aruba
a Hewlett Packard Enterprise company

执行概要

识别、连接和保护边缘移动和物联网

简介

连接到企业网络的物联网设备的大量增长给 IT 带来了诸多挑战，一方面，智能建筑带来许多好处，另一方面，没有正确的工具来自动识别、配置、认证和执行策略，众多未知设备的接入也对企业的网络环境造成了风险。

Aruba 在最新发布的产品中，采取四步走策略，轻松应对物联网边缘连接的难题：识别接入设备，使用智能交换机连接移动和物联网设备，运用业界领先的策略管理策略保护网络安全，通过合作伙伴生态系统进行创新，维护端到端的安全。

物联网带来挑战

移动设备的激增以及向智能建筑的转型，给 IT 和业务领导者带来了不小的挑战。

缺乏可见性 - 您真的了解谁接入了您的网络吗？

网络安全的第一步是要了解谁接入了您的网络 - 未受管理的智能手机、恶意端点或者物联网设备。这些都增加了攻击面，会威胁企业的安全。如果能对网络使用一目了然，IT 就可以更好地了解哪些人在使用自己的网络及其用途。IT 必须能够识别和配置每个接入网络的设备，不论其接入点在哪里。但随着未知无线和有线物联网设备的接入，这一点变得越发困难。所有设备在接入时都必须经过分析和评估、分配到指定的类别，然后根据设备类型、所有权状态和操作系统，系统自动允许或拒绝接入。

有线网络成为新的隐患。

对于企业和工业领域的组织，根据垂直市场的不同（例如运动检测器、医疗设备、工厂车间里的加工控制器等），有线物联网接入设备量的增长可能在 35% 到超过 50% 不等。过去，有关网络访问控制 (NAC) 的讨论主要围绕如何保护无线网络，因为当时大部分设备是通过这种方式接入的。确保每次会话连接的安全性已成为一项必然要求，因为无线窃听和未知用户可以通过访问点和不安全 SSID 从任何位置建立访问。

无线网络安全逐渐成为关注的焦点，这意味着有线网络被暴露在没有保护的环境下，因为人们普遍认为相比无线网络，有线网络的安全性并没有那么脆弱。然而，随着有线网络的增长，交换机的一致性被打乱，导致许多端口暴露在外，任何人都可以接入。会议室和打印机区域的端口就是典型的安全隐患重灾区。随着越来越多的物联网设备通过有线方式接入，我们需要对有线网络基础设施的安全性予以同样重视。

传统的有线基础设施并未针对物联网而优化

在传统交换环境中，劳动力并不是移动的，物联网甚至还不存在。需要保护的内容都有防火墙保驾护航，IT 仅需确保这层边界不被破坏。随着物联网时代的到来，有线基础设施需要与无线基础设施一样智能，如今的交换机需要集安全性与智能网络管理于一身，才能确保所有的接入设备安全、顺畅地接入网络。

保护网络安全需要自动化工作流

每天有数千台未知移动设备和物联网设备接入企业网络，为每个设备手动分配和执行策略显然不太现实。整个流程必须实现自动化，以最大限度地降低风险并减少 IT 的人工操作。对于静态设备和基础设施本身，也应当进行分析和自动检查，以便及时发现可疑更改。如果某个设备出现可疑活动，应当立即对其自动隔离，直到威胁评估完成。

比黑客抢先一步代价高昂

我们似乎每天都听到大规模数据外泄事件。对企业而言，安全投资既昂贵又花时间，自己闭门造车试图抢在黑客前面几乎不可能。Aruba 的合作伙伴生态系统专为领先的安全领域合作伙伴而打造，提供端到端的安全解决方案。

ARUBA 针对物联网边缘连接制定安全的蓝图

1. 在多供应商有线和无线网络上识别并分析未知设备

网络安全的第一步就是了解谁在使用您的网络，因此，识别和分析所有设备必不可少。与竞争对手相比，Aruba 的 ClearPass 系列具有独特优势，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。

全新的 Aruba ClearPass Universal Profiler 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 解决方案的组织或尚未部署 NAC 的偏远地区而设计。Universal Profiler 可以识别和分析接入设备，简单高效、省时省力。

Aruba ClearPass Policy Manager 是一款虚拟或物理设备，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。

2. 通过自动化智能接入物联网设备

向智能建筑转型意味着今天的企业需要更智能的有线基础设施。ArubaOS-Switch 的最新增强功能专为强化和维护智能边缘的安全而设计，最大程度地优化了移动和物联网设备的使用。这些增强功能支持在无线和有线网络基于角色进行访问的同时，向已接入的物联网设备识别和分配角色，从而确定关键业务应用的优先级并确保网络安全。

Aruba 第三层交换机可以实现基于用户和端口且流向移动控制器的有线流量，以便通过策略执行、延伸高级服务和加密流量的方式巩固局域网安全。为了满足物联网设备的高速增长和分布式企业中设备的接入，高性价比的 Aruba 2540（以及其他 Aruba 交换机）支持零接触配置和基于云的可选管理，以使企业能够简化和削减网络部署和管理成本。

3. 通过智能策略维护网络安全

具备设备可见性后，接下来就是自动化策略执行。Aruba ClearPass Policy Manager 可帮助您了解谁在使用您的网络，并在多供应商有线和无线网络基础设施上执行相应策略和自动化工作流。ClearPass 提供分析、策略执行、来宾访问、BYOD 设备入网等功能，帮助减轻 IT 负担、提高威胁防护并提供无缝用户体验。随着维护有线网络基础设施安全成为焦点，OnConnect 功能使用现有的交换机协议，帮您锁定薄弱环节的有线端口，例如会议室、IP 电话和打印机区域。

4. 加快创新，增强边缘安全性

Aruba 的技术生态系统包括集成了 ClearPass Exchange 的业界领先安全解决方案，确保边缘及核心端到端安全。我们最新的合作伙伴重点放在物联网安全：

- Niara 使用已知的流量模式，与设备类别进行关联，通过这种方式识别可疑行为，然后请求 ClearPass 将该设备从网络中清除。
- 当有人尝试使用虚假设备发动网络攻击时，IT 通过 Attivo 创建“虚假虚拟”物联网设备。一旦检测到虚拟设备进行不正当操作，IT 可以通过 ClearPass 将该设备从网络中清除。

结论

随着越来越多的企业逐渐接纳物联网融入主流运维，物联网设备的入网和管理变得至关重要。企业需要制定战略来确保边缘移动和物联网设备接入的安全，在保证网络和公司财产安全的前提下，充分利用智能建筑产生的价值和效率。Aruba 物联网接入的四步走方案可以识别网络的使用者、通过智能有线和无线基础设施接入设备、利用自动化策略管理保护网络安全、使用合作伙伴生态系统促进端到端网络安全，最终抢先解决潜在风险。

aruba
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