ARUBA 概览

有线和无线网络的端点可见性

当今强化安全性和合规性的前提条件

过去，走到别人的桌子旁就能看到他们有哪些设备接入网络，但如今这样的日子已经一去不复返了。自携设备 (BYOD) 和未受管理的设备（例如监控摄像头和物联网 (IoT) 类别的其他新兴端点），正在使 IT 难以保持完全的可见性。

挑战

为了识别连接的端点，传统做法通常是部署综合端点管理解决方案、代理并手动更新多端点数据库。然而，这些方法的效果都不甚理想，因为 BYOD、来宾访问部署和恶意有线及无线端点早已让 IT 不堪重负；而且这些端点也会随着用户来去不定。

未来三年内，接入网络的物联网设备预计将会达到数十亿之多，而安全漏洞的公布往往滞后，IT 专业人士一致认为解决实时可见性和报告问题迫在眉睫。他们需要能够持续监控和进行分析的解决方案，来取代定期更新的模式，并且不会受限于位置、时间或端点类型。

当今智能可见性解决方案

与竞争对手相比，Aruba 的 ClearPass 系列对于网络和安全组织而言具有独特优势，因为用户既可通过单独设备也可借助完整的策略执行解决方案来获得实时的无代理分析功能。

无论是否启用 AAA，上述两种形式都可以让您通过辨别是动态还是静态 IP 地址，持续识别有线或无线网络上的端点和网络设备。通过综合仪表板视图，可轻松查看端点总数以及按类别、系列和设备类型分组的数量。

ARUBA CLEARPASS 的优势

- 对端点进行自动检测和分类，满足安全和审计需求
- 持续监控所有设备，包括来去不定的设备
- 无代理可见性功能让您能够查找 BYOD 智能手机和物联网相关设备
- 上下文属性分享功能可将可见性扩展到各种安全和 IT 服务解决方案
- 不再需要手动维护数据库更新
- 端点数量、类型及属性一目了然，由此提高了网络性能和安全

Aruba ClearPass Universal Profiler：这是一款独立的虚拟设备，可在数分钟内完成部署并运行，专为尚未准备好部署完整 NAC 解决方案的企业或尚未部署 NAC 的偏远地区而设计。它可以满足任何企业的可扩展性需求。

Aruba ClearPass Policy Manager：这是一系列虚拟或物理设备，包括综合分析、AAA/非 AAA 有线和无线策略执行、来宾访问、BYOD 入网、端点评估功能、报告以及内置的以安全性和用户体验为核心的第三方解决方案集成。

图 1：按设备类别、系列和类型的精细可见性

ClearPass 系列可以轻松发现端点、识别和分析其属性，以确定设备类别、供应商、操作系统、IP地址、主机名称、所有者等。自动化以及 IT 可自定义的端点分类，可确保快速将新的未知物联网设备归入正确的设备系列，从而增强可见性和/或安全性。为了提高灵活性，ClearPass 还提供使用标准网络或 SPAN 端口监控来发现动态网络的选项。传统的 IT 网络访问控制解决方案可能需要您使用多个昂贵的 10G 端口来监控大型端点部署，而 ClearPass 则不需要。

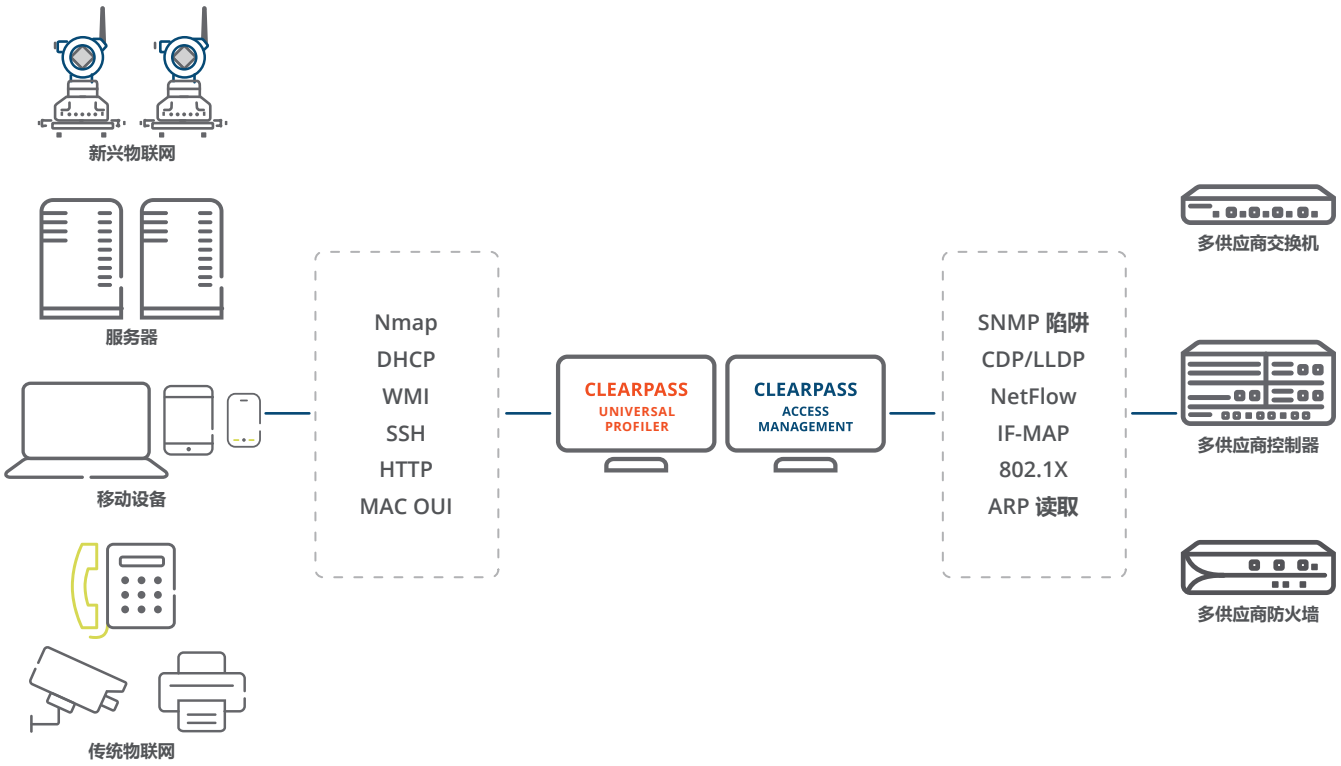

图 2：精细识别和分析方法

精细发现方法

多重分析方法可以收集每个设备的精细端点属性，以便发现潜在的性能问题和威胁风险。由此增强的可见性和上下文见解可以由两个 ClearPass 解决方案共享，也可以直接用于 ClearPass Policy Manager，以实现最优策略，判断可接入的设备，帮助 IT 以最快速度应对潜在威胁。

利用第三方解决方案的端点可见性

借助 ClearPass API、syslog 消息和 Extensions 功能，可轻松与防火墙、SIEM、端点合规性套件和其他解决方案交换端点属性，从而增强策略管理。这些解决方案可以提取端点属性，并针对每个设备类别采取特定的规则来匹配流量模式，以优化连接或阻断可疑流量。

了解更多

要详细了解 ClearPass Universal Profiler 和 ClearPass Policy Manager，以及它们具备哪些独特功能来识别所有端点、协助策略执行、更好地保护您的有线和无线网络，请访问 www.arubanetworks.com/clearpass。

a Hewlett Packard Enterprise company

www.arubanetworks.com

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | **电话：**1.408.227.4500 | **传真：**1.408.227.4550 | INFO@ARUBANETWORKS.COM