

服务器接入认证方案

随着非授权入侵事件的增加，网络上的各种应用系统面临着严重的安全威胁。对于已经部署众多服务器的单位（包括 OA 服务器、电子邮件服务器、数据库服务器等），迫切需要建立严格的访问控制措施，依据用户身份和权限，对服务器的访问行为进行控制和授权，增强服务器的安全性，防止因非法用户和非授权用户访问内部服务器造成的信息泄漏。

● 安全风险分析：

- 1) 无法对用户身份进行认证，外来非法用户可以通过各种手段攻击或访问服务器；
- 2) 无法对内部合法用户进行访问权限控制和授权；
- 3) 访问服务器过程中的数据安全和完整性无法得到保障，非法用户可以通过各种手段窃取或篡改网络上传输的敏感数据；
- 4) 对用户访问服务器的行为缺乏记录，发生安全事件时无法进行责任认定。

● 解决方案：

通过中安源可信网络安全平台，可以对不同的应用系统服务器进行统一的认证授权和访问控制。

- 1) 通过安全网关，可以建立安全服务器区（OA 服务器、文件服务器等），仅经过管理员允许的计算机才能访问此安全服务器区，而非授权的任何计算机则不能访问，从而保护服务器不被非法访问，防止内部敏感信息泄密；
- 2) 结合 USB Key（存放数字证书的硬件介质），采用双因子技术（证书和口令）提供身份认证，基于用户角色实现对网关后端安全服务器资源的访问控制；
- 3) 对整个访问过程提供高速的 SSL 加密隧道，有效保障后端各种应用服务器资源的安全；

- 4) 基于 TCP/IP 协议，支持对双膜用户环境（C/S 模式和 B/S 模式）中应用系统的安全保护；
- 5) 配置简单方便，无须对后端应用服务器进行任何额外操作；客户端不需进行任何额外配置，安装客户端程序后即可使用；

● 系统部署示意图：

