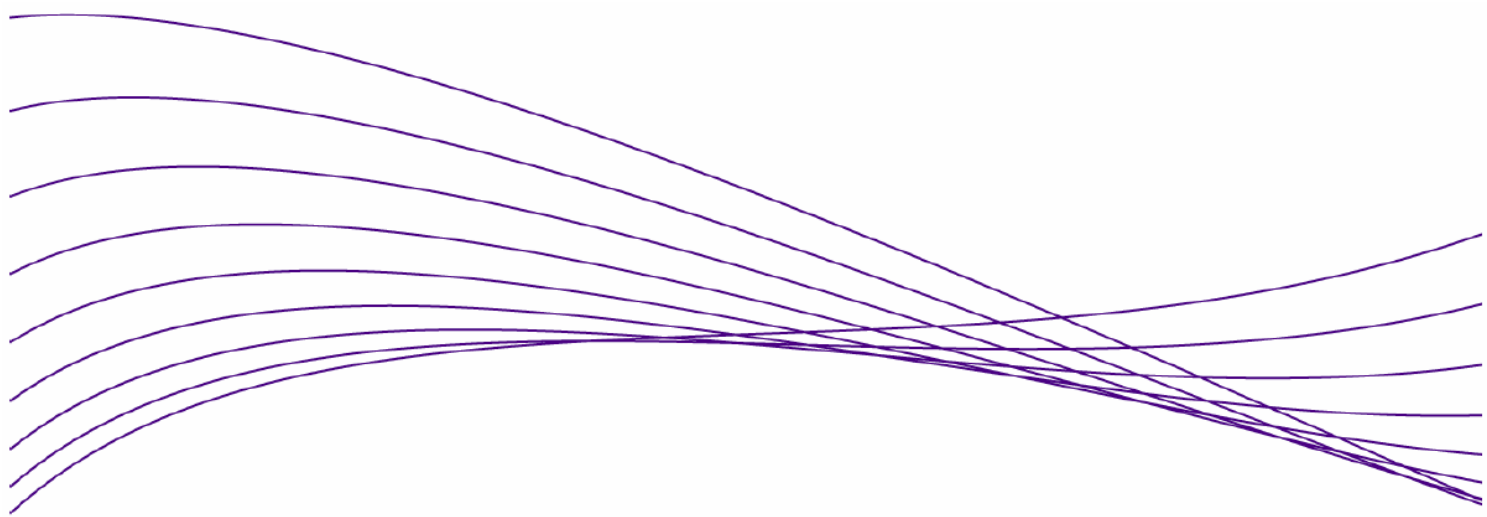


ProCurve 主动防御：全面的网络安全战略



简介.....	2
网络安全对公司的影响.....	2
重要的安全方案.....	3
什么是网络安全?	3
安全是流程，而不是产品.....	3
ProCurve 适应性边缘架构.....	4
AEA 是 ProCurve 安全战略的基础.....	4
ProCurve 主动防御.....	5
进攻与防御并驾齐驱.....	5
进攻.....	6
防御.....	6
ProCurve 如何实施主动防御.....	6
主动：访问控制和智能边缘.....	6
防御：网络免疫和中心命令.....	7
网络安全的未来.....	8
最终建议.....	8
更多信息.....	8

简介

安全问题永远存在。

越来越多的网络正在经受着比以前更隐蔽、且不断更新的攻击和威胁，包括病毒、蠕虫、木马和内部破坏等。

根据对美国企业、政府机构、金融机构、医疗机构和大学进行的《2006 年 CSI/FBI 计算机犯罪及安全调查》，大多数组织都在 2005 年经历过计算机安全事件。在这些发生过安全事件的组织中，该年有近四分之一的机构遭遇了 6 次或更多次的网络攻击。

信息技术 (IT) 行业的不断发展，让确保网络安全变得越发重要，同时也越来越难以实施。主要原因包括：

- 互联网的出现让人们可以获得更多信息，而且组织需要确保资源可以安全地用于更多用户；
- 需要移动工作的人员越来越多，而且人们想要随时随地连接网络；以及
- 在单一网络上运行语音、视频和数据，以提高工作效率、简化运营多个网络的繁杂工作并降低成本。

移动的重要性不断增加，例如：1999 年，五分之一的 PC 为移动设备；2005 年，移动 PC 占到了三分之一。在未来几年，笔记本电脑的数量将超过台式机。尽管无线网络和协作通信为各地用户带来了福音，但同时也为网络设计和网络管理人员带来了巨大的安全挑战：员工会携带移动设备离开办公室，并在可能有害的环境中使用这些设备。移动设备可能会在这些环境中感染病毒，当返回办公室后，又将病毒带入关键任务企业。如今，越来越多的人在个人和业务应用中使用同一移动设备，这增加了设备的安全性危险。

网络安全对公司的影响

安全性成本日益增加，但是如果未能有效确保网络安全，所损失的成本也在不断攀升。

2006 年 CSI/FBI 调查显示，2005 年网络安全事件所导致的损失总计约 5250 万美元。近 35% 的受访组织将其 5% 以上的 IT 预算用于确保网络安全。几乎所有组织都部署了防火墙和杀毒软件，而且大多数组织还购买了其它安全产品。

但不幸的是，他们仅注重防御来自外部的威胁和风险，而忽略了源于组织内部的大量网络攻击。

除实际攻击之外，萨班斯—奥克斯利法案 (Sarbanes-Oxley)、HIPPA、GLBA、FISMA、PCI 和 NERC 等必须遵守的法规规定，也为这些组织带来了巨大负担和巨额开支。公司必须遵守法规制定机构及内部规定的各项安全性要求。对许多组织来说，法规遵从已成为首要的安全问题。

一般来说，控制网络安全意味着公司必须：

- 控制网络访问，加强网络的适当使用；
- 消除病毒/蠕虫及不必要的网络流量；
- 了解内部和外部威胁；
- 弄清大量可用的安全智能手段，并将其转化为可执行的条目；以及
- 了解并向内部审计人员、政府机构和供应链合作伙伴阐述法规并遵从规定。

为确保公司能够实现这些目标，安全解决方案必须：

- 以可信的网络架构和合理的战略为基础，消除企业风险，并让企业重新获得网络的控制权；
- 易于部署和使用；以及
- 基于标准、可互操作、安全可靠。

重要的安全方案

传统的核心网络架构根本无法应对当今越来越频繁的潜在破坏性攻击和挑战。这些网络缺乏必要的可扩展性和动态功能，难以满足当前网络安全需求或快速变化的业务和技术要求。

本文为您提供了一个出色的网络安全替代方案：直接来自 ProCurve 适应性边缘架构™ (AEA) 的全面安全性愿景和战略 — 提供网络边缘分布式智能，并采用整体网络连接方案。全新的安全性远景，即 ProCurve 主动防御，可以在用户连接的网络边缘，将主动安全防御技巧与坚固的传统安全防御技术结合使用。而且，ProCurve 主动防御还可以显著改变网络安全的部署方式。

什么是网络安全？

要实现网络安全，先要了解安全网络的特征和所需条件。

人们通常认为网络安全就是防御蠕虫或病毒、阻止未经授权用户访问网络、或者保护网络信息和资源隐私。事实上，网络安全远不止这些。

一些网络厂商采取的安全方案仅注重使用防火墙、虚拟专用网 (VPN)、入侵检测系统 (IDS) 和入侵预防系统 (IPS)，防御外部威胁。然而，这种仅注重周边环境的方案无法应对来自组织内部的威胁，而且还会为企业引入成本高昂、操作复杂的管理架构。

其他网络厂商则将注意力集中于远离网络边缘的核心交换机或核心路由器。集中运行可能便于管理，但距离攻击“发生”地点点和被攻击的网络资源明显较远。这就好比是只在大楼中心、而不是在入口处设置警卫室。当警卫发现问题时，为时已晚。

ProCurve 采取了截然不同、却更为有效的方案。通过将重要的访问和策略执行决定移至连接用户和应用程序的网络边缘，ProCurve 主动防御可释放核心资源，提供所需的高带宽互连功能。这样，不仅可以加强网络安全，而且还可以获得运行更出色、扩展性更高的网络。

安全是流程，而不是产品

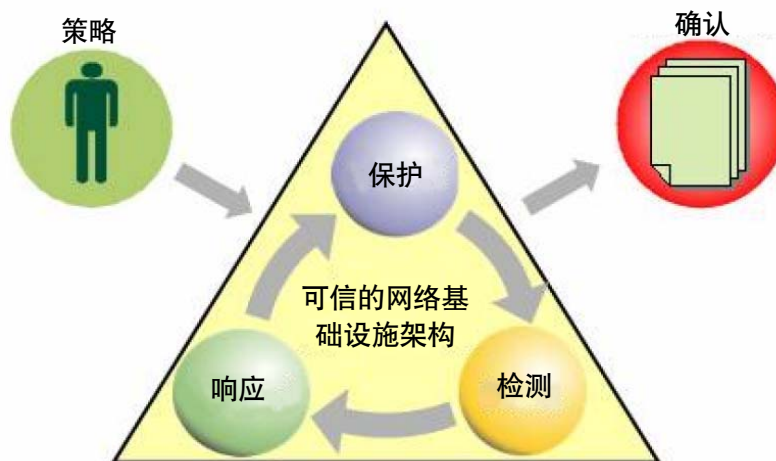
目前有许多关于网络安全的荒诞说法，包括：存在单一的简缩性的网络安全“解决方案”，以及可以一揽子地“实现”网络安全，并可以从此高枕无忧了。

不幸的是，目前许多厂商提供的网络范例更多的是支持、而不是抵消这些概念。尽管竭尽全力提供网络安全“解决方案”，但大多数网络厂商提出的“固定式”方案无法降低网络安全管理的复杂性。

切勿相信有关安全性的种种谬论，要明确有效的网络安全是一个流程，而非产品或最新补丁程序，网络安全的动态特性说明网络需要自动确保安全，从而使该网络可以自行对威胁做出反应，并抵制这些威胁。

而只有使用可信的网络基础设施架构，才能实现此类自动操作。也就是说，网络安全流程必须以网络架构为起点 — 同时该网络架构必须使用值得信赖的技术。

实际安全性流程



如上所述，配置了可以从“中心命令”网络边缘设备的管理工具的 ProCurve 安全架构，可用于：

- 在漏洞出现之前，防止安全漏洞并保护网络；阻止未经授权用户访问或侦听网络；防止在未经授权情况下在网络上部署主机和应用程序。
- 自动检测外部和内部安全性威胁；在安全漏洞发生期间检测攻击。
- 自动、适当地响应安全漏洞；关联网络威胁事件并进行动态响应，以减少攻击事件的发生。

ProCurve 适应性边缘架构

ProCurve Networking 适应性边缘架构 (AEA) 明显不同于普遍流行的网络范式，该范式使得企业网络在采用和管理上滞后或各自独立的“网中网”。与之相反，AEA 具有整体性的、全面的网络理念，可将智能特性分布到连接用户的边缘。

AEA 的主要原则是“边缘控制”及“中心命令”。由于将智能（即：网络的响应和反应能力）嵌入了连接用户和资源的网络边缘，因此可轻松实现这两大原则。同时，网络管理员可以方便地使用网络智能管理策略和原则。

来自管理中心（中心命令）的动态边缘配置（边缘控制）可实现自动功能和网络安全。这对于降低成本和网络复杂性至关重要。

AEA 是 ProCurve 安全战略的基础

AEA 的整体性和分布式智能特性促使 ProCurve 提出了与以往不同的安全性愿景和战略。重要的是，AEA 构建了安全自动化所需的可信网络基础设施架构。

AEA 的网络边缘控制说明在用户连接点即可自动制定安全性决策。该方案可直接提高工作效率、降低复杂性，并增强网络和安全管理的灵活性。

AEA 的 *中心命令* — 可以通过 ProCurve 管理工具设定安全策略，并报告警报和网络安全信息，并根据个人用户级策略，提供统一的重要网络资源访问。因此，组织可以更有效地保护安全数据，同时确保授权用户可以访问所需的网络资源，以大幅提高生产率。

重要的是，AEA 是基于行业标准构建而成的。ProCurve 不仅支持其产品标准，而且还创建和采用了网络行业标准。

因此，ProCurve 既可以确保其产品与第三方解决方案的互操作性，又可以为使用这些产品的公司提供长期的选择和灵活性。借助基于标准的安全性，公司无需考虑专有方案是否可与其它设备配合使用，即使一年或五年内出台各种条款，也可轻松应对。

ProCurve 主动防御

综合的 ProCurve 安全性理念和安全性战略 — ProCurve 主动防御，可为您提供可信的网络基础设施架构，以阻止多种威胁的侵入，并对访问加以适当控制，保护所有用户的数据完整。

主动防御战略的三大支柱包括：

访问控制：通过控制用户访问的系统以及这些用户连接有线和无线网络的方式，主动预防安全漏洞。

网络免疫：检测并响应内部网络威胁，例如病毒和蠕虫攻击；监控行为，并应用安全信息智能协助网络管理员维持高网络可用性级别。

安全的基础设施架构：确保网络实现从未授权扩展或攻击到控制面板的策略自动化；包括保护网络组件，防止未经授权经理跨越规定的安全性配置，以及可以确保敏感数据完整性和机密性的保密措施；防止篡改数据，预防数据侦听、提供端到端 VPN 远程访问支持或站点到站点保密以及无线数据保密。

安全解决方案架构



总之，访问控制、网络免疫和安全的基础设施架构这三大支柱可共同保护网络，同时确保公司可实现法规遵从和其它要求。

进攻与防御并驾齐驱

ProCurve 主动防御愿景和战略的独特之处在于，它可以同时执行安全进攻与安全防御，而且更重要的是，该策略在网络边缘即可实现。主动防御以我们的适应性边缘架构为基础，既可将智能推向网络边缘，又可保持中心控制和管理，以确保进攻与防御的同时执行。

进攻

主动（进攻）策略主要针对的是访问控制，它可以全面管理网络访问、处理多种用户类型：例如未受控制的用户、经验证的用户和完全可信的用户。

如今，很多设备都需要与网络相连，例如笔记本电脑、IP 电话、外设、PDA、各类无线设备和传统的台式机。IT 部门基本上不可能为所有访问网络的设备指定具体的运行环境。因此，采用能够识别所有用户和设备类型、并可以对其访问进行有效控制的主动访问控制解决方案就显得非常重要。该访问控制解决方案必须能够主动验证所有用户和设备的完整性和运行状态。

防御

ProCurve 主动防御策略以可靠、可自行识别和全面验证的可信网络基础设施架构为起点。

同时，基础设施架构必须可即插即用且易于管理。如果它过于复杂而无法实施，或者会降低总体系统性能，那么安全性就没什么用处。为此，ProCurve 为可信的网络基础设施架构配备了内置威胁管理和异常检测功能。这些功能均为嵌入式特性，可促进可信网络基础设施架构的防御安全性。

ProCurve 如何实施主动防御

因为深知网络安全是一项流程，而不是分散的解决方案，并需要从网络基础设施架构提供全部安全，所以 ProCurve 在其整个网络基础设施架构和产品中部署了安全功能。

下文将向您说明 ProCurve 是如何实施主动防御战略的：

- ProCurve 在其交换机、接入点及其它硬件中内置了防御安全特性，同时创建可信的网络环境。
- ProCurve 设计的网络处理器芯片，即第四代 ProVision™ ASIC，将策略执行功能嵌入了适应性边缘架构。我们将 ProVision ASIC 内置于全新的 ProCurve Switch 5400/3500 系列产品中，并计划将其用于未来产品。
- 通过 ProCurve Manager (PCM) 网络管理软件和 ProCurve Network Immunity Manager (NIM) 提供集成的安全性和性能管理，让您可以在大范围自动实施网络安全，并消除安全管理的复杂性。
- 网络边缘智能分布可以为有效的主动访问控制提供支持，该特性可通过 ProCurve Identity Driven Manager (IDM) 2.0 (ProCurve Manager Plus (PCM+) 软件模块) 实现。IDM 允许组织定义网络访问策略，以便加强网络访问的安全性，并为用户连接的网络端口提供动态安全性和性能配置。IDM 让网络管理员可以根据用户或设备身份、位置、时间和端点完整性，主动控制网络访问。
- 病毒遏制技术和异常检测可作为嵌入式威胁防御功能提供。

主动：访问控制和智能边缘

ProCurve 高级访问控制功能的推出，让企业的主动防御战略得以较早实现。其实大约十年前，该功能就已根植于 ProCurve 的重要行业标准活动计划之中 — 即 IEEE 802.1X 基于端口的网络访问控制标准。

此后，ProCurve 不断增加并改进其访问控制产品，通过其 IDM 2.0 软件模块大幅提高了全面访问控制的能力。重要的是，IDM 2.0 等 ProCurve 基于用户的访问控制方案还具备 *使用功能*：一旦用户获准访问网络，IDM 就会确定他们可访问哪些资源、在何处登录网络以及在网络中移动时会经过哪些边界。

网络管理员可以利用 IDM 制定性能和安全性管理策略。另外，IDM 可帮助报告法规遵从规定。为了实现安全访问（包括安全的无线访问），我们设计了大量的 ProCurve 产品。ProCurve Secure Access 700wl 系列，可提供顺畅的安全漫游和持续会话、集中安全配置和策略管理、自动用户身份验证以及固定和移动用户访问权限。其灵活的身份验证模式配有基于 Web 的可定制身份验证屏幕，能够验证未受控制的客户端身份（即无明确身份验证代理的端点），可实现来宾访问和出色的整体身份验证控制。

同样，ProCurve Switch xl 访问控制器模块 (ACM)，即 ProCurve Switch 5300xl 系列的一个板卡，可为您提供独特的方法，以集成基于身份的用户访问控制、无线数据保密、安全漫游以及全功能智能边缘交换机灵活性。

为有效控制网络边缘策略，ProCurve 产品采用了基于标准的 IPsec VPN 安全性，以及使用 802.1X 的有线和无线身份验证、基于 Web 的身份验证和介质访问控制 (MAC) 身份验证。

对 ProCurve 主动防御的主动领域至关重要的行业标准包括：

- IEEE 802.1X (ProCurve 发起的一项端口身份验证协议，而且 ProCurve 还是该协议的重要技术捐助商)。
- Trusted Computing Group 的 TNC (可信网络连接) (最终设备法规遵从授权；ProCurve 发起此项标准，并作为临时负责人编辑 IF-PEP 协议)。
- IETF RADIUS 扩展 (ProCurve 是这类协议的互联网起草者和技术顾问)。
- IETF NEA¹ (网络端点评估)；ProCurve 目前支持 TCG/TNC 规范并为该标准做出了贡献)。
- 另外，ProCurve 的访问控制解决方案还可以兼容 Microsoft NAP 架构。

防御：网络免疫和中心命令

ProCurve Manager (PCM) 管理软件为网络安全的全面管理（包括基于策略的高级设备和流量管理）提供了一个较完善的平台。重要的是，作为适应性边缘架构综合框架的组成部分，PCM 可简化并增强网络管理的有效性。

ProCurve 主动防御还具备嵌入式病毒检测和响应功能，包括：

- Virus Throttle 软件 — 一种 ProVision ASIC 内嵌算法，可快速检测并隔离病毒或蠕虫，防止其继续蔓延，并阻止其对网络产生危害。
- ICMP 遏制 — 让所有交换机端口均自动限制互联网控制消息协议 (ICMP) 流量，以解除拒绝服务攻击。
- 控制协议检测 — 该软件可阻止地址解析协议 (ARP) 侦听、恶意动态主机配置协议 (DHCP) 服务器和生成树根保护。
- 设备身份验证 — 允许 ProCurve 交换机和接入点使用 802.1X 相互验证，进而构建可信的基础设施架构。
- Network Immunity Manager — 一款安全性管理工具，可监控有线和无线网络的内部网络威胁，让管理员可以针对威胁检测和响应制定安全策略。

IEEE 802.1AE-2006 (MAC 安全性和以太网加密)、IEEE 802.1af (加密密钥协商协议) 和 IEEE 802.1AR (安全的设备身份) 等行业标准，对 ProCurve 主动防御的防御领域来说非常重要，而且每项标准都由 ProCurve 投票选出，并获得了 ProCurve 的大力支持。

¹工作组正等待审批

网络安全的未来

尽管预测并不完全可靠，但网络安全的未来可能仍是一个逐渐演变的过程，而不会产生大量的创新技术：将进一步集成安全进攻和防御，以及更易于部署的解决方案，以确保安全保护始终有效。

例如，ProCurve 的主动防御战略蓝图包含以下特性：

- 为 Identity Driven Manager 附加增强特性，例如无客户端和基于代理程序的端点完整性，以及灵活纠正和漏洞评估架构。
- 为 Network Immunity Manager 附加增强特性，例如增强的网络行为异常检测 (NBAD) 功能。
- 增强的边缘策略控制，包括 Web 身份验证以及无客户端端点完整性验证。
- 基于标准的端点完整性，具备可信的局域网、广域网和 WLAN 代理访问。
- 进一步增强 ProCurve Manager，以创建集访问和安全网络基础设施架构管理于一身的平台。
- 继续增强嵌入式威胁管理和基础设施架构身份验证功能。
- 附加新产品和解决方案，将其用于主动防御架构，并解决已出现、但未能识别的安全问题。

最终建议

要实现网络安全，先要了解将进攻与防御纳入单一综合系统的重要性。您必须了解您网络资产遭遇的威胁，以及在这些资产遇到危险的情况下，您企业所面临的风险。切记，要同时考虑内部和外部威胁。企业需要了解攻击的发生方式，才能确定采取哪些相应措施。

为提高安全性、降低复杂性，必须自动实施和审核安全实践。体现网络服务实施方式的企业策略，必须纳入能够报告这些策略并确保其正在运行的自动网络执行系统。此自动功能必须以值得信赖的网络基础设施架构为基础。

源自 ProCurve 适应性边缘架构的 ProCurve 主动防御，是一款具有内置灵活性的解决方案，可以满足现在和未来的安全需求。通过将进攻与防御融入互相结合、易于管理的综合架构，ProCurve 主动防御成为目前和未来可充分发挥网络潜力的理想解决方案。

更多信息

欲知有关 ProCurve Networking 的详情，请访问：www.hp.com.cn/network

© 2008 Hewlett-Packard Development Company, L.P. 本文所含信息如有更改，恕不另行通知。惠普产品与服务的全部保修条款在此类产品和服务附带的保修声明中均已列明，本文中的任何信息均不构成额外的保修条款。惠普对于本文中所包含的技术或编辑错误、遗漏概不负责。

P/N: 4AA1-0786CHP, 修订版 1, 2008 年 3 月中国印刷

