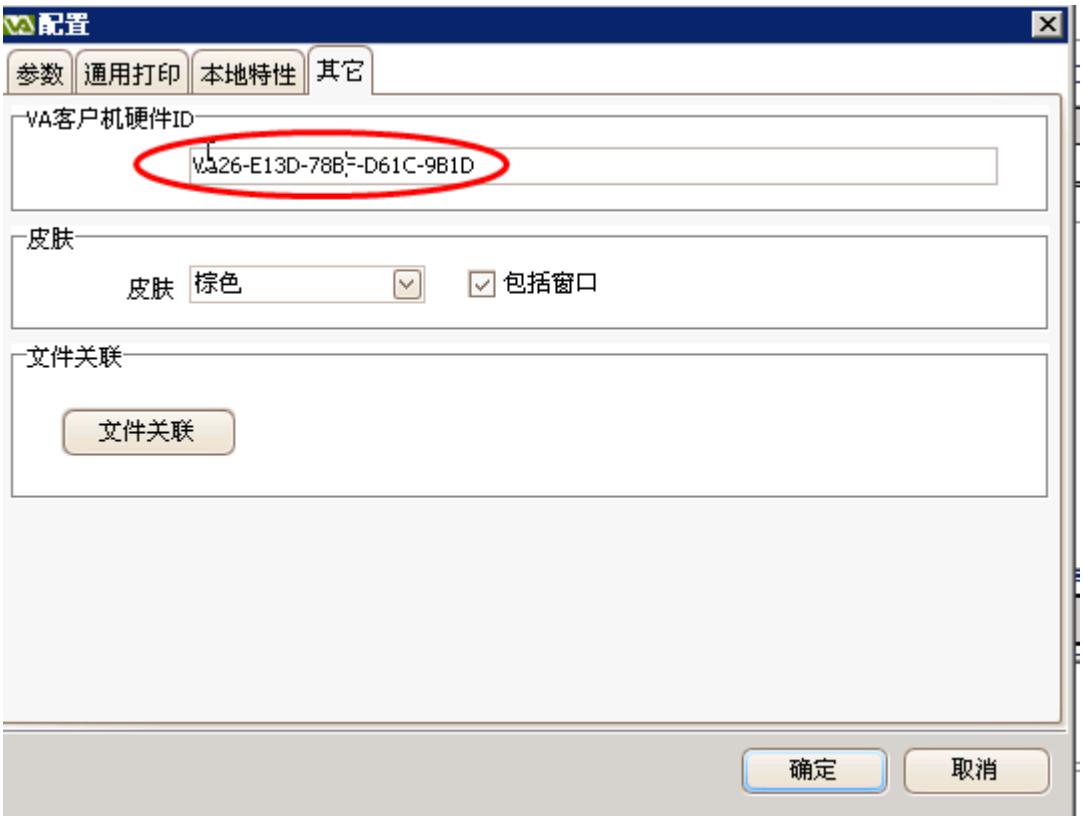
举例介绍客户机指纹：

客户机指纹，就是指客户机的硬件 ID,就像人的指纹一样，虽然人人都有，却各不相同，客户机硬件 ID 也是唯一的。

一、如何查看客户机指纹？

客户端登录，与 VA 服务器连通后，在“工具”菜单中选择下拉菜单“配置”

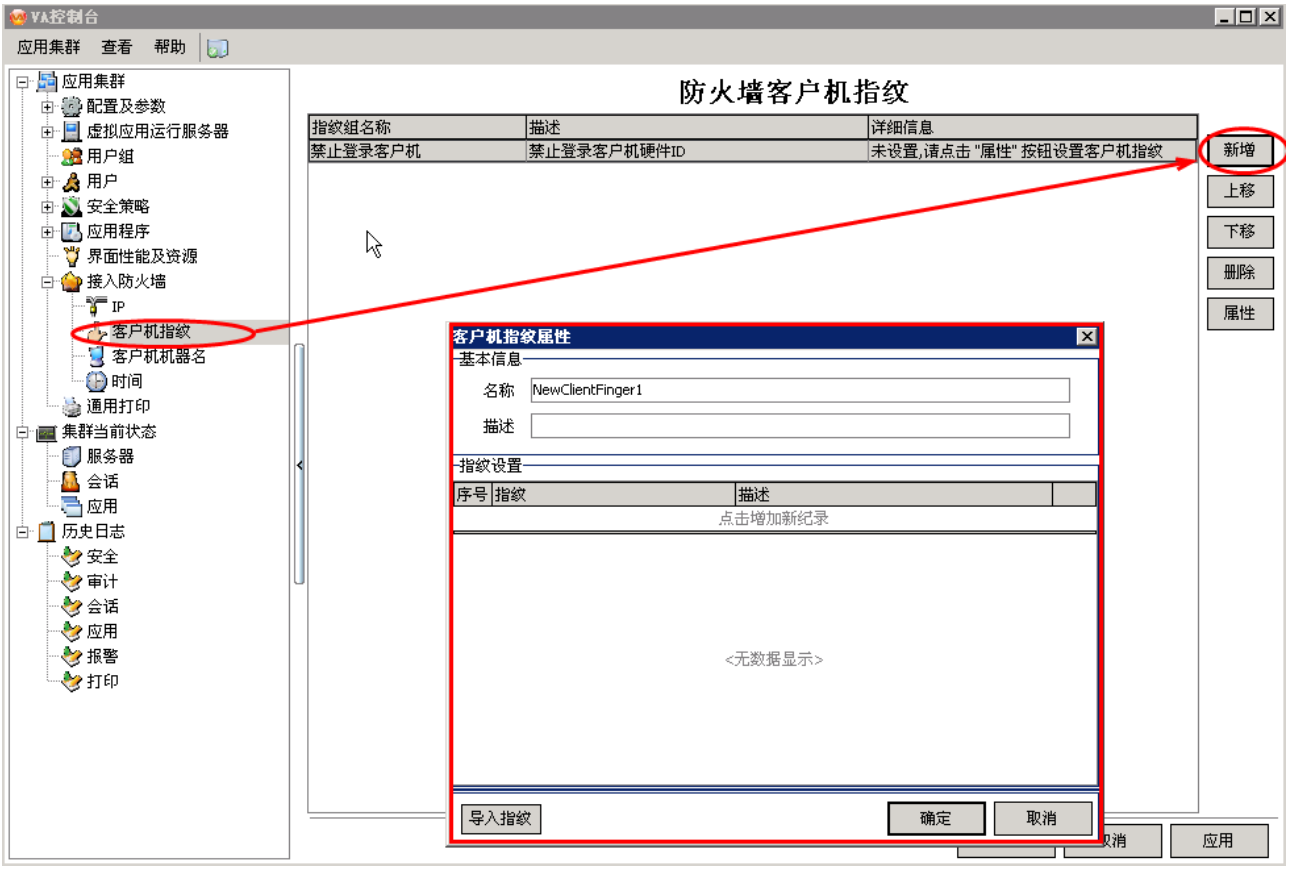
在“其它”目录下，有 VA 客户机硬件 ID，就是客户机指纹。



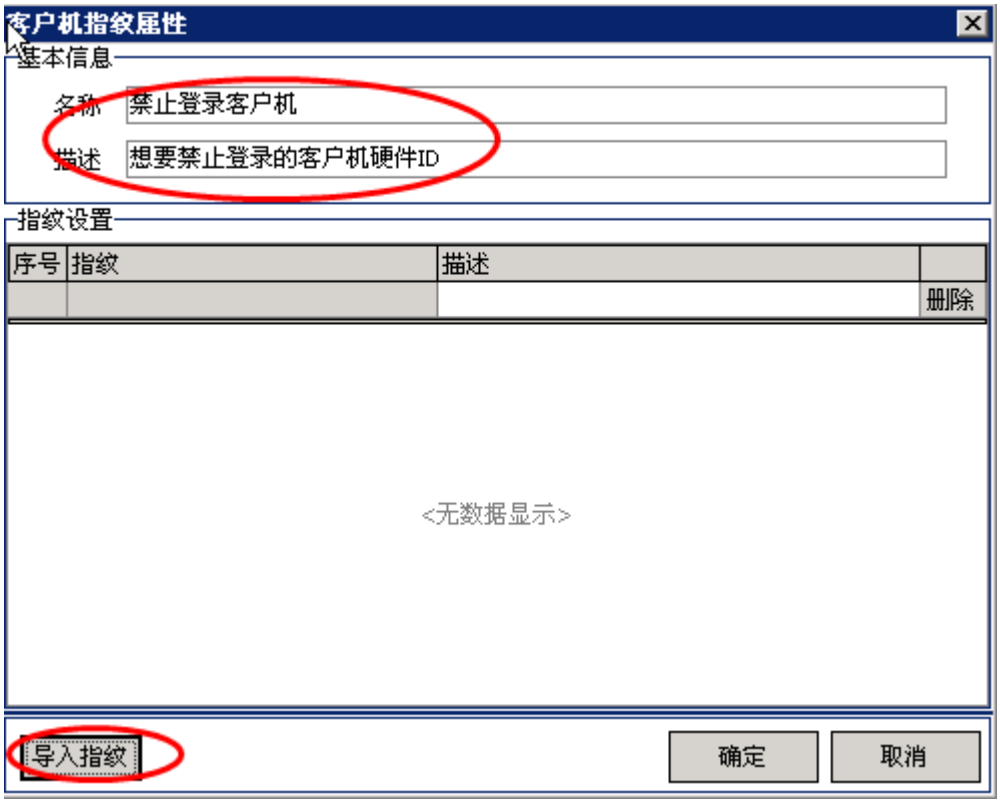
二．客户机指纹锁设置

由于客户机指纹唯一性，所以通过客户机指纹设置用户的使用权限，也比较方便。

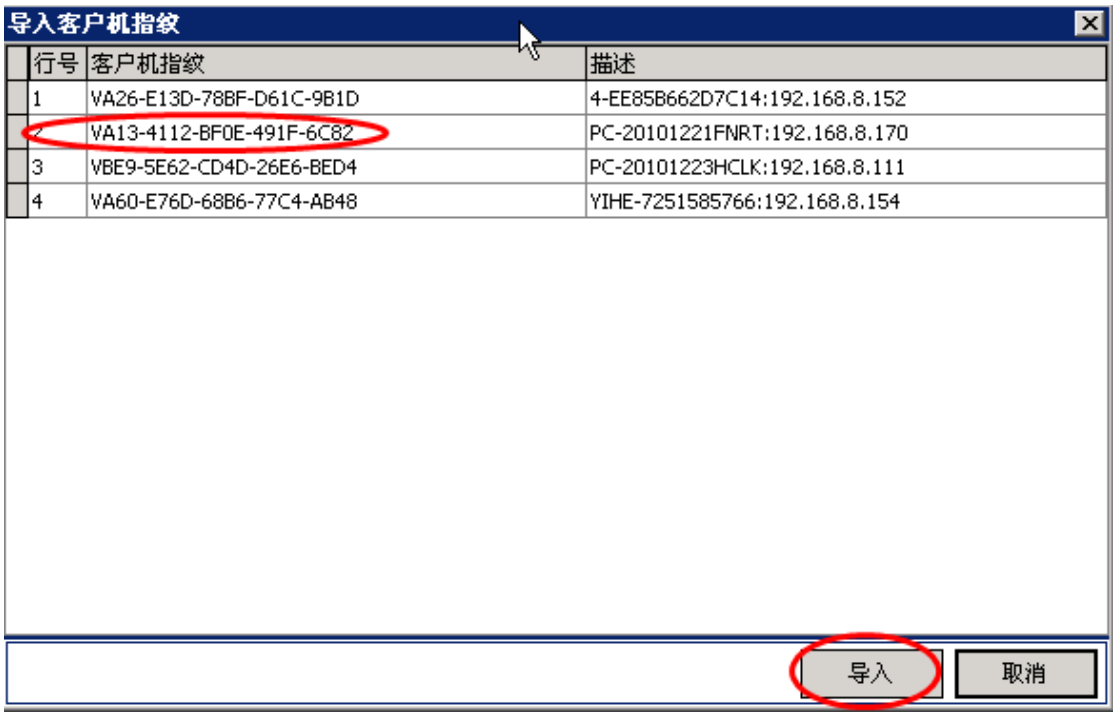
1. 选择“客户机指纹”，点击“新增”，出现客户机指纹属性对话框。



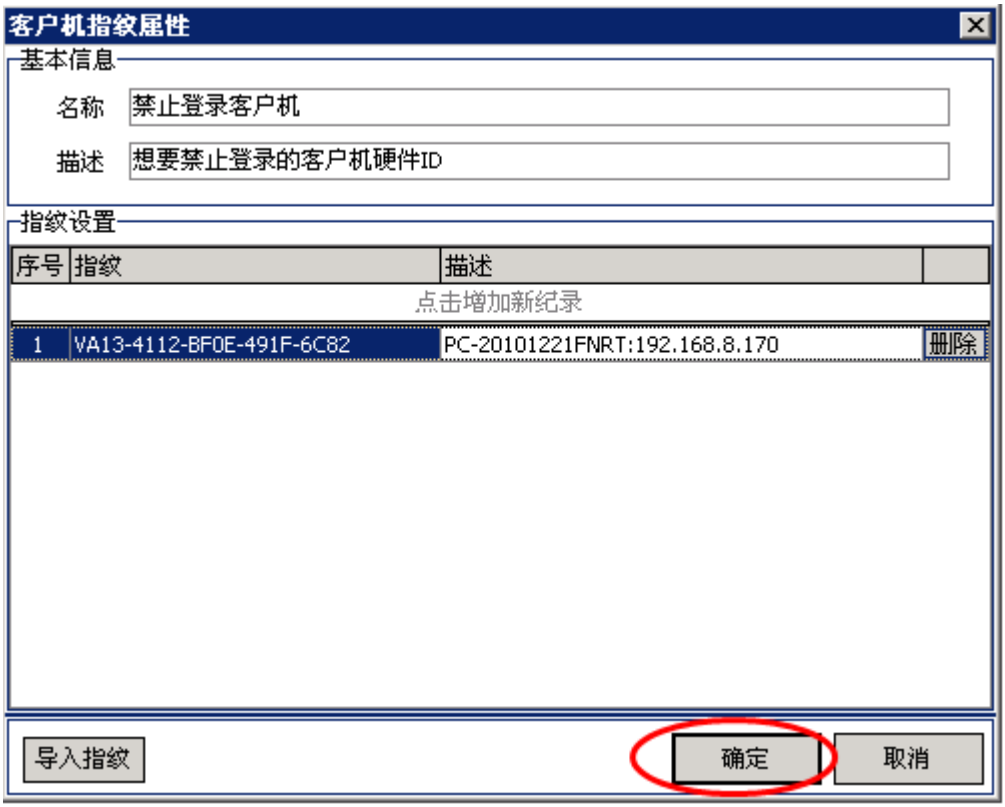
2. 在客户机指纹属性对话框中，名称，描述自行填写，在这写为，名称：禁止登录客户机，描述：想要禁止登录的客户机硬件 ID.（描述可以省略），点击“导入指纹”出现“导入客户机指纹”对话框。



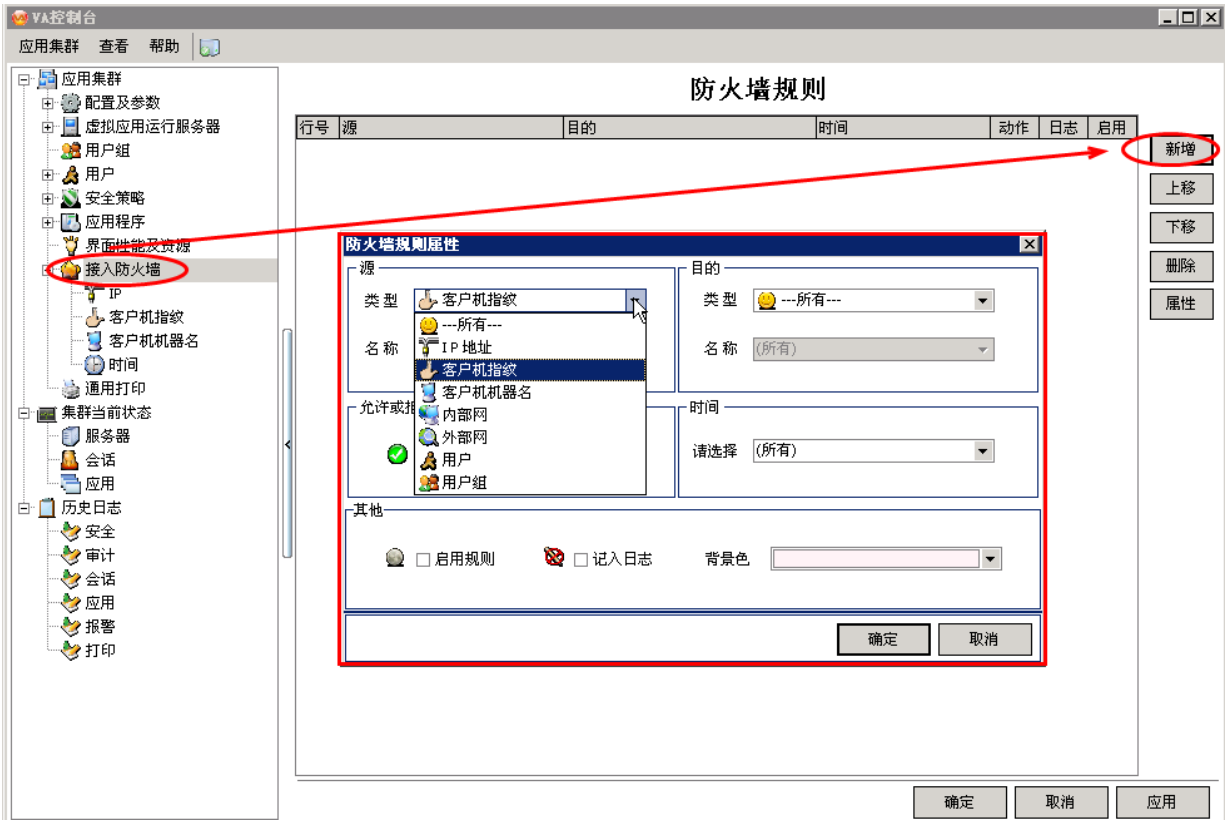
3. 在“导入客户机指纹”对话框选择所要禁止登录的客户机指纹。



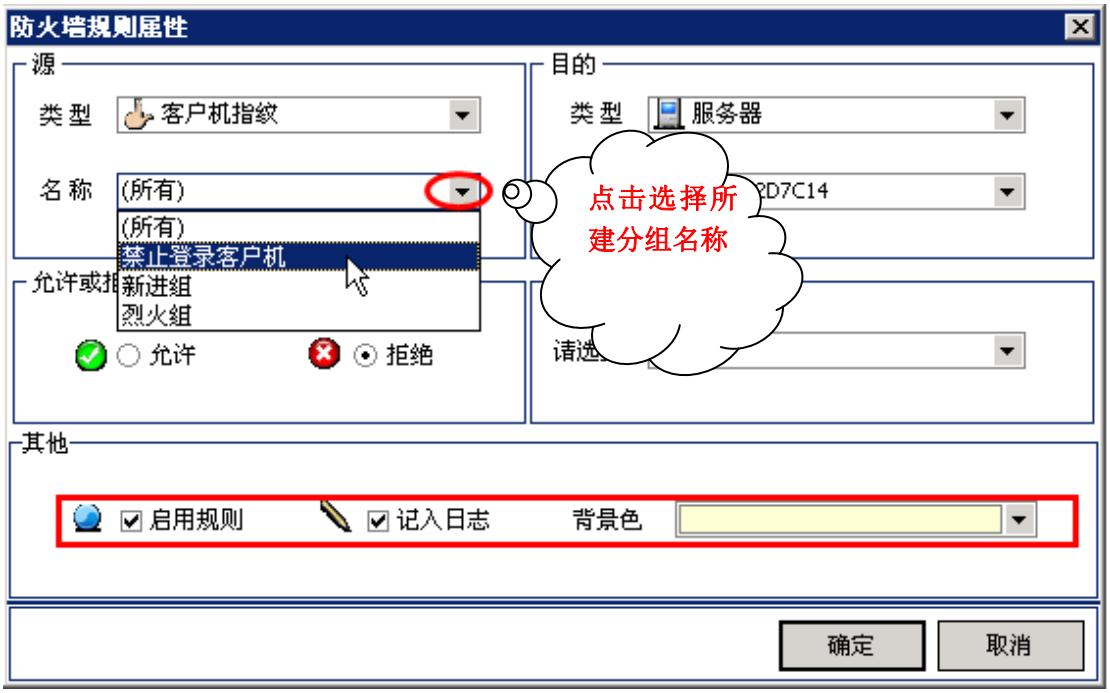
4. 导入成功，确定即可。



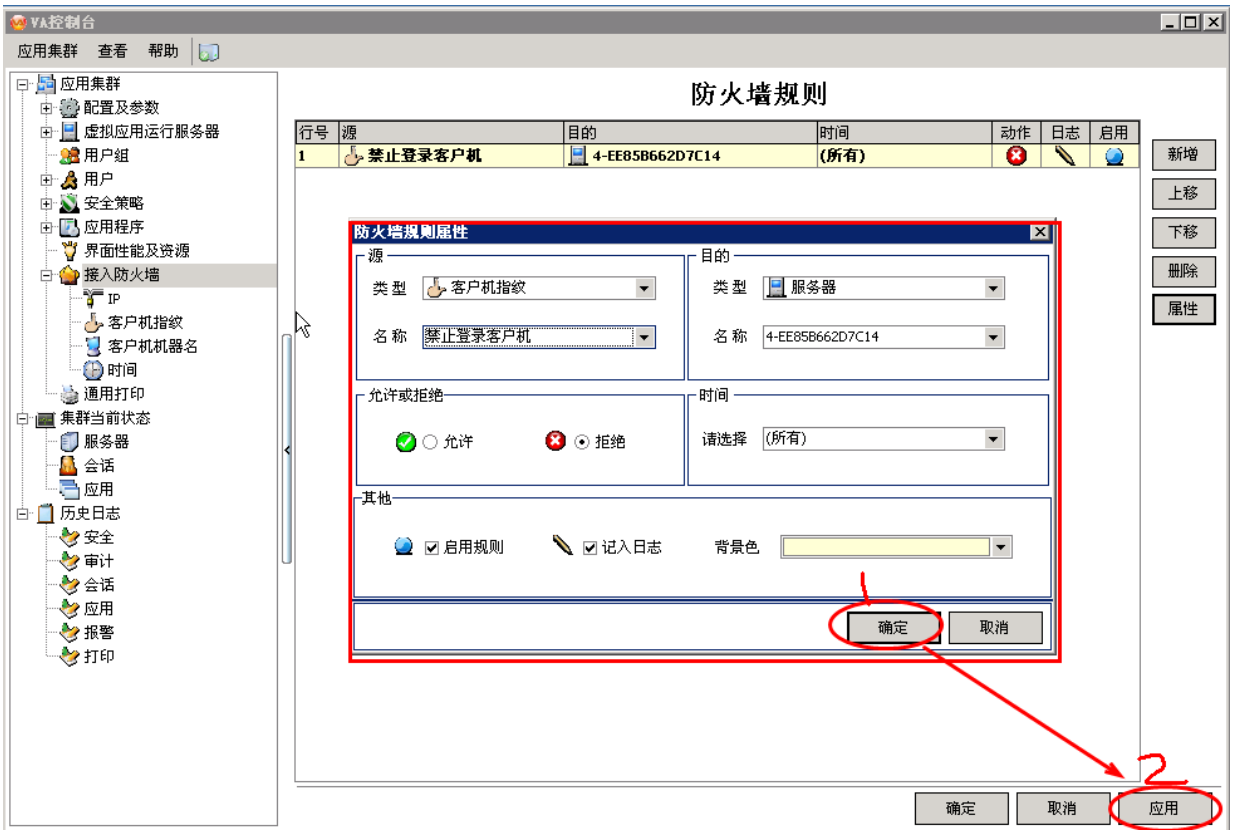
5. 防火墙规则设置，选择接入防火墙，点击新增，出现防火墙规则属性框。



6.防火墙规则属性对话框。勾选启用规则，记入日志可选，背景色自选。



7.先点击“确定”，后点击“应用”设置完成。防火墙规则生效后，禁止登录的客户机，客户端将无法再登录服务器。



在防火墙子项中，我们还可以用同样的方法，分别从客户机机器名、客户机使用时间上，根据需要，设置服务器，限制用户的使用权限。

防火墙规则介绍：

在防火墙规则中，我们除了防火墙子项可以设置以外，还可以从防火墙源类型中选择，内部网、外部网，用户及用户组进行设置服务器的使用权限。如果想要某用户，在某一特定时间内，禁止使用服务器上的已发布程序，可以通过设置源类型选择该用户，在防火墙子项中设置禁止使用的时间，再通过目的类型，设置所要禁止的已发布程序。

（注） 在防火墙不同的规则之间具有自上而下的优先级排列，比如，第 2 行如果与下面第 8 行规则冲突了，由于优先级的存在，第 8 行规则将失效，只执行优先级较高的第 1 行规则。

6.2 常见电信网关设置

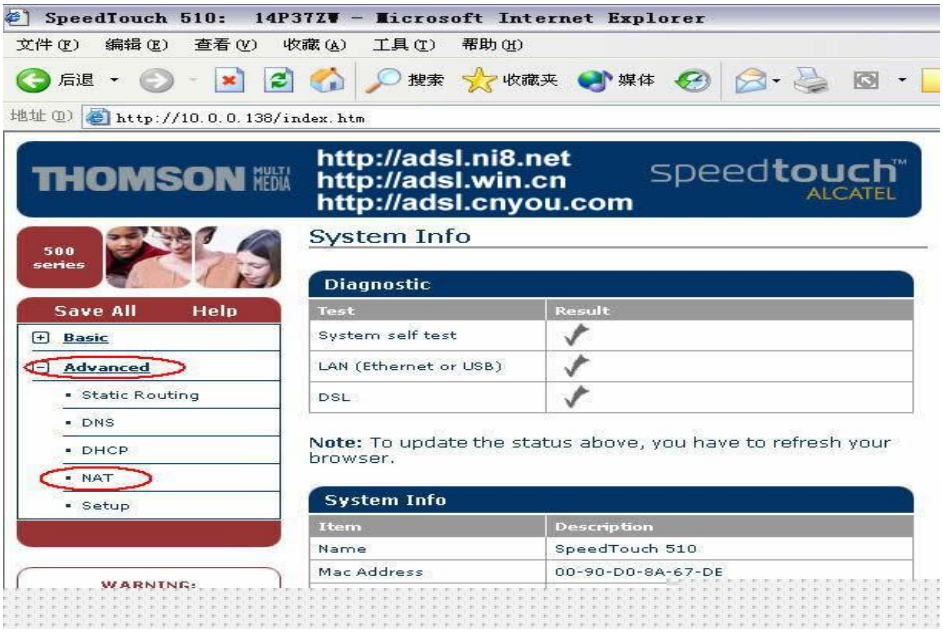
电信安装宽带时并不考虑客户作网站的需要，因此仅仅设置了共享上网，其他设置需要客户

自行设置。Adsl modem（宽带猫）的型号和品牌比较多，我们这里选择一两款常见的 Adsl modem 演示设置：

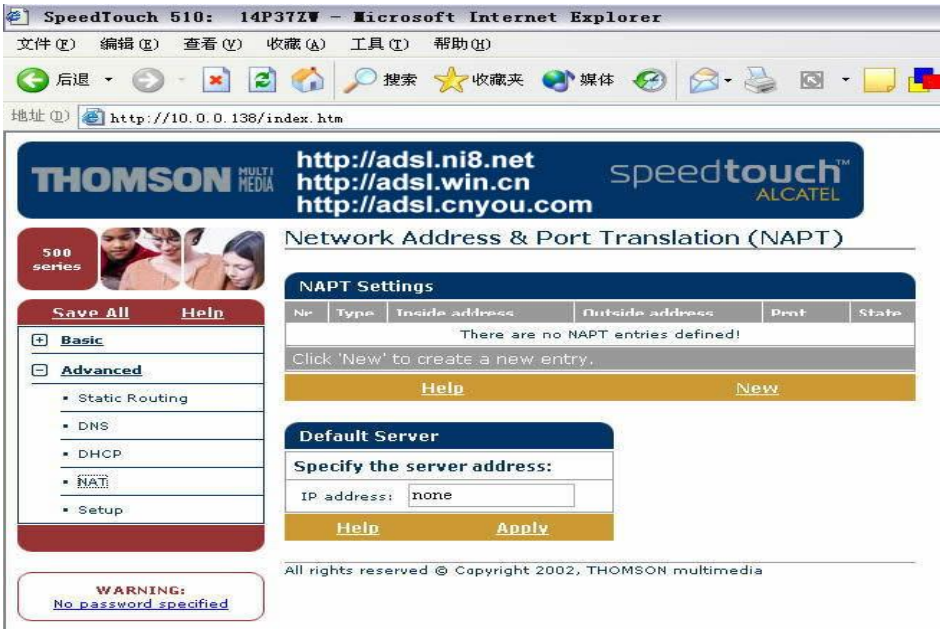
（以下的设置内容需要先将 ADSL 直接连接到某台电脑上，并将网卡设置成自动获取 IP。）

阿尔卡特 SpeedTouch Home Plus 511 ADSL 端口映射方法：

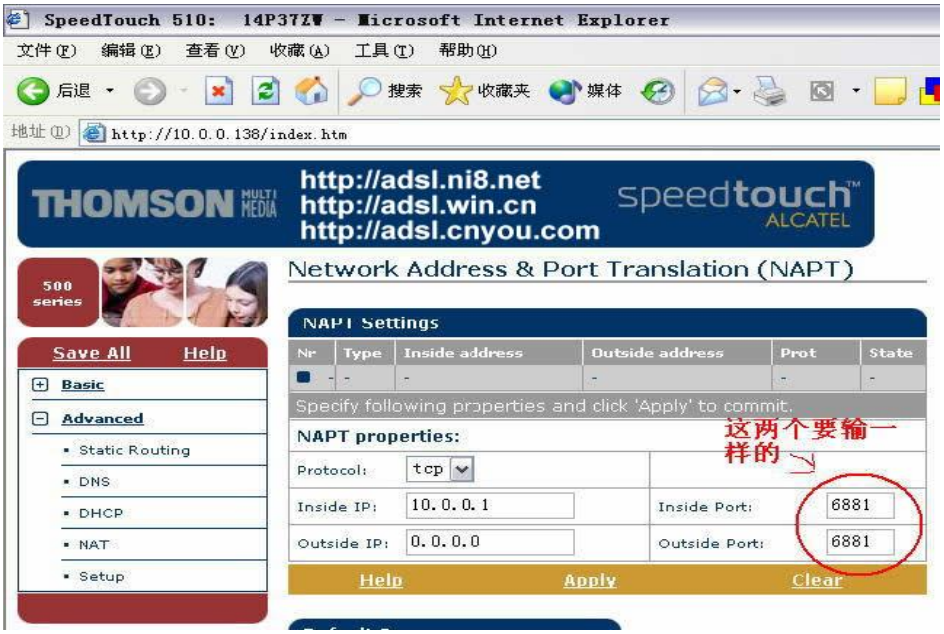
1、在地址栏输入 10.0.0.138 进入 ADSL 的 Web 设置页面，点左边的 Advanced - NAT



2、进入 NAT 的设置界面后，点右边的 New 创建新的端口映射

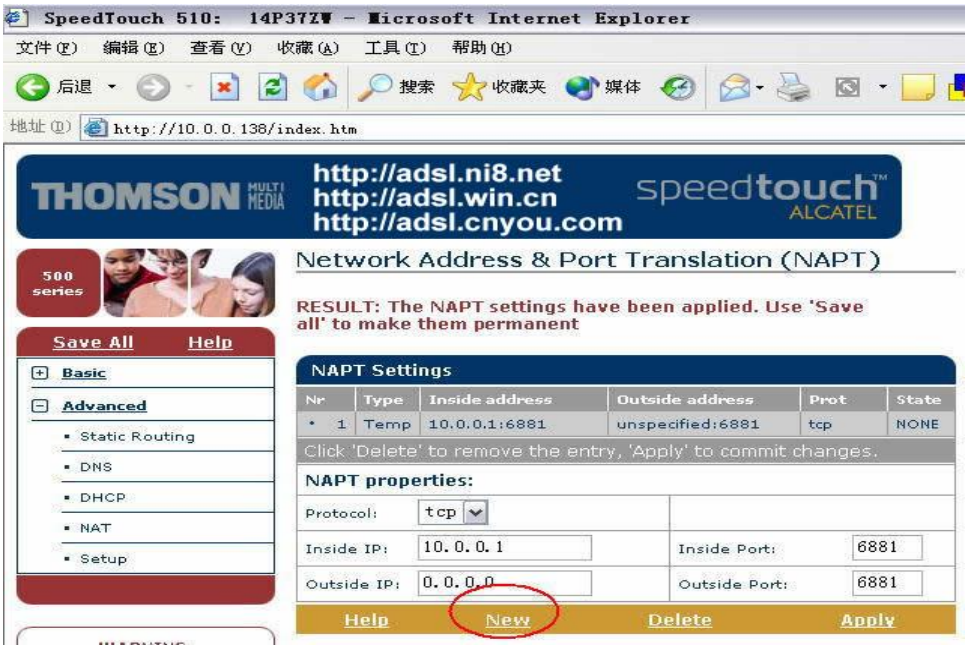


3、需要注意的是，Protocol 一定要选 Tcp，Inside IP 填 10.0.0.1，Outside IP 填 0.0.0.0，Inside Port 和 Outside IP 要填一样的，如 WEB=80、GWT= 5872 按 Apply 确认。



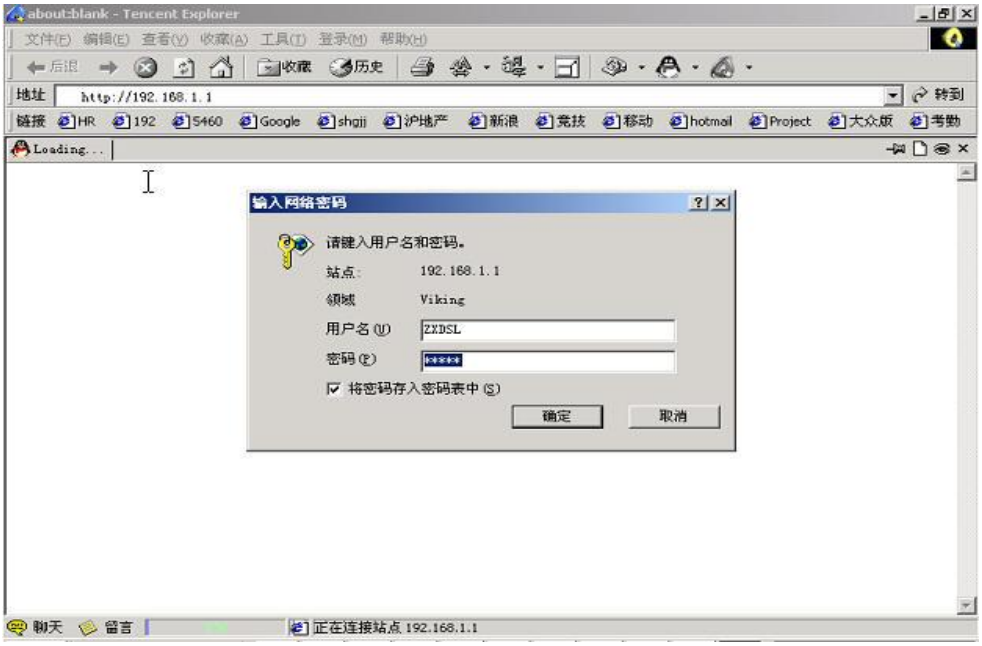
4、按了 Apply 后，我们刚才设置的端口映射就出现在 NAPT Settings 下方。此时若要再进行端口映射，可以点 New，步骤与（3）一样。

注意：设置完毕后，点左上角的 Save All 保存设置，否则拔下 Modem 的电源后 NAT 会自动清空，还要再进行设置。



中兴 ZXDSL 831、TP-link ADSl、D-link 及类似界面 adsl 端口映射方法：

1、确认您的计算机与 ZXDSL 831 已经正确连接、ZXDSL 831 已经出于上电状态。打开 IE，并输入 ZXDSL 831 的以太网网口地址 192.168.1.1，按回车键（Enter），则可出现如下画面：（TP-LINK 和 D-LINK 的一些 ADSL-MODEM 也和此相同）



2、输入用户名、密码（见说明书），然后点击“确定”按钮，进入 ZXDSL 831 配置界面如下：

3、点击“Services”,进入“Services”页面，如下图所示：

4、在 NAT OPTIONS 下拉菜单中选取“NAT Rule Entry”，出现如下界面：

5、关键点击“添加”，在弹出窗口中如下填写：附图有几种端口的设置方法

默认有一条关于 NAPT 的规则不要删除，如果没有，手动添加一条。注意：ID 号是有优先级别区分的。关于 NCPT 的设置应该为 ID1。

ALL NAPT 任意 0.0.0.0 255.255.255.255

本地 IP 和开放端口可以多填，比如：

From：局域网内的服务器 IP

To：局域网内的服务器 IP

From：5872

To：5872

以方便以后更换端口时或需要用交换机连入其它电脑时，不用再设置。

说明：

Rule Flavor 选“RDR”

Rule ID 可任意定义，只要不重复就可以

IF Name 选择你连上公网的接口，如：ppp-0(pppoe 方式)，eoa-0(固定 IP 方式)，根据您连上公网的方式具体选择。

Local Address 项填局域网内开放的机器地址。

Destination Port 项填局域网内开放的端口。

Local Port 项填 ADSL MODEM 的端口。

PS：查考附图填入，未说明部分可以不添，选默认即可。

6、点击“提交”后，进入“Admin”界面里的“Commit&Reboot”项保存后重启即可。一定要提交并保存后重启，不然前面等于白做！

7、其他的端口做法一样！只是端口号不同而已。

8、此方式只对公网用户访问局域网服务有效，局域网用户还是要输入内部地址。

MODEM设置页面里

英文版和中文版的区别

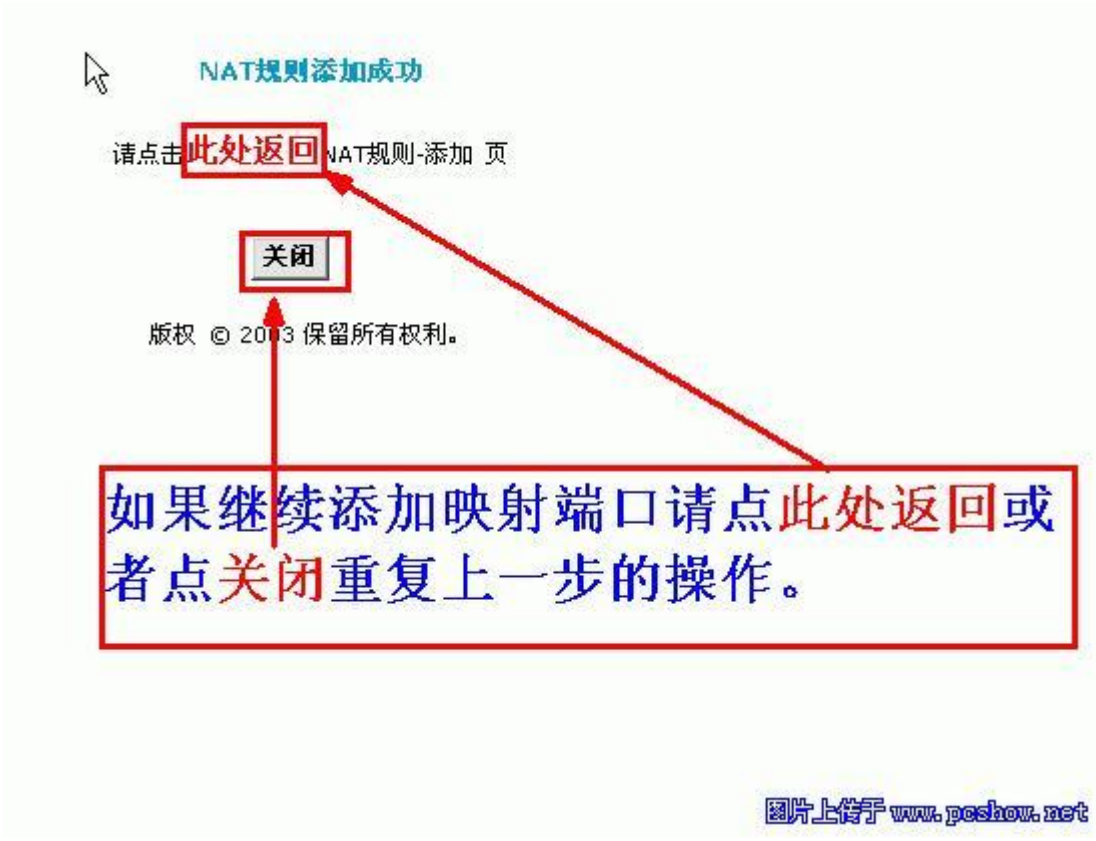
华为 SmartAX MT800 ADSL modem 端口映射方法：

第一步：

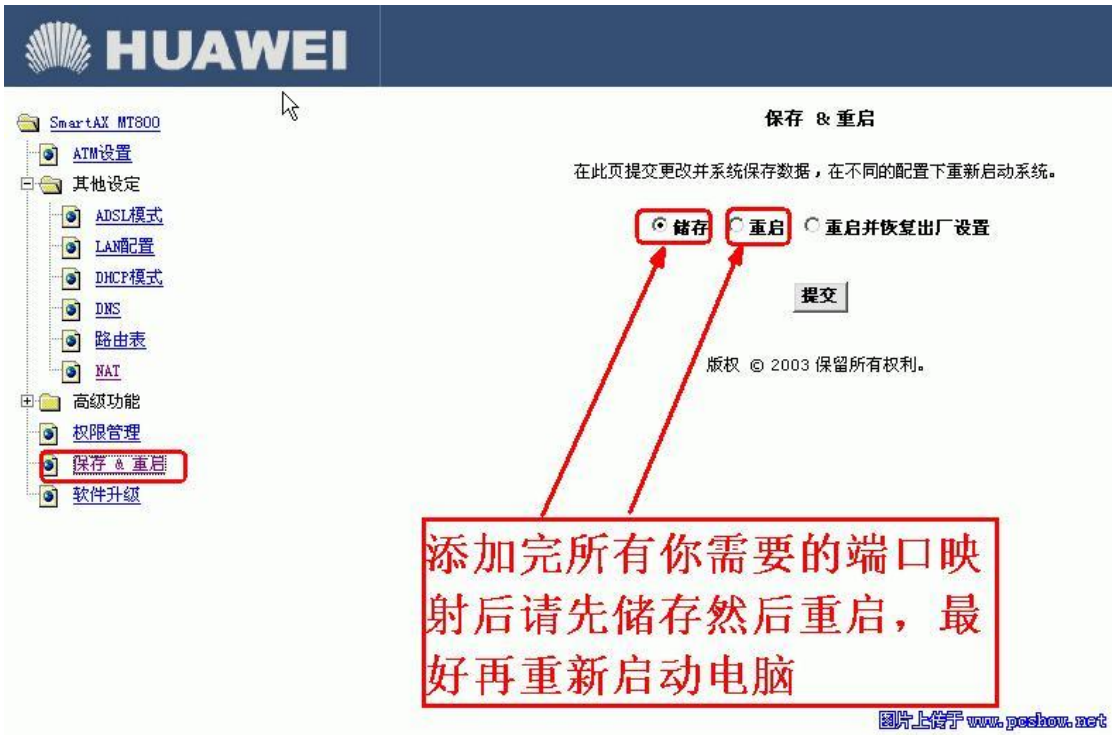
第二步：


NAT规则-添加
NAT规则信息
规则类型：
REDIRECT
协议：
TCP
UDP
本地地址：
192
168
1
3
起始目的端口：
任意其他端口
6881
终止目的端口：
任意其他端口
6881
提交
取消
版权 © 2003 保留所有权利。
此处以开6881端口映射为例，注意：本机地址一定要填你自己的内网IP地址，我的是192.168.1.3
图片上传于 www.pcshow.net

第三步：


NAT规则添加成功
请点击此处返回NAT规则-添加 页
关闭
版权 © 2003 保留所有权利。
如果继续添加映射端口请点此处返回或者点关闭重复上一步的操作。
图片上传于 www.pcshow.net

第四步：


HUAWEI
SmartAX MT800
ATM设置
其他设定
ADSL模式
LAN配置
DHCP模式
DNS
路由表
NAT
高级功能
权限管理
保存 & 重启
软件升级
保存 & 重启
在此页提交更改并系统保存数据，在不同的配置下重新启动系统。
储存
重启
重启并恢复出厂设置
提交
版权 © 2003 保留所有权利。
添加完所有你需要的端口映射后请先储存然后重启，最好再重新启动电脑
图片上传于 www.pcshow.net