

简介	2
背景资料	2
相关发展趋势	2
网络威胁	3
网络访问控制	3
NAC 的主要目标	3
AAA 安全框架	4
ProCurve Networking 的访问控制解决方案	4
工作原理	4
架构	4
ProCurve 安全网络基础设施架构	4
ProCurve Identity Driven Manager (IDM)	5
ProCurve Network Access Controller 800	6
端点完整性测试	6
RADIUS 验证	6
多重部署模式	6
ProCurve 访问控制解决方案的优点	7
商业优势	7
为 IT 管理人员带来的收益	7
总结	7

简介

如今，技术更新的速度之快令人咋舌。计算机网络的飞速发展明显改变了个人及组织交流和访问信息的方式。网络成为许多组织的重要资源，组织之间可以通过互联网和企业内部网进行实时交流，同时访问海量信息。此外，由于数据保密法规和保护有价值信息资产的要求，需要对企业内部网络上的许多数据进行保护。同时，为客户提供可靠、安全的网络访问已成为信息技术(IT)企业需要应对的重要挑战。

现在，人们已经习惯于“连接网络”——他们需要随时快速、轻松地访问信息。除公开信息外，企业内部网上的敏感信息也越来越多，工作效率也在随时随地的信息访问中得到大幅提高，而且所有连接网络的人员均可以相互访问。电子邮件、即时信息、互联网电话的广泛应用，使“连接网络”的人员可以随时随地进行交流。

当组织从便利的信息访问中获得众多优势时，也必须考虑其安全问题：必需保护有价值的专有信息，可能还要符合相关政府数据保密法规的要求，使得许多IT组织都为达到两个业务目标的最高要求而竭尽全力：数据可用性和数据安全性。我们可以直接实现任何一个目标，但这两个目标的实现方法相互冲突，不过组织在必须同时实现这两个目标。

全面的网络安全实施需要涉及许多方面。本白皮书介绍了网络访问控制(NAC)的概念，帮助组织控制网络访问和这些网络上可用的信息。另外，本文还介绍了ProCurve networking by HP提供的访问控制解决方案。ProCurve Networking致力于提供网络解决方案，使组织能够提高生产率、增强安全性、降低复杂性。

背景资料

相关发展趋势

安全性是企业IT组织一直讨论的话题。在过去十年中，控制企业网络访问的需求不断增长，这可能与网络业和业务流程的发展趋势有很大关联。

无线网络——无线网络出现之前，许多企业都依靠物理访问方式增强网络安全性；通过网络连接的位置根据需保持物理安全性。但是，他们无法划定无线网络的边界，因此可能会无意中超越组织的保护范围。网络和安全专家可快速确定控制无线连接访问的需求。他们认识到有线网络之间存在许多相同的安全问题，因此需要使用适宜的解决方案控制所有的网络访问。

移动办公员工——由于膝上型电脑的使用较台式机更为广泛，因此员工可以在企业内外的不同位置连接企业网络。当员工携带膝上型电脑来往于公共办公室或办公室到会议室之间时，不同的用户和设备会通过相同的物理网络连接与网络相连。当系统连接了一个网络端口并被固定后，安全性便可以静态应用于该网络端口。但是，因为一个端口必需支持多个不同的用户和设备，所以必需使访问和安全级别适用于这些用户(例如研发、市场营销和财务)及其设备(例如膝上型电脑、PDA和VoIP电话)。

此外，与受保护的企业外部网络相连的移动设备，会增加感染病毒或其它恶意软件的可能性。当用户携带设备返回办公室并再次进行连接时，威胁会在不知不觉中转移到企业。

共享网络访问——越来越多不同职务的人员需要共享网络。例如，许多组织需要定期与承包商、合作伙伴和供应商合作。因此通常需要为这些外部员工提供某些级别的网络访问，同时保持内部数据和资产的安全性。另外，作为优势或服务的互联网来宾访问也几乎成为站点访问者的期望。

恶意软件——攻击次数的不断增加，以及这些攻击导致的成本增加要求避免网络及其资源受到有害设备的攻击。

政府法规——现在的许多组织需要遵守越来越多的政府法规要求，例如《萨班斯-奥克斯利法案》(SOX)和《健康保险流通与责任法案》(HIPPA)。这些法规通常需要组织建立并实施有关网络安全和数据保护的策略。

网络威胁

网络攻击不断威胁着网络资产。根据《2006年美国CSI/FBI计算机安全调查》，企业、政府机构、财务机构、医疗机构和大学中的大多数组织去年都曾遭遇过计算机安全事故。而且，这些攻击变得越来越诡异和危险。最初，进行网络攻击只是个人为了展示他们掌握新技术的能力。而现在，网络攻击通常是经过周密计划的，有时甚至有内部人员的协助，而且目的多是为了获取经济利益。

传统的网络安全主要是针对网络周边而进行的，目的是防御外部威胁。因此，一些优秀的解决方案主要以防火墙、VPN设备、IDS/IPS系统和UTM为基础，来防御这些威胁。不过，防御企业网络内部威胁的要求也在不断增长。这些内部威胁主要来自恶意用户或有害的设备，是网络访问控制的重点。

网络访问控制

现在，保护网络和网络上的资源是IT组织最重要的任务之一。NAC已经迅速成为网络安全的中中之重，但也是网络安全中定义最模糊的概念之一。网络访问控制可能只是“控制计算机网络和网络资源访问的过程”。这个广泛的定义和人们增强的网络安全意识，使厂商有机会利用NAC销售各种网络安全产品和解决方案，导致人们对NAC解决方案实际功能认知上的混乱。

NAC的目标是避免网络及其资源受到恶意用户和系统的威胁，并根据某些标准和业务策略来限制网络访问，以实现该目标。这些策略可能非常简单，例如允许一组已知用户或设备访问网络，但拒绝所有其它用户或设备的访问；也可能更加复杂，以满足更多复杂业务策略的需求。通常，大多数NAC解决方案可以实现下列一个或多个目标：

NAC的主要目标

限制用户访问 — 其最基本的方式，是限制已授权用户和/或设备访问网络。但是，许多组织需要根据用户的角色提供不同的访问级别，或者要从提供的访问中受益。例如，员工可以访问内部网络资源和互联网，同时来宾用户只能访问外部互联网。

防御恶意软件 — 这需要评价网络连接设备的安全状态。必需的安全状态可根据组织策略作出，并经常对操作系统版本和补丁、安全软件(防病毒、防垃圾邮件、防火墙等)、常用软件安全设置和其他必需或禁止的软件进行检查。

遵循法规文档 — 随着越来越多政府法规的出台，组织需要实施网络数据保密策略计划。另外，他们还需要使用有关策略和策略执行方法的文档。

AAA安全框架

被沿用了很长时间的验证、授权和帐目结算(AAA)框架，充分说明了计算机资源访问控制使用的管理步骤。全面的NAC解决方案包括每一层的各个方面。

验证：验证指确定请求访问的用户(或设备)的身份和验证用户证书的过程。证书可能是简单的用户名/密码对和强大的双因素验证方案等。验证过程将用验证数据库中存储的证书评价通过验证的证书。

授权：授权指将验证的用户与相应的网络访问权限相匹配的过程。这些访问权限可能只是简单地允许或拒绝访问网络。但是，它也可能提供许多网络访问权限，定义用户可访问的大量网络资源。

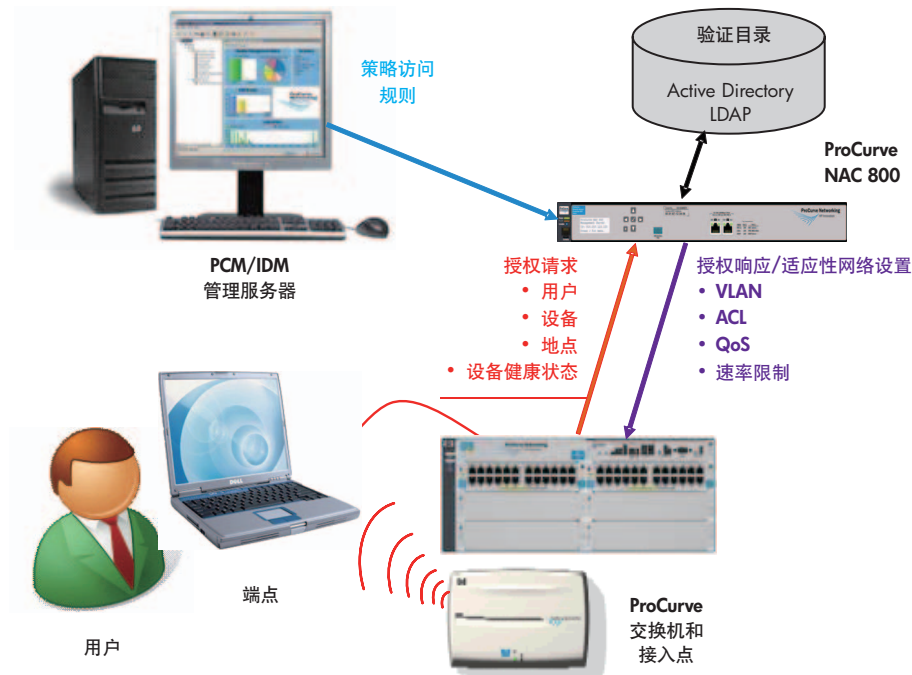
帐目结算：帐目结算指记录网络访问的过程。这通常包括所有认证请求和最终授权的完整列表，可以用于记录网络安全策略和执行的大量数据，以及调查违反网络法规的潜在行为。

ProCurve Networking 的访问控制解决方案

ProCurve 访问控制解决方案以 ProCurve 适应性边缘架构和 ProCurve “中心命令” 管理方法为基础。该解决方案使用的 ProCurve 网络设备可将智能推向用户和设备连接的网络边缘。ProCurve 的 Identity Driven Manager (IDM) 产品是一个网络访问策略服务器，可以使网络端口动态满足所连接的用户和设备的需求。ProCurve Network Access Controller 800 支持简化的验证服务部署和端点完整性策略验证。另外，这些产品可组成可增强网络安全的全面访问控制解决方案。

工作原理

架构



ProCurve 安全网络基础设施架构

ProCurve 网络设备(交换机和接入点)的一系列安全技术可满足企业网络的多种需求。这些技术适用于有线和无线网络设备，为企业网络提供统一的安全和访问控制解决方案。与访问控制相关的特性：

灵活的端口安全性：控制网络访问的最有效方法是在用户和设备访问网络之前对他们进行验证。ProCurve 设备可通过标准的 802.1X 验证提供该功能。此外，许多 ProCurve 设备还拥有两个备用的验证方式：强制页面 web 验证(Web-验证)和基于 MAC 的验证(MAC-验证)，均支持预先验证功能。这些多重验证模式可高效实施网络访问控制，提供满足企业网络综合需求的灵活性。

每个端口的多重验证类型：ProCurve 设备经过配置后，可以支持在一个端口上的同时多重验证，允许同一端口自动验证使用 802.1X 的员工 PC，稍后通过 Web-验证上的强制页面功能验证来宾的 PC 上是否配置了 802.1X。这可为常规网络用户提供简单的访问，以及验证来宾的灵活性，无需使用客户端软件即可完成。

每个端口的多重验证：此外，某些 ProCurve 设备能够在端口上验证多个会话，支持多个下游设备安全地连接单一安全端口。这在计算机连接 VoIP 电话并且计算机和电话共享同一网络端口时非常重要。

适应性网络配置：除了验证用户和设备外，ProCurve网络设备还可以帮助您为不同级别的网络访问进行授权。这些网络设备对应ProCurve Identity Driven Manager中定义的设置，可定制基于业务策略的网络访问。这些设置以用户为基础，并且可以根据VLAN或特定的访问控制列表定义允许或拒绝用户访问的网络资源。访问也可以执行网络性能设置。这样的定制使访问可以优先排列VoIP设备，极大地提高了呼叫质量，消除了丢失的可能性，或遏制来宾用户流量，从而不会对性能产生负面影响。

ProCurve Identity Driven Manager (IDM)

IDM可通过在集中管理的服务器中定义安全和管理策略，自动配置网络边缘，帮助公司最大程度提高网络的安全性和生产效率。IDM 解决方案允许网络管理员根据用户、设备、位置、时间及其它因素动态应用安全和性能设置到网络基础设施架构设备。最终建立起统一的管理基础设施架构，以及更安全、移动和融合的网络。

IDM是ProCurve Manager Plus平台的插件模块，为定义网络访问权限和监测网络访问提供了集中的策略管理界面。IDM集成了标准的RADIUS验证服务和用户目录(LDAP和Active Directory)，可验证连接网络的用户和/或设备，然后在基本验证的基础上添加一套丰富的授权功能。

IDM利用中心功能的ProCurve命令动态实现边缘端口配置的自动化，并为每个网络连接提供独特、适当的网络访问。将控制推向网络边缘，在更靠近端点的地方实施安全和性能设置，以增强实施效果。

IDM可简化并组织网络访问策略。虽然这样可以为每个用户确定独特的访问权限，但不现实，也不能与业务策略相适应。通常，组织内有极少的团体需要使用独特的网络访问策略。

IDM定义了可共享常用网络访问权限的用户团体。通常，这些团体由部门(例如市场营销部)、职务(例如采购)定义。每个团体都有独特的规则，可以根据业务策略告知用户连接网络时获得的访问权限级别。

这些规则以常用业务概念为基础。IDM可以根据下列信息提供独特的访问：

- 用户是谁？
- 该用户属于哪个团体？
- 用户的设备(PC、膝上型电脑、PDA等)是否运行的是企业要求的软件？
- 用户在哪里(交换机/端口)？
- 时间？

反过来，IDM将确定相应的网络访问权限级别：

- 允许/拒绝该团体使用资源
- 为该团体分配了性能属性

有些人认为，网络边缘智能化非常复杂，IT企业难以管理。他们认为，在网络边缘可能有数千个端口和更多用户，因此相对于网络核心交换机来说，更难于实施和使管理智能化。

但是，如果实现配置和所需智能行为的自动化、降低复杂性，网络管理将变得更简单，也可以增强用户体验。

这种方法与传统策略有很大的不同：配置后的特定交换机和特定端口以特定的方式运行。该新方法使任一交换机和端口都能为每个人提供独特的功能。不管用户在什么地方或如何连接，该方法都能为用户提供相同的网络功能、资源和视图。

这是智能、适应性网络和IDM的要素。网络的行为不再统一；相反，它能相应满足每个用户的需求。

ProCurve Network Access Controller 800

ProCurve Network Access Controller 800 (ProCurve NAC 800)利用ProCurve访问控制解决方案在访问企业网络之前评价端点的完整性。此外，它具有RADIUS验证功能，可与ProCurve中心命令管理平台相集成。

端点完整性测试

ProCurve NAC 800的主要作用是评价端点连接网络时的健康状态。验证端点连接网络之前的健康状态可拒绝受感染或有害系统的访问，也可以将其隔离，使其不会攻击其它网络系统，从而降低网络系统停机，节约成本。此外，当端点与网络连接时对其进行测试，以及持续的验证后健康状态检查。

端点完整性测试可用于确定端点的整体安全性状态。评价端点时，不仅要确定系统当前的健康状态，还要评价端点保持健康状态的能力。ProCurve NAC 800为评价系统的当前健康状态和相应的配置提供全套的测试，以避免受到其它系统的攻击。这些测试可检查：

- **操作系统：**服务包、热修复、自动更新设置
- **安全软件：**防病毒、防间谍软件、防火墙、对等应用程序、允许和禁止的程序和服务
- **安全设置：**适用于浏览器和应用程序
- **必需和禁止的软件：**可由管理员定制
- **恶意软件：**检查某些常见间谍软件、蠕虫、病毒和木马

RADIUS 验证

ProCurve NAC 800装置也提供基于RADIUS的验证服务，实现安全的网络访问。RADIUS是基于标准的验证服务，几乎是使用网络基础设施架构实施的所有NAC解决方案的基础。该验证服务可以与IDM配合使用，提供网络设备的适应性网络访问权限。

多重部署模式

ProCurve NAC 800拥有可满足企业网络需求的多重部署模式。所有实施方式都利用预先授权安全策略检查，以保护网络不受有害系统威胁。这些实施模式可以一同为整个网络提供全面的访问控制覆盖。

802.1X 执行：使用ProCurve网络设备中的802.1X功能 — 最有效、最高效的执行方法之一，建议在支持802.1X验证的设备环境中使用。利用RADIUS验证的用户和设备。端点已隔离，因此可以进行安全策略测试。然后连接网络，或者放入修复网络，使用户可以解决导致隔离的安全设置问题。

In-line 执行：在此模式下，ProCurve NAC 800可以设置网络流量经过它，并且积极过滤新的连接并对其进行测试，确保其符合安全策略的要求。这是一款测试端点的高效解决方案，可通过VPN连接器远程连接。

DHCP 执行：ProCurve NAC 800与企业DHCP服务器相集成，可在端点请求网络地址时隔离这些端点。端点已通过网络地址隔离，因此可对其进行安全策略测试。如果符合策略要求，会为这些端点提供一个新的网络地址并允许其加入网络。如果不符合策略要求，可以放入修正网络，帮助用户解决导致隔离的安全设置。此方法对于802.1X验证不可用的环境很有用，因为网络基础设施架构不为其提供支持。

ProCurve 访问控制解决方案的优点

如今，企业纷纷大力提高网络的生产率、可靠性及安全性，在让适当人员轻松获得所需信息的同时，创建安全策略，阻止无访问权限的人员获得这些信息。而且，现在许多企业都需要记录安全策略，显示其实施方式。这些要在不对现有网络基础设施架构进行不断升级的前提下予以完成。ProCurve 访问控制解决方案可满足您的以下需求，是IT组织的得力助手。

商业优势

业务需求	ProCurve 访问控制解决方案
提高网络生产率	控制网络访问，只为验证的用户和设备提供相应的访问权限(基于策略)
更出色的网络可靠性	及时隔离受感染或有害的系统，以防止其连接网络并感染其它系统
标准符合性帮助	提供网络访问安全策略报告，以及所有允许和拒绝网络访问的详细日志
投资保护	利用内置 ProCurve 交换技术执行经验证的网络访问，并提供安全的授权资源访问

为IT管理人员带来的收益

IT需求	ProCurve 访问控制解决方案
避免未经授权用户和设备访问网络	提供方便易用、基于策略的网络访问控制，该访问控制集成了标准 RADIUS 验证服务和用户验证目录
端点完整性验证	在允许端点进入企业网络之前进行端点预授权测试，然后进行后期授权测试，确保这些端点的安全
网络威胁和使用信息	记录和报告所有网络访问，包括在网络上的时间、发送/接收的网络数据、安全状态结果、提供的网络访问权限和失败的登录尝试。

总结

ProCurve 访问控制解决方案是 ProCurve 主动防御安全策略的重要元素，用于建立可信的网络基础设施架构。它可以与包括 ProCurve Network Immunity Manager 的 ProCurve 网络抗干扰解决方案配合使用，加强连接用户的网络边缘的安全。ProCurve 访问控制可形成初始网络安全层，在允许用户和设备访问网络之前对其进行验证，并继续验证连接设备的健康状态和安全状态。

ProCurve 访问控制解决方案通过下列方式提供超值价值：

- 提高网络生产率
- 大幅提高网络可用性
- 最大化 ProCurve 交换机的当前投资
- 根据用户和业务策略确保数据访问的安全
- 为局域网、无线局域网和远程访问用户提供统一的访问控制解决方案

通过 ProCurve 中心管理命令提供可轻松部署和管理的访问控制解决方案，以及全面的访问控制功能。

欲了解有关 ProCurve
Networking 产品和解决方案
的更多信息，请访问网站：

www.hp.com.cn/network



© Hewlett-Packard Development Company, L.P. 2007 年版权所有。本文信息如有更改，恕不另行通知。惠普产品与服务的全部保修内容在此类产品和服务附带的保修单中明确说明。本文所含信息不得视为额外的保修承诺。惠普对本文中所包含的技术、编辑错误或遗漏恕不负责。

Itanium 是 Intel Corporation 或其子公司在美国和其他国家/地区的商标或注册商标。

P/N: 5982-9129CHP, 2007 年 9 月中国印刷