 网络访问控制(NAC)是最有前途的安全技术之一，但也是误解最多的一种技术。部分原因是，厂商希望利用NAC进行一些宣传炒作，吸引用户的注意力，但事实上他们所销售的只是一些外围产品而已。很多希望考虑NAC的公司因此望而却步，因为他们无法彻底理解NAC到底是什么、有什么作用以及投资需求到底有多大。 给NAC一个定义 要想拨开这团迷雾，第一步就是定义NAC。根据Forrester Research的定义，“ NAC是一种软件技术和硬件技术的混合体，可根据客户系统符合策略的情况对其访问网络能力进行动态控制。 ”目前市场上可列入此类的产品包括Cisco公司Network Admission Control架构和Juniper公司统一访问控制环境中的各个组件。可以列入此类的单一设备包括ConSentry Networks、StillSecure和Vernier Networks等公司的产品。其他的NAC厂商，如Lockdown Networks和Mirage Networks也在通过各自的伙伴进行此类产品的研究与推广工作。 可信计算集团(TCG，Trusted Computing Group)是一个编写NAC标准的行业集团，其目标是促进多厂商互操作性。该集团也拥有自己的NAC方案。可信网络连接(TNC)规定了厂商用于TNC 架构的各类设备上的产品接口。TCG将NAC定义为一种“ 能够在端点连接至企业网络的过程中应用和执行各类安全要求的开放的、非专用的规格。 ”因此，厂商可以根据TNC的网络访问控制标准来构建自己的产品，但也可以依靠其他产品来实现可操作的网络访问控制

部署。 可以说，NAC是高层次的技术。实际上，网络访问控制是一个扫描计算机及其他设备的进程，它可以在这些计算机或设备进入网络之前确定其是否符合企业在安全方面的策略。例如，这些对象的病毒扫描软件是否更新至最新版本?操作系统是否已经施加补丁?它们的个人防火墙是否启用? 这一进程需要用到一种引擎，而该引擎应当将扫描结果与策略进行对比，确定设备是否有资格获得访问权。它规定这些设备必须能够执行策略引擎的决定，例如阻止访问、限制访问某些资源或只允许访问一个能够更新安全功能的独立网段。 理解网络访问控制的世界 这才是网络访问控制的核心。一些公司自诩为网络访问控制厂商，但其真正的意思是，自己的产品能够适用一个更为宽泛的网络访问控制环境。 例如，CA声称该公司已经加入了Cisco公司的NAC计划，利用其eTrust反病毒和反间谍软件为Cisco的Trust Agent提供状态信息。该代理程序可从桌面计算机和笔记本中安装的CA的软件和其他软件上收集数据，为这些试图访问网络的计算机开发出一套配置方案。 类似的还有IBM公司的Tivoli Security Compliance Manager。该产品可以兼容Cisco的网络访问控制技术，因为它能够扫描进入网络的计算机。但该产品本身并不能规定设备是否获得访问权，它仍然需要Cisco或其他厂商的基础设施来执行这些策略。 eTrust和Security Compliance Manager软件适用于网络访问控制(NAC)架构，但却无法创建自己的网络访问控制环境。Cisco、Microsoft和TCG都列出了数十家合作伙伴，并表示这些伙伴的产品适用于自己的网络访问控制方案，并且都声称自己是网络访问控制厂商。因此，客户必须弄明白这些厂商所说的“ NAC支持 ”到底是什么意思。 还有另

外一个关键因素也使问题变得更为复杂。微软公司拥有自己的网络访问控制架构，名为Network Access Protection(NAP)。由于该架构具备微软的支持，并且可以利用微软公司无处不在的服务器和桌面软件，因此NAP是网络访问控制领域中一个非常重要的角色。但问题是，该架构中关键的组件目前还没有上市，因此除了微软公司NAP平台的公开测试版之外，谁也无从对其互操作性进行全面的测试。 从好的一方面来看，包括Cisco在内的75家厂商都已经承诺其设备上市时将与微软的NAP组件实现互操作。Cisco公司正在开发NAP和 Cisco NAC之间的互操作性。同时Cisco还在积极推动IETF通过NAC的相关标准。虽然Cisco目前并没有参加TCG，但有30家合作伙伴正在出售与 Cisco NAC兼容的设备，另外还有27家厂商正在开发此类产品。 确定网络访问控制的要求 Opus One资深合伙人兼网络世界实验室联盟成员Joel Snyder指出，无论厂商的选择是什么，企业必须知道自己在采用NAC之前需要在网络方面解决哪些挑战。但令人惊讶的是，很多企业都急于采用网络访问控制，但这些企业并没有制订好保护其投资的商业要求。 科罗拉多州立大学商学院是较早采用网络访问控制的用户之一，而且该学院在采用此类技术之前就已经制订了明确的目标。这所学院的技术主任Jon Schroth指出，学院希望控制访客和学生对网络资源的访问，但也希望尽可能地保持基础设施的开放性。同时，他也不想添置大量的设备，或者在用户的设备上安装任何软件。 Schroth选择了Vernier公司的EdgeWall设备。该设备可对用户进行验证、扫描其机器并根据学院Active Directory服务器中提取的数据来执行各项策略。他说: “ 我们采用的全部是微软的系统，因此我们希望尽可

能地利用这些资源。”由于EdgeWall在接入交换机和核心交换机之间执行各项策略，因此它可以在不修改网络拓扑结构的情况下与学院的HP ProCurve和3Com交换机和谐共处。其他的网络访问控制方案，例如Cisco的方案和TNC方案，都使用交换机上的802.1X端口验证来执行各项策略。Schroth表示，他最终可能选用这些架构中的一种。就目前而言，EdgeWall的工作状况良好，而且在学院计划两年后对交换机进行升级之前，EdgeWall很可能仍然能够满足所有的需要。他说:“也许到那时，我们会采用一种能够集成到交换机中的更为广泛的网络访问控制架构。”另外一家较早采用网络访问控制技术的用户在最近斥资25万美元采购了全新的Extreme Network交换机，而该技术对于保护这项投资起了非常关键的作用。KAMO Power公司是一家总部设在俄克拉荷马州Vinita市的一家电力公司，主要为堪萨斯、阿肯色、密苏里和俄克拉荷马州提供服务。该公司IT总监 Robert Lemm说:“我不可能为了满足一个项目的需求而花费25万美元的巨资去购买交换机。”Lemm表示，KAMO Power公司希望利用网络访问控制更好地保护其网络免受其能源合作机构有害流量的危害。他曾经考虑过Cisco NAC设备，但后来又放弃了，因为这种设备必要使用Cisco的交换机。即使他已经拥有了这些交换机，在这些交换机上实施NAC必然会导致额外成本的产生。他说:“如果我们已经有了Cisco交换机，我们仍然需要为每一台交换机购买授权。”如果没有这些授权，Cisco也可以将CiscoSecure Access Control Server(ACS)网络访问控制设备部署在KAMO Power公司的Extreme交换机上并执行访问策略，但如果这样做，每一台ACS设备都可能成为一个潜在的独

立故障点。他说:“ 从网络可靠性的角度来说，这种做法是很不明智的。 ”Lemm也排除了Extreme公司基于其Sentriant设备的访问控制系统。去年，当他考察该系统时，该系统可以在第3层进行筛选，但无法完全适应到第7层，而第7层的能力正是他希望获得的。 最终，他选择了Juniper的Infranet Controller策略引擎，并将其与Microsoft Internet Authentication Service验证服务结合在一起，确定终端设备应获得哪种访问权。Extreme的交换机和Juniper集成安全网关(Integrated Security Gateway)可以与防火墙、VPN和入侵探测系统结合在一起形成完整的策略执行点。 他说，虽然这些部署工作使用户避免对所有的交换机进行替换，但这仍然没有达到理想的境界。Juniper需要一整套企业范围的管理系统来管理网络访问控制系统的各个部分，从而节省管理工作所消耗的时间。目前，他使用Web接口直接管理单个机器，或者利用NetScreen Security Manager来管理Infranet Controller。 网络访问控制的基本原则 网络访问控制的基本原则是，虽然这类技术还是一种没有完全定义的新兴技术，但它在适当的条件下仍然可以发挥巨大的价值。Forrester Research的分析师Rob Whiteley指出，应用网络访问控制的关键是只用它来满足一些具体的需求。Whiteley认为，用户在选择网络访问控制技术时应当有长远的发展眼光，使未来的安全性和网络采购活动能够适应这些处在不断发展过程中的、更为宽泛的网络访问控制架构。他说:“ 谁也不希望部署一串安全孤岛，因此这一点非常重要。 ”网络访问控制与您 在确定网络访问控制产品是否适合您的企业之前，您可以向自己提出以下几个问题: * 如果终端在连接到网络之前就可能已经受到感染，那么它对网络构成的危险

有多大? * 在三种主要的网络访问控制方案(Cisco、TNC或NAP)中，哪一种最容易集成到我现有的安全环境中?我是否能够等到标准或互用性测试出台后再来选择自己的方案? * 与目前正在进行的其他安全计划相比，网络访问控制的重要性有多高? * 在实施网络访问控制时会对网络产生一些干扰，我能承受多大程度的此类干扰? 您也可以向厂商提出如下问题: * 贵公司的产品在哪些方面能够适应更为宽泛的网络访问控制架构?当单个机器的状态发生改变时，它是否能够验证和扫描终端、检查策略符合性、执行策略、创建策略或管理策略? * 贵公司的网络访问控制产品的未来发展路线图是怎样的? * 要想支持贵公司的网络访问控制设备，我需要对网络基础设施进行哪些升级和替换? * 贵公司是否支持移动访问? * 贵公司是否可以证明产品的投资回报率? 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