解决方案概述

动态网络隔离

有线和无线网络统一的简单和安全访问

越来越多的物联网设备以及业务关键型移动网络和云服务的使用正在推动数字化工作场所的创新，这就引出了一个问题 — 网络边缘是否足够智能，是否可以安全地连接所有类型的设备和用户？传统的有线和无线网络在创建时并未考虑关键业务移动网络、物联网接入或安全性。如今，使用手动和静态方法对遍布园区网和分支网络的这些不断变化的移动网络和物联网设备进行配置带来了新的安全风险，并已成为 IT 团队每天都要面对的一项繁重任务。

为了简化并保护网络，Aruba 动态网络技术可以将有线和无线网络上的策略统一起来，进而保证流量的安全和分离。现在，企业经常出现业务网络、物联网和IT管理终端网络并存，并要求 IT 部门提供端到端运维、同时优化网络体验的情况

动态网络隔离充分利用 Aruba 基于角色的基础策略功能、用户防火墙、丰富的第 7 层应用程序可见性、以及内置 Web 内容过滤等智能特性。

主要优势

- **更好的一致用户体验** — 将用户角色、应用程序深度数据包检查和设备分析功能从无线网络扩展到有线网络
- **更加简单的网络运维** — 通过减少 SSID、ACL、子网和有线网络端口所需的配置节省时间并消除 VLAN 蔓延
- **提升安全性和设备可见性** — ClearPass 和策略实施防火墙 (PEF) 可提供增强的可见性和策略实施

关键业务和技术驱动因素

更加简便的策略管理

接入物联网和客户端设备一般需要多个接触点 — 通常需要在网络中的每一跳手动配置新的 VLAN、ACL 或子网。对于大型分布式网络，需要不断进行的移动、添加和更改操作也可能是耗时，且容易出错的。设计安全性较高，同时又能降低复杂性的网络通常是相互排斥的。

增强用户体验

当用户在办公桌之间或站点之间进行移动时，无论他们在哪里连接网络，也不管他们使用怎样的连接方式（有线或无线），他们都希望获得相同的网络体验。让他们使用虚拟专用网 (VPN) 是一个挑战。任何需要 IT 人员支持的网络体验都会遭到诟病。用户体验（无论是员工、客人、购物者还是学生）会影响到组织的成败。连接智能手机、打印机或视频会议设备等新的设备类型通常是在 IT 人员不知情或无需 IT 人员支持的情况下完成的。理想的情况是，IT 人员既可以提供完美的体验，又能在安全网络上获得所有事物的可见性并进行简便的管理。

从智能照明到安全摄像头或徽章阅读器，物联网设备正迅速部署在各种规模的网络中。这种新发现的网络连接方式带来许多极具吸引力的优势，但也会让网络面临安全风险，因为这些设备与敏感的财务、医疗和业务关键型数据在同一条路径上传输。这些设备很少内置强大的安全功能，也缺乏可靠的身份验证机制。密码以明文形式存储，它们缺乏安全的客户端，而且它们通常位于不安全的公共区域，这就会为网络漏洞敞开大门。

预计到 2020 年，连接到企业网络的物联网/无外设设备数量将增长到 200 亿以上，同时也会暴露出众多的网络漏洞、

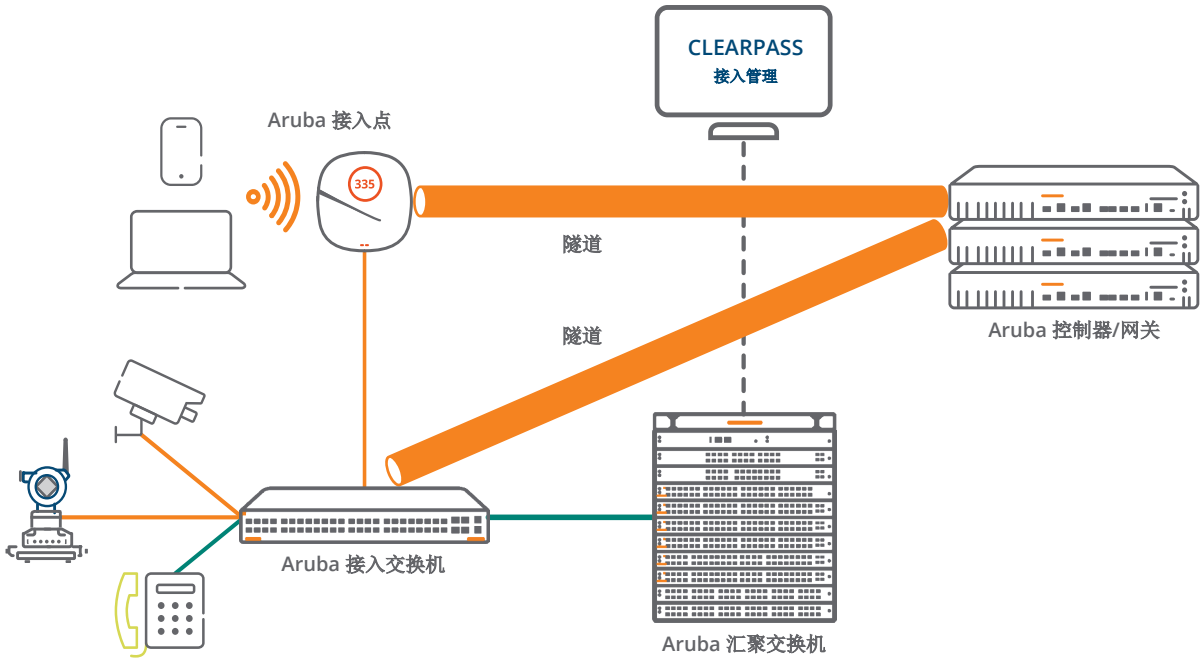
来源：Gartner（2017 年 1 月）

将 WLAN 创新技术扩展到交换层

动态网络隔离技术可以对 Aruba 的安全策略管理和 WLAN 策略强制功能进行扩展，使有线网络接入变得简单又安全。这种功能意味着我们可以根据端口或用户角色为有线终端设备动态分配策略，理想情况下，到 2020 年，物联网设备的数量预计将达到 200 亿。Aruba 网络交换机现在可以在 ClearPass 和移动控制器的支持下，用于策略管理，在统一网络接入方面发挥关键作用。

基于角色的策略

通过实现动态网络隔离，我们可以根据设备类型、使用的应用程序，甚至是用户或设备所在的位置制定基于角色的策略决策和访问权限。基于角色的策略最初用于解决无线网络安全问题，按用户类型（如员工、访客或承包商）划分网络流量，同时通过消除复杂的静态网络配置大大简化网络管理。这一强大的功能简化了 IT 工作流，如管理接入和 BYOD 策略，并确保了更好的应用程序性能。



动态网络隔离，Experience Edge 的一部分

将基于角色的动态策略管理方法扩展到无线接入点和有线交换机可提供一种简单、安全而且独特的方法，管理并强化用于移动网络、物联网和云的各类安全策略。Aruba 的移动控制器/网关（用于执行 ClearPass 策略定义）能够动态地理解和利用角色。这一功能可以动态分配策略，进而可避免管理复杂的静态 VLAN、ACL 和子网所需的耗时且易出错的任务。

第 4-7 层网络隔离

Aruba 交换机可以利用的第二个基础功能就是网络隔离。Aruba WLAN 架构通过在接入点和控制器或网关之间使用隧道来保持流量的安全和分离。这种基于隧道的隔离技术可通过使用 Aruba 内置的策略实施防火墙 (PEF) 提供安全性，如对高风险流量进行防火墙检查。Aruba 策略防火墙可以提供非常详细的情境策略（用户、设备、应用程序、位置），无需额外购买价格高昂的防火墙作为安全检查和防御的第一道防线。通过基于身份、设备类型和位置的情境策略，因为流量可以与相应的角色进行适配，您可以使用单个网络配置满足不同用户组的需求。

通过使用这种 WLAN 隧道架构，Aruba 交换机现在可以提供一种基于角色的隔离方法，而不是传统的、更依赖手动的本地 VLAN 使用方法。这种方法特别适合不受信任的物联网设备或提供应用程序可见性，因为 Aruba 交换机现在可以通过隧道动态地将选定的流量传递到控制器，以便进行数据包深度检查和设备身份验证，其工作原理和接入点非常类似。例如，我们可以动态地为安全摄像头分配一个角色，该角色权限只允许其流量被转发到指定服务器，从而消除恶意进入网络其他部分的机会。

这种新的隔离功能可提高隧道的安全性，隧道可以设置为基于端口的隧道 (PBT)，将所有身份验证都在控制器上完成，也可以设置为基于用户的隧道 (UBT)，使身份验证在交换机上完成的。这种隔离方法作为一种叠加模式，它可以在不对整个交换基础设施进行拆分和替换的情况下，在选定区域中使用安全隧道，从而实现与传统 VLAN 模式的共存。

动态网络隔离可通过将移动控制器建立为统一的策略实施引擎来简化和保护有线和无线网络。来自接入点或交换机的流量被封装在 **GRE** 隧道中，以供策略实施防火墙 **(PEF)** 进行检查。

解决方案组成部分

Aruba 无线接入点

可满足任何环境需要的 802.11Ac 和 802.11ax Wi-Fi 性能。内置 AI 和定位服务，可为 IT 人员提供为用户和物联网设备提供最佳体验所需的自动化和可视性。

Aruba 网络交换机

创建一个无线网络和有线网络集成的基础平台，为园区和分支网络提供可扩展性、安全性和高性能。动态网络隔离可为 IT 团队提供一种简单的方法，以应用安全策略，提供高级服务，并通过隧道对网络中任何位置的有线用户和物联网流量进行安全隔离，可以使用在控制器上完成身份验证的，基于端口的隧道 (PBT)，也可以使用在 Aruba 交换机上完成身份验证的，基于用户的隧道 (PBT)。

Aruba 网关和移动控制器

作为解决方案的关键部分，控制器或网关可以充当有线和无线流量的策略执行器。IT 人员可以通过 Aruba 移动控制器（运行 AOS 8.1 或更高版本）实施安全策略实施、带宽合约和其他流量限制。在分支环境中，Aruba Central 管理的分支网关可执行此角色。策略实施防火墙可以作为支持这两种环境的底层网络技术。

具有分析功能的 Aruba ClearPass Policy Manager

集中管理和实施用于无线和有线网络接入控制的网络接入策略。它的主要功能是设备分析、身份验证、授权和策略定制。使用 ClearPass 定义角色和权限后，它们就会在有线和无线网

络接入中跟踪用户或设备。因此，如果用户改用未知设备，或处于不安全的网络，策略将自动更改其授权权限。ClearPass 上还可以配置可下载用户角色 (DUR)，无需在交换机上定义角色或策略。

总结

为了更好地满足业务关键型移动网络和新兴物联网的连接需求，Aruba 创新的动态网络隔离解决方案可通过动态应用统一策略并在网络中的任何位置执行高级服务简化 IT 运维并提高安全性。这可确保为所有无线和有线网络用户无缝分配、自动应用并独立执行恰当的接入和安全策略。

SO_DynamicSegmentation_SK_092419 a00058593enw