 CVS是一个著名的版本控制工具，无论是对个别程序员还是一个开发团队来说，CVS都是非常有用的版本控制工具，而且它是免费的。CVS的功能也很强大，总体上它是一个C/S结构的软件，使用者首先要架设一个CVS服务器，在CVS服务器上导入项目实例、设置CVS项目访问控制等。而客户通过客户端来访问CVS服务器，客户可以取得项目最新代码副本、提交自己修改的代码等，而客户可以从Internet、LAN、甚至本机来访问CVS服务器。 事实上，许多从事软件开发的个人或且组织都在使用这个免费的软件来帮助进行软件开发。但用户一方面在使用CVS的诸多功能进行版本控制的时候，却忽视了安全方面的设定，于是问题也因此而产生了。我们都知道软件作一种特殊的产品，它是有价值的。对于一个软件公司来说，软件的源代码就是企业最宝贵的资源，如果泄漏出去，可能会给企业带到重大的损失，甚至会影响到企业的生存。许多公司为了让在家或是出差在外的同事也可以进行工作，通常会把CVS服务器放在Internet上，而放在Internet上的CVS服务器就是一个可以泄漏源代码的重要途径，所以也更要认真考虑其安全性的问题。 本文就以一家中小型的软件开发公司为例，来介绍如何在Internet上架设一个安全的CVS服务器，以供分布在各地的员工通过Internet来访问它。 在这个假设的例子当中，这家软件公司采用10M的ADSL专线接入Internet，并拥有一组固定IP。为了达到较高级别的安全，公司逐级采用了以下的策略和

方法： 第一层保护：在网关使用防火墙 在接口网关处安装了防火墙，并划分了DMZ、内网、外网三个区域。CVS服务器和公司其它的对外服务器都放置在DMZ区域中，防火墙对DMZ区域实施不同内网、外网的专门安全策略，对于CVS服务器也实施专门安全策略。 第二层保护：对安装CVS服务的机器进行操作系统加固 公司使用的是Red Hat Linux，最初安装的Linux中缺乏严格的安全设定，需要进行操作系统加固才能达到更高的安全。 第三层保护：利用CVS自身的安全特性 这一部分，笔者将会在后文详细讲解CVS服务器的安装配置等 第四层保护：人员培训和制度 对于使用CVS的员工进行CVS的使用培训，介绍如何安全的从外部连入CVS服务器，以及如何保护个人的CVS账号等信息。由于开发人员可能从公司内网中来访问DMZ中的CVS服务器，也可能通过Internet从公司以外的地方来访问DMZ中的CVS服务器。所要要针对这两种情况制定相应的CVS访问制度，同时要求员工保护好自己的用户名和密码。 在以上四层保护中，本文重点要介绍的是第三层保护。 首先是CVS基本的安装： 1.下载源码 通过摸索引擎可以找到CVS的源代码包，也可从CVS的官方网站cvshome.org上开始寻找，由于CVS历史上也出现过一些安全漏洞，所以建议要定期去其官方网站看看有没有最新版本推出。目前最新的是2003年12月18日推出的1.12.5版本。 