 当传统的终端安全技术(Antivirus、Desktop Firewall…etc.)努力保护被攻击的终端时，它们对于保障企业网络的可使用性却无能为力，更不要说能确保企业的弹性与损害恢复能力。 针对于此，目前出现了几种安全接入技术，这些技术的主要思路是从终端着手，通过管理员指定的安全策略，对接入私有网络的主机进行安全性检测，自动拒绝不安全的主机接入保护网络直到这些主机符合网络内的安全策略为止。目前具有代表性的技术包括:思科的网络接入控制NAC技术，微软的网络接入保护技术NAP以及TCG组织的可信网络连接TNC技术等。 综上所述，NAC和NAP的优势在于其背后拥有思科、微软这样的网络与操作系统的巨头，这些技术将随着其下一代产品同时绑定发布。NAC已经随思科的新一代网络设备一起，在2004年推向市场，而NAP则于2006年底，随微软的Windows Vista操作系统一起，推向市场。而TNC的优势在于其开放性，目前TNC规范已经发展到1.1版本，TCG组织的成员都可以对其提出自己的意见，并且由于技术的开放，所以国内厂商也可以自主研发相关产品，例如之前的TPM一样，可以拥有自主知识产权。 NAC技术网络接入控制(Network Access Control，简称NAC)是由思科(Cisco)主导的产业级协同研究成果，NAC可以协助保证每一个终端在进入网络前均符合网络安全策略。 NAC技术可以提供保证端点设备在接入网络前完全遵循本地网络内需要的安全策略，并可保证不符合安全策略的设备无法接入该网络

、并设置可补救的隔离区供端点修正网络策略，或者限制其可访问的资源。 NAP技术 网络访问保护NAP技术(Network Access Protection)是为微软下一代操作系统Windows Vista和Windows Server Longhorn设计的新的一套操作系统组件，它可以在访问私有网络时提供系统平台健康校验。NAP平台提供了一套完整性校验的方法来判断接入网络的客户端的健康状态，对不符合健康策略需求的客户端限制其网络访问权限。 为了校验访问网络的主机的健康，网络架构需要提供如下功能性领域: 健康策略验证:判断计算机是否适应健康策略需求。 网络访问限制:限制不适应策略的计算机访问。 自动补救:为不适应策略的计算机提供必要的升级，使其适应健康策略。 动态适应:自动升级适应策略的计算机以使其可以跟上健康策略的更新。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com