 近年来，一个新的安全防护名词越来越流行，这就是“ 访问控制 ”技术。虽然耳熟能详，但其确切的含义对很多用户来说却非常模糊，它与防火墙、防病毒、IDS等安全防护技术有何不同？它如何保护用户的信息资产？6月6日，在冠群金辰公司的服务器安全研讨会上，通过与冠群金辰公司的访问控制专家交流，记者理解了这一全球最新的安全技术。 什么是访问控制技术？ 顾名思义，访问控制技术通过控制与检查进出关键服务器中的访问，保护服务器中的关键数据。它是一种主机防护技术，但与传统的主机防火墙、主机防病毒或主机入侵检测等防护技术的功能却不同。为了便于理解，冠群金辰公司技术总监郑林先生用了一个非常恰当的比喻描述访问控制技术的功能定位，他以目前正在热播中的世界杯足球赛为例，他说：“如果说安全保护就像保护自己的球网不被攻破一样，防火墙是中卫、IDS是后卫，则访问控制就是守门员随时准备扑出任何非法的进入。 ”一般的防火墙、IDS、防病毒只能检测到异常的进攻行为，而对系统中伪装成正常用户的行为却无能为力，如超级用户权限过大所造成的误操作或有目的的破坏行为等；它们对大型企业中管理跨平台系统所带来的管理开销大幅度增长的情况也毫无办法；对数据库内部的非法操作也无法觉察，而这些问题往往是影响业务正常运行的主要因素。 郑林以冠群金辰的访问控制代表产品eTrust Access Control(eAC)为例，阐述了访问控制技术的内涵：首先，它

是基于主机的安全保护软件；其次，它来源于大型机上实现的安全技术；第三，它对访问的控制可以实现：谁能访问信息？能访问到什么信息？在何时访问？从何地访问？使用什么程序访问？ eAC的安全核心防护功能包括：限制超级用户的权限、资源保护、防止隐形身份、基于主机的分布式防火墙、提升口令安全机制、堆栈溢出保护及审计等。其特色在于为多平台提供了强大而方便的管理功能，它几乎支持目前所有主流的操作系统，所有的安全策略可以通过策略模型数据库（PMDB）集中定制，然后在多级层次配发到各实际的工作服务器上。另外，它能提升各种操作系统的安全级别，而占用系统的资源非常少。 针对目前“ 访问控制 ”名词有被滥用的危险，郑林建议，可以用一个简单的方法区别是否是真的访问控制产品：是否能查出超级管理员的错误行为。 为什么要推出访问控制技术？ 冠群金辰总经理陈葵认为，访问控制技术的提出主要是为了应对两种趋势。一是用户应用环境变化而引起的安全需求的变化。现实中，每个用户的业务都各不相同，这导致他们对安全的需求也不同，比如金融行业强调业务的保密性和可靠性，媒体网站则强调抗服务攻击能力等。因此，安全解决方案和安全管理不可能有一个固定不变的模式，必须针对具体用户业务的实际安全环境，采用个性化的安全解决方案。每一个安全工具只能重点针对一个环节的安全，承担着细分化的任务，新的服务器防护，是为了给关键数据提供一种类似安全保险柜的功能。 第二个趋势是由系统本身的特点和安全技术的演变而造成。这体现在两个方面，一是从网络结构和信息分布上看，用户业务资源（包括文件、数据、服务、设备、用户身份、操作系统核心、

命令等）主要驻留在主机或服务器上，因此，基于主机、服务器的核心防护对用户业务的安全至为重要。另外，传统操作系统本身存在多种缺陷，用美国国防部制订的TCSEC标准来衡量，商用Unix和NT系统只能达到C2级安全标准，这远远不能满足主机安全的需求，而基于主机的访问控制则能提升操作系统的安全级别。安全技术的突破让细致的主机资源保护成为可能，尤其是冠群金辰公司采用CA公司经过多年大型机系统研发而开发出的独特的访问控制产品eAC，其他厂商很难在短时期内超越。 先进的服务器防护理念以及技术上的突破，决定了访问控制技术将成为未来安全防护的主流。