安全攻略探秘全新一代安全接入技术 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E5_AE_89_E5_85_A8_E6_94_BB_E7_c98_460925.htm 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目前已经随思科的新一代网络设备一起，在2004年开始推向市场，而NAP则计划于2006年年底，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。 TNC技术 可信网络连接技术TNC(Trusted Network Connection)是建立在基于主机的可信计算技术之上的，其主要目的在于通过使用可信主机提供的终端技术，实现网络访问控制的协同工作。又因为完整性校验被终端作为安全状态的证明技术，所以用TNC的权限控制策略可以估算目标网络的终 端适应度。TNC网络构架会结合已存在的网络访问控制策略(例如802.1x、IKE、Radius协议)来实现访问控制功能。TNC构架的主要目的是通过提供一个由多种协议规范组成的框架来实现一套多元的网络标准，它提供如下功能：平台认证：用于验证网络访问请求者身份，以及平台的完整性状态。 终端策略授权：为终端的状态建立一个可信级别，例如：确认应用程序的存在性、状态、升级情况，升级防病毒软件和IDS的规则库的版本，终端操作系统和应用程序的补丁级别等。从而

使终端被给予一个可以登录网络的权限策略从而获得在一定权限控制下的网络访问权。访问策略：确认终端机器以及其用户的权限，并在其连接网络以前建立可信级别，平衡已存在的标准、产品及技术。评估、隔离及补救：确认不符合可信策略需求的终端机能被隔离在可信网络之外，如果可能执行适合的补救措施。 对比分析 以上可以看出，NAC、NAP和TNC技术的目标和实现技术具有很大相似性。首先，其目标都是保证主机的安全接入，即当PC或笔记本接入本地网络时，通过特殊的协议对其进行校验，除了验证用户名密码、用户证书等用户身份信息外，还验证终端是否符合管理员制定好的安全策略，如：操作系统补丁、病毒库版本等信息。并各自制定了自己的隔离策略，通过接入设备(防火墙、交换机、路由器等)，强制将不符合要求的终端设备隔离在一个指定区域，只允许其访问补丁服务器进行下载更新。在终端主机没有安全问题后，再允许其接入被保护的网络。其次，三种技术的实现思路也比较相似。都分为客户端、策略服务以及接入控制三个主要层次。NAC分为：Hosts Attempting Network Access、Network Access Device、Police Decision Points三层.NAP分为：NAP客户端、NAP服务器端、NAP接入组件(DHCP、VPN、IPsec、802.1x).TNC分为AR、PEP、PDP三层。同时，由于三种技术的发布者自身的背景，三种技术又存在不同的偏重性。NAC由于是CISCO发布的，所以其构架中接入设备的位置占了很大的例，或者说NAC自身就是围绕着思科的设备而设计的.NAP则偏重在终端agent以及接入服务组件)，这与微软自身的技术背景也有很大的关联.而TNC技术则重点放在与TPM绑定的主机身份认证与主机完整性验证

，或者说TNC的目的是给TCG发布的TPM提供一种应用支持。从发展上来说，目前NAC与NAP已经结为同盟，即网络接入设备上采用思科的NAC技术，而主机客户端上则采用微软的NAP技术，从而达到了两者 互补的局面，有利于其进一步发展。而TNC则是由TCG组织成员Intel、HP、DELL、Funk等企业提出的，目标是解决可信接入问题，其特点是只制定详细规范，技术细节公开，各个厂家都可以自行设计开发兼容TNC的产品，并可以兼容安全芯片TPM技术。