

面向网络访问控制的统一安全访问解决方案

McAfee Unified Secure Access 解决方案

McAfee® Unified Secure Access 是全球首款将终端及网络安全与访问控制及策略审计相集成的网络访问控制 (NAC) 解决方案。

与许多现有 NAC 解决方案不同，迈克菲集成解决方案不但拥有简易准确、经济高效、扩展力强等特性，而且能够有效抵御网络内外的各种安全威胁。这款解决方案集成了自适应策略技术，可以在一款 NAC 解决方案中综合多项评估和控制功能，有效改善您的安全。同时，它能够通过基于应用程序和基于身份信息的技术来控制访问行为并抵御各种威胁，对有权访问关键网络资源的人员严格控制。此外，Unified Secure Access 还可利用现有网络和系统组件，并通过 McAfee ePolicy Orchestrator® (ePO™) 进行集中管理，充分保护您的投资。

主要优势

充分利用现有基础设施

- 可以方便地获取和添加组件，从而打造一套全面的 NAC 解决方案

可与 McAfee ePO 集成

- 使用一个集中控制台来管理终端安全、法规遵从审核以及访问控制

面向员工、合作伙伴以及访客来宾的准入控制

- 针对不同类型的用户提供相应级别的网络访问

根据情况变化调整控制策略，尽量减少错误和维护支持工作

- 根据情况变化调整控制策略，避免误锁定用户

准入控制

- 在准入前后评估终端运行状况并针对违反策略的行为进行修补自动修复

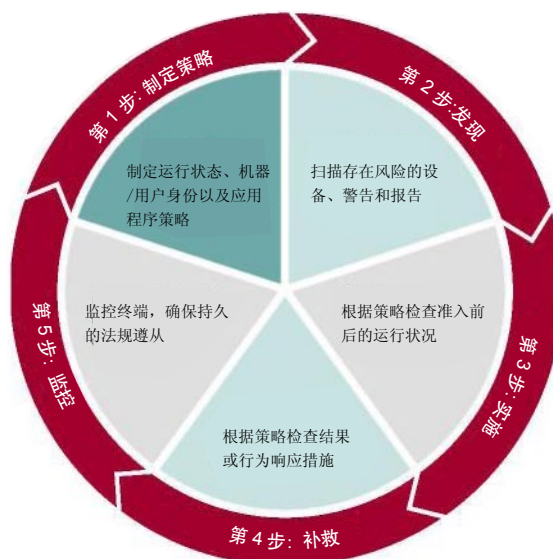
检测网络内有风险或未知的机器和设备

- 检测智能手机、医疗设备、游戏控制台等

提供全面的报告和控制

- 检测和报告终端变化、用户身份信息、访问过的应用程序以及恶意行为

- McAfee NAC 设备支持来宾访问，并提供内置的基于身份信息和应用程序的网络访问控制
- McAfee NAC 软件支持托管用户，并提供终端运行状况评估和本地访问控制
- 面向 McAfee Network Security Platform 的 McAfee NAC 模组综合了 NAC 和网络入侵防御功能，支持来宾访问



McAfee Unified Secure Access 包含三大组件：McAfee NAC 设备、McAfee NAC 软件和面向 Network Security Platform 的 McAfee NAC 模块。根据需要合理搭配这些选购产品，打造全面的 Unified Secure Access 解决方案。

规格

N-450 型号

- 2 Gbps 吞吐量
- 支持 5000 多台并行运行的主机。请注意：实际要求视具体环境可能有所不同。
- 20 个 10/100/1000 端口
- 可同时支持 10 个连续网段
- 支持 SFP
- 支持 DHCP 服务器 — Microsoft、Infoblox 和 Lucent QIP
- 支持 VPN — Cisco、Juniper SSL、和 Nortel
- 与另一设备搭配使用时支持高可用性配置
- 有效的故障转移支持

	1 McAfee NAC 设备	2 McAfee NAC 软件	3 面向 Network Security Platform 的 McAfee NAC 模组	Unified Secure Access 解决方案
准入前控制	×		×	×
准入前监控和控制 (通过 IPS)			×	×
本地访问控制和补救		×		×
来宾访问门户	×		×	×
基于身份信息和应用程序的控制	×		×	×
终端状况评估		×		×
风险系统检测		×		×
主机隔离	×	×	×	×
ePO 集成	×	×	×	×

McAfee NAC 设备

McAfee NAC 设备拥有与 Network Security Platform (入侵防御系统功能) 插件相同的 NAC 功能。如果将这些 NAC 功能与特制硬件搭配使用，将能够打造最经济高效的企业级 NAC 平台。强大的业内领先平台可以同时为 5000 名甚至更多用户提供连续的网络访问控制，线速可达 100 Mbps 至 2 Gbps。



NAC 模块可提供以下功能：

- 灵活的部署 — 用户可以选择采用动态主机配置协议 (DHCP) 模式进行部署，也可选择基于 VPN/LAN 或网络无限接入点进行线内部署
- 针对未受管理主机的访问控制 — 通过安全访客访问门户、主机安全状况评估以及针对访客访问的基于时间的预配置，降低未受管理主机的风险
- 基于身份信息的访问控制 — 通过与 Microsoft Active Directory 集成，根据用户在组织内的角色提供网络访问
- 全面的准入后控制 — 按照应用程序协议、源/目标地址和端口提供网络访问控制
- 有助于促进法规遵从和风险管理的 NAC 监控和报告
- 模拟模式，支持在试行模式下进行测试，无需真正实施
- 风险管理 — NAC 监控与 McAfee Vulnerability Manager 的集成有助于确定存在漏洞的主机是否在尝试频繁访问网络



McAfee NAC 软件

作为 McAfee Total Protection for Endpoint—Advanced 套件的一项重要组件，McAfee NAC 软件是受管理主机（如员工、订约人和远程用户管理）的理想解决方案。无论您是需要制定策略、检测存在风险的或未知设备、评估运行状况，还是要实施策略或进行修补，它都能满足您所需。

主要特性

- 通过集成的 McAfee ePolicy Orchestrator 4.0 制定策略：简单、灵活并且扩展力强
- 与 McAfee Network Security Platform 和 NAC 设备集成，对未受管理的系统实施策略
- 通过与 McAfee Policy Auditor 共享用户界面和检查库，简化法规遵从工作，减少错误发生
- 基于可扩展配置检查单描述格式 (XCCDF) 和开放漏洞评估语言 (OVAL) 的 3000 多项检查 — 面向第三方应用程序、常用软件和操作系统补丁 — 以及定制检查
- 与 Microsoft Network Access Protection (NAP) 紧密集成，用于控制 Windows 终端
- 针对定制检查的全面支持大大提升了策略的灵活性
- 借助各种手段检测和控制受管理与未受管理系统：代理（预先安装或可分散）、风险系统检测、Network Security Platform 以及 Microsoft NAP framework
- 充分发挥现有 Microsoft 产品（包括 Windows Server 2008、NAP、Windows XP 和 Windows Vista）的投资
- 可在现有迈克菲产品的基础上轻松升级

规格

请注意：实际要求视具体环境可能有所不同。

McAfee Network Access Control Server 硬件要求：

- 使用与 ePolicy Orchestrator 4.0 server 相同的硬件。在添加 McAfee Network Access Control 时，我们建议您使用推荐的硬件配置，而非最低配置。有关详细信息，请参阅 ePolicy Orchestrator 4.0 文档。
- ePolicy Orchestrator 4.0 (安装了 patch 2)、Rogue System Detection 2.0 或更高版本和 McAfee Network Access Control Client

系统要求：

- 内存：512 MB 或更大 RAM
- 操作系统：Windows 2000 Professional SP 4; Windows 2000 Advanced Server SP 4; Windows 2000 Server SP 4; Windows 2000 Terminal Services SP 4; Windows XP Professional SP 2 或更高版本; Windows Server 2003 Enterprise SP 1 或更高版本; Windows Server 2003 Standard SP 1 或更高版本; Windows Server 2003 Web SP 1 或更高版本; Windows Vista (所有版); McAfee Agent 3.6 Patch 2 或更高版本

面向 Network Security Platform 的 McAfee NAC 模块

面向 Network Security Platform 的 McAfee NAC 模块可在特制硬件上与入侵防御软件搭配使用，并能够与 ePolicy Orchestrator 集成，打造一款易于管理的 NAC 解决方案。强大的业内领先平台可提供连续的网络访问控制，线速可达 100 Mbps 至 2 Gbps。

附加 NAC 模组可提供以下功能：

- 灵活的部署 — 用户可以选择采用动态主机配置协议 (DHCP) 模式进行部署，也可选择基于 VPN/LAN 或网络无限接入点进行线内部署
- 针对未受管理主机的访问控制 — 通过安全访客访问门户、主机安全状况评估以及针对访客访问的基于时间的预配置，降低未受管理主机的风险
- 基于身份信息的访问控制 — 通过与 Microsoft Active Directory 集成，根据用户在组织内的角色提供网络访问
- 按照应用程序协议、源/目标地址、端口、主机状况变化以及 IPS 检测到的恶意行为提供网络访问控制
- 有助于促进法规遵从和风险管理的 NAC 监控和报告
- 评估模式，支持在试行模式下进行测试，无需真正实施
- 风险管理 — NAC 监控与 McAfee Vulnerability Manager 的集成有助于确定存在漏洞的主机是否在尝试频繁访问网络

规格

- 要求使用 v5.1 软件
- 支持 DHCP 服务器 — Microsoft、Infoblox 和 Lucent QIP
- 支持 VPN — Cisco、Juniper SSL 和 Nortel
- 可用于所有 I 系列和 M 系列平台 (M-8000 除外)



迈克菲(上海)软件有限公司

北京市朝阳区门外大街16号中国人寿大厦1709室

邮编: 100020

电话: (8610) 85722000

传真: (8610) 85752299

上海市徐汇区虹桥路3号港汇2座4005-4006室

邮编: 200030

电话: (8621) 61458878

传真: (8621) 61132278

广州市天河区体育东路118号财富广场西塔15楼106室

邮编: 510620

电话: (8620) 38860668

传真: (8620) 38860638

McAfee销售热线: 800-819-8879 www.mcafee.com/cn

