
# NAC 技巧与应用

# NAC 技巧与应用

如今网络访问控制（NAC）技术正趋向成熟，然而由于 NAC 的范围过于广泛，用户面对各种各样的 NAC 产品总是会有很多顾虑。本技术手册从网络访问控制技术、网络访问控制的选择技巧、网络访问控制的实施技巧和网络访问控制的实际应用这四个方面对网络访问技术进行了介绍，希望能给大家一些帮助。

## 网络访问控制技术

过去的两年里，网络访问控制（NAC）技术已经成为信息安全业内耳熟能详的术语。但 NAC 是不是仅仅只是炒作呢？ 许多预测说 2009 年会是“NAC 之年”。这一预测似乎并没有完全变成现实，但人们认为 NAC 在普及上的延迟更多的是因为经济不景气，而不是因为缺乏使用 NAC 的热情和意愿。人们仍然坚信，NAC 技术运用得还不够，NAC 的市场将会有显著的增长，特别是当经济开始好转的时候。

- 网络访问控制：是时候应用了吗？
- 网络访问控制技术：言过其实还是运用不够？
- NAC 与端点安全框架 何去何从？

## 网络访问控制的选择技巧

网络访问控制（NAC）的采用正在增长——08 年上半年的 Infonetics 报告中就报告了与 07 年的第一季度相比，增长了 16%。但是即使是在巩固的市场上，为您的企业选择最好的技术也不是件简单的事情。

- 如何选择 NAC 服务

## 网络访问控制的实施技巧

2003 年，由于 Blaster 蠕虫的活跃，专业安全技术人员首次开始对网络访问控制（NAC）进行关注。六年后的今天，网络访问控制仍然缺少一个单一的标准，并且被证明它比第一次出现时更难实施，并且 NAC 现在如果说不是至关重要的但也仍然是一项非常有价值的安全技术。

- 网络访问控制应该包括什么？
- 部署网络访问控制（NAC）的诀窍(上)
- 部署网络访问控制（NAC）的诀窍(下)
- 控制网络访问的五个步骤
- 企业如何免费实施网络访问控制技术(NAC)

## 网络访问控制的实际应用

如果有些人可以进入你网络的内部，那么他们就可以获得你的 Windows 系统的访问权。你需要在你的网络设备上执行严格的访问控制列表，并且只对那些需要的用户授予访问权。那么网络访问控制应怎么具体应用呢？

- 实例:网络访问控制帮助航空公司减少安全风险
- 如何使用网络访问控制来保证非盈利性组织安全

# 网络访问控制：是时候应用了吗？

网络访问控制(NAC)已经成为了一个不能回避的网络安全流行术语。随着 50 多家厂商声称已经拥有某种形式的 NAC 解决方案，这个事情更加模糊不清和令人困惑了。如果厂商是正确的，现在正是部署 NAC 的时机。从许多方面看，这些厂商并没有离题太远。

市场研究公司 Gartner 副总裁和著名分析师 John Pescatore 说，有许多言过其实的宣传。所有这些厂商对于 NAC 都有自己的说法。但是，你不必等待开始实施这些技术。

据 Pescatore 说，企业必须首先查看具体存在什么问题或者痛点，然后再利用 NAC 来解决。这些问题可能会指出应用哪一类 NAC 是一个好的起点。

**定义你的 NAC 目标**

市场研究公司 Current Analysis 高级分析师 Andrew Braunberg 说，每一个人对 NAC 都寄予很高的希望。但是，他补充说，需要确定 NAC 的准备情况，把问题归纳为企业必须首先问自己的几个简单的问题。要记住的事情是:你的起点在哪里?我要解决的痛点是什么?NAC 解决方案能达到那个目标吗?当你做这个事情的时候，你的 NAC 解决方案的整个内容是什么?

Pescatore 和 Braunberg 基本上一致认为，企业正指望把 NAC 用于客户网络接入。虽然安全和保密的客户接入是考虑采用 NAC 的合理理由，但是，它并不需要全新的基础设施来容纳思科的 NAC 框架或者微软的 NAP 等产品。

Braunberg 表示，提前确定 NAC 部署的规模是有好处的，特别是在许多公司有一个“如果你没有在每一个地方都使用 NAC 的话，NAC 有什么好处?”的想法的时候。

Braunberg 说，我认为，人们应该开始解决他们现在感到痛苦的问题。但是，仍有许多市场教育工作要做。

市场研究公司 Burton Group 高级分析师 Eric Maiwald 也赞成这个观点。当问到企业现在是否应该开始考虑 NAC 的问题时，他说，这个问题没有答案。

Maiwald 说，企业必须评估推动他们采用 NAC 的因素是什么。对于大多数机构来说，考虑 NAC 是因为 NAC 是一种最新的和最伟大的技术，因为遵守法规的问题，或者因为他们要控制客户或非雇员访问企业网络。

Maiwald 说，控制谁能够进入你的网络是很长时间以前做不到的事情。NAC 确实是一种新东西吗?或者 NAC 是下一代安全漏洞管理技术吗?NAC 是下一代入侵防御系统吗?

由于 NAC 能够用于网络的不同点上(如内部、带外以及软件代理等)，企业需要调查他们强制执行的点应该在什么地方。

Maiwald 说，强制执行点是这里关键的点之一。他们要在哪里强制执行网络访问控制呢?如果我要在内部应用，如果这个设备失效了，我应该做什么?

企业应该考虑哪一种类型的 NAC 在他们的环境中的影响最小，是 ConSentry、Vernier 和 Nevis 等公司的内部解决方案，Lockdown 和 Forescout 等公司的带外解决方案，还是 Elemental 和 InfoExpress 等公司的软件代理?Maiwald 说，内部和带外设备似乎正在受到许多关注。

**NAC 的五项功能**

Braunberg 说，完整的 NAC 解决方案应该堵住五个漏洞。它应该执行准入之前的检查、主机状况检查和准入之后的检查。它还应该熟悉 ID 和基于 ID 的网络资源。

Braunberg 表示，总的来说，没有一家厂商能够提供一个同时解决这五个问题的最好的解决方案。但是，总的来说，这项技术已经足够成熟，能够解决指定的每一个领域的问题。现在，Juniper 公司第二阶段的统一访问控制产品拥有最广泛的方法。

Braunberg 补充说，对于最初使用 NAC 的企业来说，同时解决这五个 NAC 方面的问题是没有必要的。他说，我认为你不需要同时解决所有这些领域的问题以便从今天的 NAC 解决方案中获得价值。

市场研究公司 Gartner 的高级分析师 Pescatore 说，有三种广泛类型的 NAC 技术。所有这些技术都能达到不同的监视水平。首先，有一些从思科和微软等公司产品升级的基础设施。这些是最完整的 NAC 解决方案。但是，许多公司都没有提出这种广泛的 NAC 部署，因为这种解决方案价格昂贵，而且需要彻底升级基础设施。

Pescatore 说，大多数企业都没有准备那样做。我们对客户说，如果你已经升级了你的思科网络，这个事情是你应该考虑的。

Pescatore 说，NAC 还以软件代理的方式提供，如杀毒软件、个人防火墙和设置管理工具等。一些小厂商还制作 NAV 设备。这些设备不能解决每一个 NAC 的痛点。但是，这些设备为更广泛的应用打开了大门。他建议说，你应该坐下来考虑你应用 NAC 的真正动机。

一些公司要在允许一台设备进入网络之前确定这设备是不是危险的或者有安全漏洞的。其它一些公司不得不允许非雇员或者非雇员的 PC 进入网络。

Pescatore 说，如果那是你的全部动机，你就不需要批准在全面升级中的一切花费。

其它公司采用 NAC 的动机还包括对于安全的担心。例如，一家公司也许允许非雇员的 PC 进入网络。但是，这些公司也许还需要找一些工具监视网络中可能存在的潜在威胁。

Pescatore 说，你可以从小范围的应用开始，做客户网络，然后再进一步发展。如果这个网络明年要升级路由器和交换机，最好考虑使用思科 NAC 和微软的 NAP。

一些公司对繁荣和充满言过其实的宣传的市场中的 NAC 技术的成熟程度仍存在疑问。但是，Pescatore 指出，一些公司正在使用各种类型的 NAC 产品，没有出现重大的故障。至于完全的 NAC 框架，他建议谨慎对待。

他说，许多公司正在把 NAC 技术用于客户访问，而且效果很好。但是，真正的问题的全面的解决方案发挥作用的很少，除非你正在试验一个全面的解决方案。

Pescatore 补充说，无论你的起点在哪里，任何水平的 NAC 应用都不是一次性的投资。

原文链接：http://www.searchsecurity.com.cn/showcontent_1168.htm

*（作者： Andrew R. Hickey 来源：TechTarget 中国）*

# 网络访问控制技术：言过其实还是运用不够？

过去的两年里，网络访问控制（network access control，NAC）技术已经成为了信息安全业内耳熟能详的术语。但 NAC 是不是仅仅只是炒作呢？

去年，我做了许多预测说 2009 年会是“NAC 之年”。这一预测似乎并没有完全变成现实，但我认为 NAC 在普及上的延迟更多的是因为经济不景气，而不是因为缺乏使用 NAC 的热情和意愿。我仍然坚信，NAC 技术运用得还不够，NAC 的市场也将会有显著增长，特别是当经济开始好转的时候。

## 网络访问控制（NAC）技术概述

网络访问控制技术给企业带来了两个主要好处：网络认证和端点安全检查。通过结合这些功能，安全专家能对个人和系统访问网络更有信心。它的目的是防止威胁的都未经授权的用户访问网络，还有授权用户访问网络的易受攻击的（或更糟一点，受感染）的设备。

在关键的 NAC 产品的成功在于高质量的姿态检测代理（posturing agent）：该软件运行在端点上，确定该设备是否符合该组织的安全政策。最好的产品能够把对安全软件的当前和合理操作的检查与操作系统特定的安全配置参数验证结合起来。

一般来说，现在的 NAC 产品在这些上面都做得不错，特别是加上现有网络设施的安全功能（通常做法是是从其它设备的厂商那里采购 NAC 产品）。在这种情况下，当 NAC 产品检测到用户非法身份验证或设备不能满足该组织的姿态的要求，它就能够通过把设备限制在交换机口的一个隔离区来收回访问权限。

## NAC 是否物有所值？

这个价值百万的问题就是部署 NAC 所耗费的大量时间和资金是否能给企业带来足够的回报。在考虑这个问题时，我鼓励你仔细考虑并回答几个问题：

在我们这种应用环境，NAC 能成为现有问题的解决方案吗，还是用它来查找问题？ 不要仅仅因为大家都在说 NAC 就去购买 NAC 产品。一定要确定你有正当的业务目标，而且这个目标最好通过 NAC 达到。

我们的端点安全控制配置是否有问题？ 如果你有一个网络，完全是管理的系统和你的存在强制执行的恶意软件防护软件和安全设置，通过配置管理系统，您可能没有必要的姿态所提供的保护的 NAC 。 如果你的网络安全是由受管理的系统组成，并已通过配置管理系统配备好了恶意软件防护软件和安全设置，这样的话，你可能并不需要 NAC 提供的姿态防护（posturing protection）功能。

我们的网络有大量的未知用户吗？ 如果你运营的网络有大量的访客，比如学院或大学的网络，那么 NAC 就是一种很好的途径，用以验证访客是否有权限访问网络，以及防止他们把受感染的设备接入到网络中。

如实回答这几个问题可以让你对 NAC 到底能给你的企业带来些什么了然于心。如果你有意在你们那部署 NAC，那么我建议你再读读我的另外一篇文章《Phased NAC deployment for compliance and policy enforcement》，它详细讲解了 NAC 的实施策略。或许你也会对我播客上讲解结合现有安全工具使用 NAC 的内容感兴趣。NAC 是一项复杂的技术，如果配置和管理得当，它能运作得很好，因此如果你们的业务如果真的需要部署 NAC 的话，就不要让那些夸夸其谈影响你对 NAC 的评估。

原文链接：http://www.searchsecurity.com.cn/showcontent_23797.htm

*（作者：Mike Chapple 译者：Sean 来源：TechTarget 中国）*

# NAC 与端点安全框架 何去何从？

端点安全大概是近年来信息安全领域的一个热门话题，这并不奇怪。不管你多么努力地防御网络边界，漫游的笔记本电脑和设备总是必然会把蠕虫、病毒和间谍软件带入到你的网络上。

配置了无线适配器的大众化笔记本电脑具有的移动功能解放了大批员工，他们可以在任何地方办公，无论在办公室、在家里还是在路上。咨询顾问和厂商可能连接到你的网络使用一小时或者一天——你如何防范他们可能带来的潜在危害呢？

网络基础设施和操作系统软件领域的两大巨头：思科和微软各自都启动了这方面的计划，确保端点设备只有符合安全策略，才可以访问企业网络。并不奇怪的是，思科的网络访问控制（NAC）依赖思科的交换基础设施；而微软的网络访问保护（NAP）通过 Windows 操作系统发挥作用。除了这些普遍但专有的方案外，可信计算组织（TCG）正在开发基于标准的可信网络连接（TNC）。

如果让你来选择，该选择哪个方案来保护端点安全、让本地网络避免遭到已成为漫游恶意软件收集器的“已中招”机器的攻击呢？

**确实马上需要解决方案**

面对需要立即引起注意的安全问题，你应当寻求这样的解决方案：可以定义细粒度策略、检测连接到网络上的每个设备、评估遵从策略的级别、执行访问策略，以及补救未遵从策略的机器。

这对任何一个安全系统来说都是过高要求，积极采用端点安全并非易事。三大架构：NAC、NAP 和 TCN 都不完整，实施成本也很高；而且很复杂，不易理解。它们都从不同方面来处理端点安全问题，所以彼此并非相互排斥也就不足为怪了：

- 思科的 NAC 专注于网络基础设施和策略定义及管理；当然，它假定你会使用许多思科路由器，采用思科的安全解决方案；而且在将来牢牢保护端点时，希望继续使用思科的系列产品。
- 微软的 NAP 偏重于健康评估和补救方案；它假定你从微软服务器和桌面系统开始着手；并且假定你主要关注的是确保它们安全运行。

- 可信计算组织的 TNC 采用了粗略的架构方案；它假定每个桌面系统都含有一种专门的硬件，负责验证端点的安全未遭到破坏；并且依靠这个硬件来监控及执行端点策略。

我们不妨看一下这些计划，看看它们声称具有的功能以及各自存在的不足。

**思科的 NAC**

NAC 处于领先位置，这归功于同时出现了支持它的架构和产品。NAC 旨在通过实施在路由器和交换机以及 Windows 和 Linux 客户端中的可信模块来保护网络访问。

现有众多厂商支持 NAC，理由很充足：你需要其中几家厂商来组建一套完整的解决方案，以便满足端点安全需求的所有五个方面。你至少需要在端点上运行两个代理，才能处理比较复杂的策略以及检查遵从 SSL VPN 的情况。

NAC 使用的客户软件思科可信代理（Cisco Trusted Agent）负责收集设备信息，并使?02.1X 机制，把信息传送到思科的远程验证拨入用户服务（RADIUS）服务器：安全访问控制服务器（ACS）。而 ACS 与第三方策略服务器（反病毒和补丁）进行通信，确定遵从情况，并通过交换基础设施执行网络访问。

有些分析师认为，NAC 需要部署太多的部件；实施起来可能有难度，因为要管理所有的互联网操作系统（IOS）更新工作，以便各部分协同工作；而且基础设施出现变化时，需要维护。

NAC 的问题在于：它自身会带来全孤岛；依赖思科的 RADIUS 服务器作为惟一的验证机制；而且思科交换机需要最新版本的固件。此外，NAC 不一定与思科的遗留基础设施协同工作，除非遗留系统更新到最新固件。

英国电信 Radianz 公司是一家面向金融服务行业的知名 IT 服务商，公司副总裁兼首席安全官 Lloyd Hession 说：“NAC 问题的一方面在于，你必须升级 IOS 版本。我的网络上共有 4 万个路由器，对它们进行更新可不是容易的事情。”Hession 改而选择了 ConSentry 公司，那样他不需要对网络进行 MAC 层过滤和访问控制。ConSentry 销售的嵌入式安全设备能够自动评估及执行端点安全策略，确保遵从策略。

另外，NAC 架构缺少补救功能——它在管理端点本身的补丁级别方面不尽如人意。另外，设备经过评估后，采取什么措施方面缺乏很强的灵活性。只有这两种情况：要么通过评估，允许连接到网络上；要么未通过评估，被转移到访问权限有限的某个虚拟局域网（VLAN）上。

Altiris 公司的产品经理 Rich Lacey 负责处理本公司的 NAC 兼容产品，这种产品提供了通过桌面管理和复制来补救的解决方案。他说：“通过补救机制，让客户端摆脱隔离区域，这确实是一门技艺，这也是我们现在所做的。”

思科得到了迈克菲、趋势科技和赛门铁克等反病毒产品的支持，另外还得到了几家软硬件厂商的支持。

Hession 并不觉得把代理安装到所有端点上特别吸引人。他说：“代理存在的问题在于，你最终不得不安装多个代理，以便支持你想要处理的所有事情，比如反病毒和访问控制。思科的 NAC 迫使我往代理这个方向走，但我不想走这条路。”

思科公司安全技术部门的产品经理主管 Russell Rice 说：“我们目前支持代理。但我们也会开发无代理的解决方案，那样就能主动扫描及评估其他非 Windows 设备。”

NAC 正在把支持范围扩大到代理以外的领域，而 Qualys（其产品 QualysGuard 支持 NAC）等厂商正在提供这种服务：可支持无代理监控无法使用代理的网络设备，比如打印机及其他嵌入设备。

**微软的 NAP**

NAP 还没有实施在任何产品中，不过这项方案得到了 60 多家厂商的支持，其中许多厂商为了保险起见，同时支持 NAC。

NAP 把安全策略管理和执行功能集成到了 Windows Server 中——自活动目录的早期以来，Windows Server 就多少缺乏这种功能。

微软公司负责 NAP 的 Windows Server 事业部的集团产品经理 Mike Schutz 说：“NAP 将会提供通过各种机制来执行策略的功能，使用验证主机的 IPSec、802.1X，或者通过 VPN 或 DHCP。”

与 NAC 一样，NAP 也使用客户软件：隔离代理（Quarantine Agent），把信息传送到微软的网络策略服务器；与思科的 ACS 一样，网络策略服务器也与第三方服务器一起检查遵从策略的情况。NAP 承诺会提供多种执行选项，包括 DHCP、IPSec VPN 和 802.1X。

NAP 最初将单单支持 XP SP2、Longhorn Server 和 Windows Vista，需要在每个设备上安装 NAP 更新。这将给使用旧版本 Windows 的公司带来问题，而且需要使用新的操作系统，还要测试及管理 XP 升级。另外，验证和执行服务器即 DHCP 和 RADIUS 服务器将需要 Longhorn，这就需要进一步升级，NAP 的专有性因而更明显了。

Schutz 说："我们并不认为 NAC 和 NAP 是两者择一的情况。我们已宣布，我们将开展互操作性解决方案方面的合作，那样客户就可以选择满足自身需求的最佳方案。"不过，微软和思科目前都还没有与 TCN 解决方案兼容，眼下也没有这方面的计划。

佐治亚州富尔顿县政府已经在试用 NAP，使用早期版本的微软服务器和 Vista 桌面电脑及笔记本电脑。

负责管理该县 IT 部门部署 NAP 的 Keith Dickie 说："一切都仍处于测试中。不过我们的几名 IT 员工正在生产环境的机器上使用 NAP，没有任何问题，包括把赛门铁克的诺顿反病毒软件与微软的 SMS 和 Windows 服务器集成起来。"

该县在使用 IPSec 验证，部署的 NAP 可以检查一系列健康要求，包括确保诺顿反病毒软件的版本最新。

**可信计算组织的 TNC**

TNC 由支持一批开放标准的几十家业界重量级公司（思科除外）组成。好消息就是，标准或多或少符合之前提到的网络访问控制安全的五个要求：策略定义、检测、评估、执行及补救。坏消息是，不是所有标准都已经得到了定义；糟糕的是，也没有多少产品支持真正实施解决方案所需要的大部分标准。

TNC 的关键要素是支持 RADIUS 和 802.1X 验证服务器和协议的功能，另外还有端点上的可信硬件芯片和软件。

TNC 的联合主席、Juniper Networks 公司的产品经理 Steve Hanna 说：“这可不是需要全面改动的叉车式升级（forklift upgrade）。”它与思科采用的方案有着尤其明显的区别，后者使用思科的 ACS 验证服务器。

名为可信平台模块（TPM）的一种公钥基础设施（PKI）芯片增强了验证功能，有助于通过硬件实现方案来防止软件遭到潜在破坏，从而保护笔记本电脑的安全，远离未授权用户，比如窃贼或者仅仅捡到丢失笔记本电脑的人。

Hanna 说：“如今你根本没法信任软件，因为 PC 可能遭到了零日漏洞（zero-day vulnerability）或者用户通过互联网下载的东西的破坏。要发现这个问题，惟一的办法就是借助可信硬件。”许多笔记本电脑厂商已经把可信硬件模块添加到了各自的产品线当中，包括戴尔、富士通、惠普和联想。

一旦验证检查获得通过，可信硬件里面的程序就会把控制权交给第三方软件代理，由代理检查设备遵从策略的情况，与负责处理网络验证和登录访问的 TNC 架构协同工作。作为一项开放标准，TNC 有望使用任何一种执行机制。

思科的竞争对手 Juniper 已经在提供符合 TNC 的产品，这不足为怪。Juniper 之前收购了开发 RADIUS 服务器产品的 Funk 软件公司。

**SSL VPN 支持是软肋**

这三款解决方案都缺少了支持 SSL VPN 有功能。TNC 的 Hanna 说：“谁都没有支持 SSL VPN 的任何产品，我们还无法支持它。不过我们预计很快就会出现这样的功能。”

SSL VPN 方面要走很长的一段路。没多少厂商提供支持众多反病毒扫描器的功能，许多只支持 Windows/IE 组合，或者在网络登录之前扫描网络连接。问题的一方面在于，大多数 VPN 厂商在完成开发了第一批产品之后才添加了支持端点安全的功能。举例说，北电网络（Nortel）和 Aventail 在各自的 VPN 产品中有两套不同的访问控制——一个支持端点安全，而另一个不支持。许多 SSL VPN 厂商正与第三方端点安全厂商合作——提供 NAC、NAP 和 TNC 之外选择的市场在日渐壮大。

**不能等下去？**

虽然思科、微软和可信计算组织之间的营销大战日渐升温，但企业们在寻求这样的解决方案：眼下管用；又可能支持 NAC、NAP 和 TNC，以便将来升级。有几家厂商现在交付的产品至少能够满足保护网络访问的部分要求。

这些产品提供众多检查及执行选项，以控制得到管理及没有得到管理的设备，并且为客户提供了很大的灵活性。许多产品提供基于登录、代理、ActiveX 或者 Java 的扫描方法，确定端点遵从策略的情况；你可以根据自身的要求，对这些扫描方法进行混合搭配。另外，这些产品日益提供 DHCP、802.1X、基于代理的、嵌入式设备或者 NAC 等选择，而不是单一的执行机制，所以贵企业确实可以选择与自己的环境一致的方案。

实际上，思科拥有与自己的 NAC 架构并不完全相符的第二种方案，名为“干净客户机访问”（Clean Client Access），这是它收购 Perfigo 公司的成果。它能够实现基于代理的端点评估、客户机与策略管理以及补救等服务。

**没有简单的答案**

事实上，没有哪家厂商拥有完整的解决方案可以保护你的所有端点、确保资源安全。你要找到一款产品来处理不同的安全策略，从而保护那些漫游笔记本电脑和关键的网络资产。另外，除非你有一个完全同类的网络，全部由运行 IE 的 Windows XP 用户组成，否则就需要支持其他操作系统和浏览器。尽管厂商的说法都很动人，但没有哪家厂商即将提供可与代理技术和无代理技术一起使用的通用的端点解决方案。

如果你坚持使用 XP/IE 环境，如果所有用户都使用管理员权限来访问系统，如果你不介意他们通过浏览器下载某种 Java 或者 ActiveX 应用程序，那么你使用其中一种第三方设备产品，或者使用 Juniper 和 Aventail 等公司提供的 VPN 解决方案，差不多就能如愿以偿。

如果微软的 NAP 远景与你的远景相一致，不妨使用 Windows ISA Server 2004 运行 VPN 隔离机制，以此获得先机。一旦 Windows ISA Server 2004 最终在明年初发布，将成为 Longhorn 代码的基础。

而如果你把所有思科路由器更新到最新版本，而且继续一律使用思科的产品，那么思科及合作伙伴的其中一款 NAC 解决方案可能适合你。

但如果上述场景不符合你的情况，你就要安排好工作，实施最佳的端点安全解决方案。与所有信息安全项目一样，最可靠的忠告就是，全面了解贵企业和业务需求。要弄清楚这些问题：

- 移动员工有哪些？他们使用哪些操作系统和安全应用软件？他们又如何连接到网络上？
- 顾问和厂商经常访问网络吗？
- 你的网络基础设施是什么？它支持哪些执行/补救机制？它是同构网络吗？它是比较新、使用最新版本的固件吗？有没有无法支持基于网络的解决方案的遗留路由器和交换机？

理清 NAC、NAP 和 TNC 需要一段时间，你要自行决定如何保护访问网络的端点。要选择这样的解决方案：至少能满足那些最关键的要求，而且与贵企业在将来的计划相一致。

原文链接：http://www.searchsecurity.com.cn/showcontent_3714.htm

*（作者：David Strom　译者：　来源：TechTarget 中国）*

# 如何选择 NAC 服务

网络访问控制（NAC）的采用正在增长——08 年上半年的 Infonetics 报告中就报告了与 07 年的第一季度相比，增长了 16%。但是即使是在巩固的市场上，为您的企业选择最好的技术也不是件简单的事情。

你必须要问：

- 你选择了在线应用吗，还是带外或者基于交换机的产品呢？
- 你采用了什么政策？
- 你需要过去 post-connect 或者 pre-connect 设备评估吗？
- NAC 对你的公司产生的利益值得在网络上配置和维护 NAC 的投入和困难吗？

Verizon 是专业的 NAC 服务，但是管理的服务是另一件事情。

Verizon 的安全解决方案市场经理 Omar Khawaja 说：“选择太多；太复杂了，太深入了，太广泛了。

思科的 NAC 应用是个例外，它可以提供管理的服务。

服务是厂商不确定的，支持大部分的领先 NAC 解决方案。根据选择的不同，Verizon 可以在采用前先开始评估和客户的配置策略。

Khawaja 说：“问题是客户甚至不知道 NAC 可以对它们特定的环境起到什么作用。他们想要把 NAC 用于客户访问、远程无线访问、非管理设备访问还是企业 LAN 访问呢？”

原文链接：http://www.searchsecurity.com.cn/showcontent_19370.htm

*（作者： Neil Roiter　　译者：Tina Guo　来源：TechTarget 中国）*

## 网络访问控制应该包括什么？

最近，对于什么是构成一个“完整的”网络访问控制解决方案的内容存在许多争议。最初的网络访问控制（如主机状态检查、隔离和补救措施）的定义一直在显著地扩大。网络架构和网络运维管理员毫无疑问都开始质疑这个词汇是否被滥用了，以至于失去了一些真正的含义。

要保证不可避免的“赶时髦”效应让厂商推出与一年前标记的东西明显不同的网络访问控制产品。尽管存在这些担心，我仍喜欢为网络访问控制提供比去年看起来更广泛的定义 。

研究公司 Current Analysis 认为，一个完整的网络访问控制解决方案应该包括下列功能：主机状态检查;隔离和补救措施；熟悉身份和基于政策的身份识别以及资源访问控制；入网后威胁保护、隔离和补救措施。

我们从这个扩展的定义中获得的东西是把网络访问控制与 IT 基础设施更紧密集成在一起的能力，从而把网络访问控制作为一个真正的普遍存在的访问控制系统。这将为当前的网络提供两个单独的、但是同样重要的增强功能，提供网络层身份管理和一个防御威胁控制台。

在网络接入解决方案中，熟悉用户身份的好处确实是显而易见的。有趣的是网络接入解决方案定位于安全解决方案是很普通的，因为它们仅与安全有关。正如以前预料的那样，网络访问控制没有增加任何额外的安全功能，而是要保证机构全面利用其现有的安全投资（例如，检查杀毒软件是否安装、打开并且更新了）。

把网络访问控制系统定位于一个系统管理、审计和遵守法规的解决方案至少是很明显的。但是，要全面利用网络访问控制作为审计和遵守法规的管理工具的潜力，这个解决方案需要把网络通讯与特定的用户和具体的政策联系起来。现有的解决方案一般采用以应用程序为中心的方法做这件事情。这个事实也许是偶然的，而不是设计上的。本星期宣布的消息称，甲骨文（以应用为中心进行身份识别管理的典范）与 Identity Engines 公司（一家熟悉身份的网络访问控制厂商）的合作将成为一种趋势。这种趋势是更迅速和更完全地向网络访问控制解决方案提供熟悉身份的技术。

要成为一个活跃的安全系统，网络访问控制解决方案需要支持入网之后的威胁保护。目前许多网络访问控制解决方案确实支持定期重新检查主机配置的入网之后的保护措施。如果发现一台设备没有遵守规则，就把它放在隔离的地方并且进行修复。然而，更强大的功能是利用网络访问控制实施点来封锁网络通讯，或者根据现有网络或基于主机的安全产品的威胁检测结果来隔离具体的设备。随着网络访问控制功能集成到网络基础设施，安全厂商将尽它们最大的努力做事。这些事情包括检测新兴的威胁，并且通过消除专用线路内的安全设备来简化网络。

我们将看到我们距离拥有这种广泛功能的网络接入解决方案还相差很远。但是，我们的第一步肯定是一致赞成朝着这个方向发展。市场需求将围绕更广泛的解决方案发展，因此，你将看到进行合作和收购的厂商以及他们提供这些解决方案的技术。

原文链接：http://www.searchsecurity.com.cn/showcontent_1165.htm

*（作者：Andrew Braunberg　译者：　来源：TechTarget 中国）*

# 网络访问控制：部署 NAC 的诀窍(上)

2003 年，由于 Blaster 蠕虫的活跃，专业安全技术人员首次开始对网络访问控制（NAC）进行关注。使用这项技术可以在网络入口处检查学生们的计算机状态，将病毒和威胁阻挡在外。作为一个我们采访过的学术性机构，谁不想在自己的网络上使用 NAC 呢？

六年后的今天，网络访问控制仍然缺少一个单一的标准，并且被证明它比第一次出现时更难实施，并且 NAC 现在如果说不是至关重要的但也仍然是一项非常有价值的安全技术。确实如此，Forrester 研究公司已经在最近的一份报告中预测，今年将是 NAC 比较轰动的一年，这个“看门狗”技术将会迅速变成网络基础设施中必不可少的一部分，它也会是促使企业安全策略倡议更加有效的组成部分。Gartner 公司的研究主管 Lawrence Orans 认为，NAC 是“一个可以添加到自己网络中的有价值的防御，”并表示，“我们给出的建议是，现在就可以实施 NAC。”

现在，这项技术已经不仅仅只是检查并隔离那些没有遵从最新的安全保护的终端设备，据 Forrester 公司分析师 Robert Whiteley 介绍。现在，很多公司都使用 NAC 来不断地检查终端的异常行为，甚至用来监测员工进入网络的角色和权限。NAC 可以检查到你从来都不知道的东西或者是被你长时间遗忘了的东西，因此，它也可以帮助你进行资产管理。

公司们正在使用 NAC 来限制访客和承包商的访问，并且为远程和无线雇员提供了便利。结果是，NAC 的部署更加容易，企业们可以选择适合自己网络和安全需求的恰当的解决方案。

供应商们还坚持表示，NAC 不只是适用于大公司。

“NAC 现在部署起来非常容易，是否要部署它取决于你要用它来做什么，而且，对于中型企业们来说，他们也没有理由拒绝使用 NAC 并从中获益，” StillSecure 公司首席战略官 Alan Shimel 说，该公司于 2004 年推出了它的 Safe Access NAC 产品。

开始部署网络访问控制（NAC）

在使用 NAC 之前，你需要先研究一下三个主要的结构：

带内（In-band，也称 in-line），用户和上行网络之间的系统在此安装，也可以说是访问交换机和核心交换机之间。

带外(out-of-band)，或者是数据通讯渠道之外的用于与 NAC 生态系统沟通的系统。

基于软件的解决方案，在终端上直接安装一个中介代理工具，能够进行自动修复。

你需要对供应商进行筛选

你应该浏览一些供应商，他们都有自己的跳跃式 NAC 产品分享。Forrester 列出了一些供应商的名单：思科系统公司（Cisco Systems）、Juniper 网络公司以及最受关注的微软公司（Microsoft）。其他的公司还有 Symantec 公司、McAfee 公司、Nevis 网络公司、Mirage 网络公司、StillSecure、TippingPoint 技术公司和 HP ProCurve 公司。Gartner 公司在 2008 年发表了一份 NAC 的市场范围。分析师们提醒说，该领域的整合已经日趋成熟。

原文链接：http://www.searchcio.com.cn/showcontent_18417.htm

*（作者： Linda Tucci 译者： 贾晋玲 来源：TechTarget 中国）*

# 网络访问控制：部署 NAC 的诀窍(下)

在部署 NAC 时，还有一些其他的因素和经验需要注意，这些都是通过对几个主要的 NAC 供应商及他们的客户进行采访之后总结出来的：

在开始部署之前，一定要纵观整个安装过程，明确想要达到的目的。

很多公司都是根据自己的网络类型、自己的实际问题和自己的安全系统来决定选择哪个 NAC 供应商。很多公司部署 NAC 来解决访客和厂商的访问问题，Whiteley 说，因此，当他们发现目前的这个供应商正好能够提供访客访问的解决方案，他们就会首先选择这个供应商。如果在将来的某个时候，他们又决定对内部员工实施基于角色的访问控制，他们会发现用于访客管理的解决方案并不是针对分部员工管理的最佳解决方案，Whiteley 说。

“我们发现，很多公司都是用非常合理的资金支出将 NAC 部署到位，并且在未来的 6 到 12 个月中，这项投资或者是废弃的，或者是需要投入更多的资金来解决问题，”他说。

相反，要采用一种业务方式实施 NAC。

首先，要确定一下需要网络访问控制的各种情况。Forrester 发现，最成功的 NAC 解决方案能够至少支持四种与业务相关的情况。

业务分析应该扩展到三个额外的领域中，TippingPoint 公司 NAC 产品管理主管 Seth Goldhammer 建议：用户身份识别、形势评估和访问执行。“在每个领域中，业务都要基于用户类型和网络领域来确定其组织的优先事项和限制事项。这将有助于今后的用于满足需求所需要的最佳技术的选定，”他说。

永远不要大规模实施 NAC 部署。

专家们的意见是一致的：不要低估了 NAC 部署的复杂性。花费六个月实施 NAC 是很正常的，但是，我们采访过的用户（全部是大学）表示他们完成一个 NAC 系统一般需要一个夏天。分析师们和供应商都建议公司们应该在三个阶段推出网络访问控制能力：监测网络内容状态、描绘网络流通情况，然后执行策略。

“把整个部署分成几个阶段，然后逐个去验证实施，” Bradford 网络公司负责营销的副总裁 Jerry Skurla 说。

Goldhammer 认为分步实施还应该包括位置和用户：会议地点、无线访问、内部和外部用户群体（访客及员工）。

重整 IT 团队。

这么说可能会有些不当。在协同部署 NAC 过程中至少应该包含 IT 部门三个领域的员工：网络、安全和计算机团队。网络团队负责确定网络如何执行这项任务及这项技术怎样在网络上运行，安全团队主要负责安全策略。当一个终端需要整合——很多 NAC 系统能自动完成这个任务——台式机团队就需要涉及近来以确保修复正确进行。

培训终端用户。

另外一个通过我们采访过的 NAC 用户和供应商而得出的经验是：最好是提前，告知用户，由于 NAC 的使用需要改变网络准入或访问，他们需要知道一些新的步骤。 （大学一般都在学生入学之前就对他们进行 NAC 流程培训。）

“如果计划得当，终端用户的培训再加上分步实施能够取得 NAC 预计的效果：减少了对帮助台的电话求助，同时还保持了最新的，规避风险的终端用户群体，” Goldhammer 说。

提醒你的网络经理：不要被 NAC 数据搞得眼花缭乱。

NAC 提供了大量的关于你的网络的数据，这些数据你之前从来都不知道。这听起来不错。但是，千万不要被这些报告整得手忙脚乱，特别是那些涉及到管理链的报告。要坚持分析状况，具体问题具体分析。

“很多管理人员，包括 CIO，都只是想知道，‘这是否会成为一个日常的威胁还是一个疯狂的威胁？’” Bradford 公司的 Skurla 说。

原文链接：http://www.searchcio.com.cn/showcontent_18447.htm

*（作者：Linda Tucci　译者：贾晋玲　来源：TechTarget 中国）*

# 控制网络访问的五个步骤

在第一部分中，我解释了处理网络消除边界的关键之处并非取消网络外围，但是不得承认，网络外围存在诸多漏洞，你必须采取措施，以保护数据的安全，防止恶意信息流通过网络外围。在第二部分中涵盖了强化 Windows 的几个步骤，此外，这里，我们将关注确保网络基础设施安全的步骤。

一个普遍存在的安全错误是将网络和应用程序视为从来都不会互相作用的不同实体。你可能会让不同的人来维护、使用不同的安全策略、不同的程序等等。在保护这些服务器上数据的完整性方面，强化 Windows 服务器会大有帮助，但是你也必须要强化网络基础设施本身。首先采取如下五个步骤。

### 1．执行访问控制列表（ACL）

如果有些人可以进入你网络的内部，那么他们就可以获得你的 Windows 系统的访问权。你需要在你的网络设备上执行严格的访问控制列表，并且只对那些需要的用户授予访问权。比如，休斯顿的用户是否需要访问纽约的系统呢？如果不需要，这些系统之间通过信息流的可能性对于业务来说并不是必要的。

### 2．执行基于网络的访问控制（NBAC）

将系统连接到网络过去常常是件麻烦事：你必须构建网络驱动程序、分配地址、并在物理上连接各个系统，进而使得它们可以对话。尽管这使得未经授权的系统要想容易地连接到网络变得极其困难，但是它却导致了过多的管理费用。然后，像星型连环状网络和动态主机配置协议（DHCP）等技术使得将系统连接到网络变得尤其简单。起初我很高兴。但现在，我意识到任何人都可以连接到网络上。实际上，我所访问过的大约 90%的客户都配备有活动的网络插孔，我很容易就可以插入，并获得网络访问权，如果他们有一些书面的策略，表明未经授权的连接是不允许的。

NBAC 旨在提供一个执行机制来支持这些书面的策略。有了 NBAC，你就可以界定什么是授权用户，并且确保所连接的系统正在运行合适的补丁和软件版本。如果没有运行合适的补丁和软件，就会将其安置在检疫状态，直到系统经过了修补和升级。

### 3．限制远程连接

执行 VPN 是一个冒险的尝试。它允许用户和病毒都可以访问网络。不要允许 VPN 访问你的整个网络，而要执行网络访问控制列表，限制仅使远程用户可以访问服务器和他们所需要的资源。比如，使用 VPN 来连接到 Citrix 或者终端服务器机房，以确保唯一允许通过 VPN 的信息流是通往 Citrix 服务器的 Citrix 信息流；如果某个远程客户的系统受到感染，它将不会感染你的网络。

**4．限制并保护无线连接**

如果在你的放火墙后面执行访问控制，无线局域网连接给你的网络外围带来了一个特别大的、敞开的漏洞。因此，创建你的无线局域网连接应当像任何其它远程连接一样：在放火墙外部终止它们，并在访问内部资源和受保护资源时，要求 VPN 连接。

**5．执行 IPsec**

在你的网络上执行 IPsec 是保护数据在传输过程中不受到威胁的一种不错的方式。但是它也并非灵丹妙药。比如，如果某个计算机受到了 Slammer 的感染，那么在信息传输之前，IPsec 仅能确保 Slammer 信息流是经过加密的。然而，当与其它强化方法一起使用时，IPsec 可以作为保护你的内部流量免于受到窥探的有效方法。

**结论**

由于网络消除了边界，你就不能再完全依靠网络外围来保护系统和数据。全部去除网络边界并不是解决方法，只强化外围也不行。你必须同时强化你的 Windows 系统和网络基础设施，网络边界不能起到保护作用，或者被规避绕开时，保护数据。

原文链接：http://www.searchsecurity.com.cn/showcontent_13549.htm

*（作者：Wes Noonan　译者：李娜娜　来源：TechTarget 中国）*

# 企业如何免费实施网络访问控制技术

很少有公司或机构像业内专家在过去几年中预测地那样大规模实施 NAC（网络访问控制技术）。预算的限制、实施的复杂性和网络访问控制好处的误解都是网络访问控制用户群增长缓慢的关键原因。

但我们应该如何定义 NAC?难道它纯粹只是一个 SSL VPN 网关，具备在设备允许进入企业网络之前保证端点策略得以执行的能力?还是一种建立在网络结构中更全面的技术?这个答案是因人而异的，因此，许多机构到目前为止还没有投资这项技术是毫不奇怪的。当 NAC 在企业中的任务和好处还不明确的时候，安全经理如何能够说明投资这个技术是合理的?在本期应用指南中，我们建议采取一些没有任何成本的方法，让你的公司试验 NAC 技术，以确定它是否能够改善企业的网络安全。

**时代的征候**

最近，厂商开始免费发布功能有限的 NAC 产品，以便提高用户数量，并解释清楚 NAC 是什么。例如，思科今年年初宣布将开放 CTA(Cisco Trust Agent)的源代码。后来思科撤销了这个决定。但是，在 2007 年 9 月，StillSecure 公司向大众推出一个免费版本的 NAC 产品：Safe Access。是否应该将 NAC 整合到公司网络中？Safe Access Lite 为公司在做这样的决定前，提供了一个使用简化安装，试验 NAC 技术的机会。同样，最近由包括 TippingPoint 和赛门铁克在内的六家领先的网络和安全厂商创建的 OpenSEA (Secure Edge Access)联盟为那些对 NAC 技术有兴趣的机构提供一种免费的 NAC 客户端软件，或者称为 802.x。

**对开源软件的呼唤**

许多机构转向开源软件网络 NAC 产品以取消商业 NAC 技术的成本。Packetfence 是一套开源 NAC 系统，由两位哈佛大学雇员开发的，提出的口号是“NAC 服务大众”。这个软件易于实施，并且具有许多思科和微软等 NAC 厂商也同样提供的功能。Packetfence 不要求使用具体厂商的设备，还包括一个名为 ZEN(Zero Effort NAC)的 VMware 虚拟设备，适用于内部没有 Linux 专业技术人员的公司。

由于适合度不一或者公司政策不同，开源也许并不是每家公司的最佳选择，但它肯定是低成本或无成本的选择方案之一，帮助公司根据自身的环境，决定这项技术是否应该必

须采用。不管长期的 NAC 计划是围绕开源，还是昂贵的商业产品发展，记住：推迟做出购买的决策是明智的。对 NAC 产品的需求预计将日益增长，需求将带动竞争，竞争将最终导致 NAC 产品的价格下调。

原文链接：http://www.searchsecurity.com.cn/showcontent_4055.htm

*（作者：Peter Giannoulis　来源：TechTarget 中国）*

## 实例:网络访问控制帮助航空公司减少安全风险

航空航天业是一个管理非常严格的行业。与政府和美国航天局合作意味着许多检查和权衡。

EADS Astrium 北美公司知道这一切。这个网络包含不能和不应该被任何人访问的敏感数据。但是其它公司的客户、承包商和访问者也要能够访问这个网络。

该公司商务管理经理 George Owoc 说，我们必须要对无权访问的人隔离这个网络中的数据。

最近，欧洲航天公司 EADS 的子公司 EADS Astrium 在一个测试环境中推出了 Lockdown 公司的“Enforcer NAC”（NAC，网络准入控制）设备。

Owoc 介绍说，这种标准的设备能够根据一套灵活的参数强制限定对网络的访问。你可以根据端口位置、安装的软件、应用程序、重要的更新和补丁等参数批准或者拒绝访问。然而，这个产品最大的优点是 Enforcer 能够根据活动目录中的身份批准或者拒绝访问。

在保密的区域，只有某些组能够根据身份进入子网。为了交换和查看那个区域的数据，访问这个区域的任何人都要获得批准。遵守认证要求的需求推动了 NAC 解决方案的产生。

Owoc 半开玩笑地说，这基本上可以使人不至于因为犯这种错误而蹲监狱。他补充说，允许任何人访问这个许可证可能会影响你未来保护这种许可证安全的能力。

其他获得批准访问这个网络的人将被放到一个单独的虚拟局域网。客人和访问者都被一起放到一个不同的虚拟局域网中。这个虚拟局域网与饭店中的网络相似。在那种网络中，你可以访问互联网，但是，不能访问其它应用程序。

Owoc 说，我们依靠虚拟局域网控制那种访问。这与思科的 NAC 在功能上非常相似。对于我们来说，这是一个一站式的解决方案。

Owoc 表示，在把 Enforcer 应用到测试环境中之前，他的公司使用过 Lockdown 公司的 Auditor。但是，那个产品不能集成活动目录。在那个时候，如果一位客户要访问的话，Owoc 必须亲自去那里批准这个访问。

Owoc 说，如果我不在那里，他们如何获得访问权限呢？现在，这种事情可以放手了。我不需要到那里监视那些人了。

Owoc 解释说，对于本地用户来说，NAC 解决方案是不可见的。只有在他们进行身份识别的时候才会启动这个解决方案。客人和访问者都被放到一个“饭店”网络。由于这是基于身份识别的，因此，用户插入哪一个端口都没有关系。这样就完全自动化了。我不必担心谁插入了哪一个端口。

使用 Enforcer 产品引起了人们对于试验 Lockdown 公司未来的产品 iNAC 的兴趣。Owoc 说，使用 iNAC 设备，不会因为设置错误或者缺少补丁或者病毒等问题封锁一个用户访问这个网络，这个系统将向这台机器发出更新程序。他说，我不用关闭这些机器，我可以强制它们进行升级。

据 Lockdown 公司称，iNAC 解决方案还可以同 Enterasys 公司的 Dragon 和 Sentinel 安全设备集成在一起，以及同 Patchlink 公司的安全设备结合在一起。Owoc 表示，一旦 EADS Astrium 北美公司获得和应用 iNAC 设备，他将把这种设备与 Patchlink 公司的产品结合在一起。

据 Lockdown 公司负责市场营销的副总裁 Dan Clark 说，Enforcer 与第三方厂商的产品结合在一起增强了一级安全并且实现了许多应用程序之间的双向通讯的自动化。

Clark 表示，在 Lockdown 计划与 Enterasys、IBM、英特尔和微软的解决方案结合在一起的同时，Patchlink 公司的这两种产品又对 NAC 系统增加了额外的检查。

当与 Patchlink 的产品结合在一起的时候，Enforcer 检查并要求 Patchlink 提供一个补丁。这个补丁将自动更新设备。在更新之后，这个设备将放回网络之中。

原文链接：http://www.searchsecurity.com.cn/showcontent_1169.htm

*（作者：Andrew R. Hickey　来源：TechTarget 中国）*

# 非盈利组织如何使用网络访问控制来保证安全？

对于非盈利性组织来说，志愿者是成功的重要因素，但对于 IT 经理和网络安全人员来说，他们在这方面也会遇到一个安全威胁，特别是当志愿者使用自己电脑访问网络时。本文将为大家介绍一个法律援助公司如何通过使用网络访问控制（NAC）来消除这个威胁。

“我们有 12 个办公点，而每个位置有时会有志愿学生使用，”Georgia Legal Services Program (GLSP) 的 IT 主管 Joseph Mays 说。“我认为需要增加一个我们原有网络之外的网络，这样当学生接入他们的电脑时，他们不会向我们的网络传播可能导致我们原来网络完全瘫痪的病毒。”

GLSP 是一个 Cisco Systems 部门，在 12 个办公点有大量的 Catalyst 3560 和 2950，所以 Mays 考虑将 Cisco 作为他 NAC 项目的一个潜在供应商。可惜，他认为使用 Cisco NAC 产品可能需要更新他的基础架构的 IOS，这是他无法实现的，因为他的大多数远程公办点都没有现场 IT 人员。作为一个非盈利性组织，GLSP 对价格很敏感。NAC 的价格是一个问题，但是实现的成本也是重要的一部分。

“实现这个需求和升级所有的交换机可能会增加我们的差旅成本以及需要派一个工程师去现场实施这个升级，”他说。

Mays 在研究了一些其它 NAC 供应商后发现了 InfoExpress 的 CyberGatekeeper 和 Dynamic Network Access Control (DNAC)。

“通过使用 CyberGatekeeper 产品，我们能够在一天内实施 NAC，”他说。“在将客户端安装到所有桌面电脑并设置为监控模式后，它能清晰地告诉我们电脑上加载了什么软件，有什么类型的应用，以及[它允许我们]看到我们的 McAfee [电脑安全]技术是否已经升级了它的桌面客户端。没有这个工具，我们就无法知道我们的桌面电脑的状况。”

选择一个独立的 NAC 供应也使 GLSP 避免过于依赖某个供应商。“通过使用这个 DNAC 产品，我们能够在任何位置部署任何一个供应商的交换机，而不需要关心它是 Cisco 还是 HP 还是其他供应商的产品，”Mays 说。“DNC 都能支持这些产品。”

他使用 NAC 控制员工和志愿者在网络中使用的这些应用。例如，AOL Instant Messenger (AIM) 在网络中是禁止的，替代的是一个内部的 IM 工具。如果一个用户打开 AIM 或某些 P2P 文件共享工具，InfoExpress 就能够隔离这些设备并提示用户点击一个修复链接。点击这个链接会关闭这个禁止的应用。

InfoExpress 实际上已经帮助 Mays 避免了可能的严重安全性问题。

“我们曾经遇到这样一个情况，有一个用户浏览一个网站，感染了一种蠕虫病毒，它试图禁用 McAfee，”他说。“DNAC 禁用了这个蠕虫并将这个用户从网络隔离以便进行修复。我们有一个脚本程序，它能够弹出窗口，提示用户‘请联系帮助台。’这个用户就会呼叫帮助台，我们就能够前往查看造成问题的原因。因为 NAC 已经将该桌面电脑从网络隔离，所以我们能够将它带到实验室，然后修复这个问题。”

原文链接：http://www.searchnetworking.com.cn/showcontent_33527.htm

*(作者：Shamus McGillicuddy　译者：曾少宁，陈柳　来源：TechTarget 中国)*