解决方案概述

# 为用户和设备提供简单安全的访问

面向网络边缘的 Aruba 动态隔离解决方案

IoT 设备数量增长以及移动性关键业务和云服务的广泛使用推动了创新，这也使得我们面临着一个问题：网络边缘是否具备足够智能，从而安全地连接所有类型的设备和用户？旧的网络在创建之时，并未考虑到移动性关键业务、IoT 接入或安全性。现在，针对这些遍布于整个园区和分支机构网络中不断变化的移动和 IoT 设备，使用手动的静态配置会造成新的安全风险，并已成为 IT 团队每天面临的繁重任务。

Aruba 的动态隔离解决方案通过独有的智能化方式来帮助解决这一复杂的挑战。它不仅可以为 IT 团队简化访问层管理，同时还提供了更安全、一致的体验，不受用户或设备类型以及连接方式的限制。通过将 Aruba 无线网络基于角色的策略功能扩展到有线交换机，动态隔离解决方案提升了安全性，提供一致的用户体验，并简化整个有线和无线网络中的 IT 操作。

## 实现简化统一访问的推动力量

### 策略管理复杂性

网络发展日新月异，在进行管理和保护的同时提供出色的客户体验是一项巨大的挑战。开通有线用户和 IoT 设备涉及企业网络的多个环节，而针对有线和无线网络实施统一的策略不仅费时，还可能使得故障排除过程异常复杂且困难。在具有众多设备类型和用户的大型网络中，管理网络上事物的增减同样也会占用大量时间并且易于出错。为了防止网络入侵，以简单、统一的方式设计具有可靠的安全性以及有线和无线访问控制的网络势在必行。

### 改进用户体验

用户在进行场景转换时，例如从办公桌面到会议区域，或者从宿舍到课堂，他们希望不论在哪里进行连接，不论是通过有线还是无线方式连接，都能获得相同的网络体验。并且，要求用户使用虚拟专用网络 (VPN) 也非常麻烦。任何需要 IT 支持的客户体验都会被认为是糟糕的体验。而不论员工、访客、购物者还是学生的用户体验，对于组织的成功与否都会产生影响。连接新的终端类型，例如智能手机、打印机或视频会议设备，这些操作通常应该不需要掌握 IT 知识或者无需支持即可完成。理想情况下，IT 应该提供无缝的体验，同时在安全的网络上维护对所有事物的可见性和管理能力。

### IoT 设备的增长及新的安全关注

从智能照明到安全摄像头和标签阅读器，IoT 设备正在快速部署于各种规模的网络中。这种新出现的网络连接带来了许多极具吸引力的优点，不过同时也将网络暴露在安全风险中，因为这些设备与敏感的财务、医疗和关键业务数据采用相同的传输途径。这些设备极少内置了可靠的安全功能，同时也缺乏可靠的身份验证措施。这些设备以明文存储密码、缺少安全的申请方并且其物理位置通常处于不安全的公共区域，这为网络入侵打开了大门。

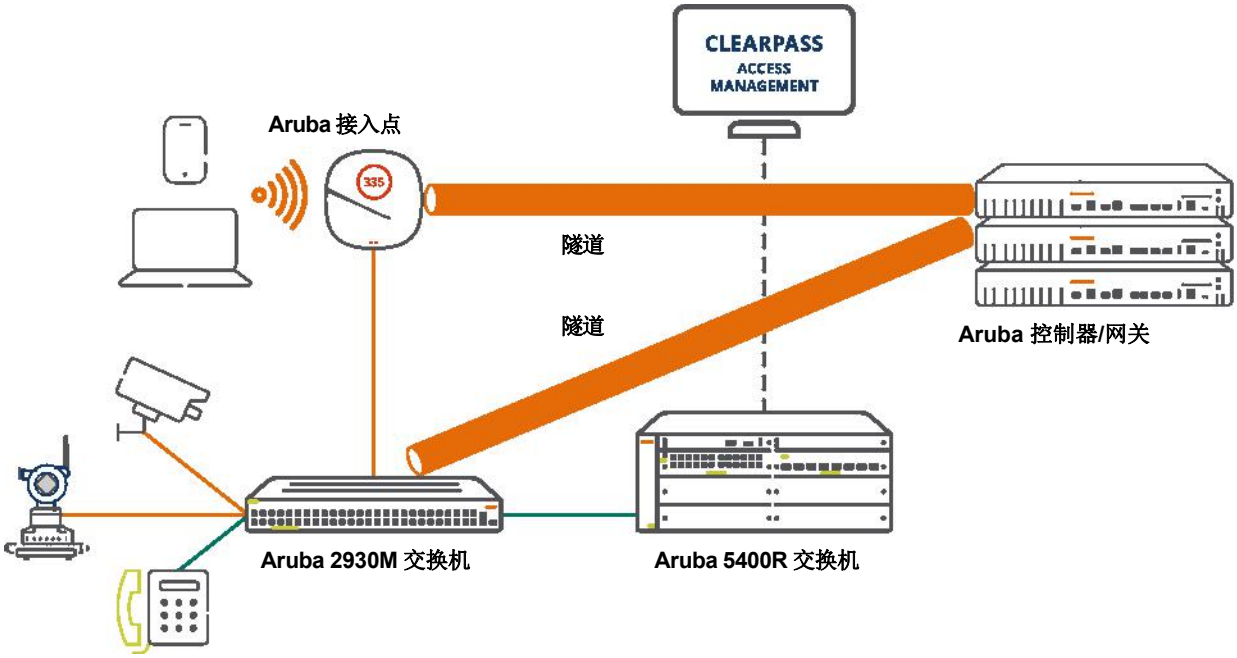
> 到 2020 年，预计连接到企业网络中的 IoT 设备数将超过 200 亿，网络漏洞也会随之而来。
>
> *资料来源：Gartner（2017 年 1 月）*

## 将 WLAN 创新扩展到交换功能中

Aruba 的动态隔离解决方案利用 Aruba 独特的安全接入和策略管理解决方案，简化了有线网络接入的安全性。此功能的重要性在于，交换机不再仅仅为旧设备提供有线接入，它还作为网络聚合器，为不断增长的新兴 IoT 设备提供连接。通过实施基于角色（员工、访客、摄像头等）的策略，利用 Aruba 控制器和 Aruba ClearPass 的智能进行策略管理，Aruba 接入交换机现在可以在网络边缘提供所需的安全保护。

## 基于角色的策略

通过实施动态隔离，将根据设备类型、所用应用程序以及用户或设备的位置来确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满足无线安全需求，它根据用户类型（例如员工、访客或承包商）将网络流量分类，同时避免了复杂的静态网络配置，从而显著简化网络管理。这一强大的功能实现了流畅的 IT 工作流，例如管理访问和 BYOD 策略，并确保更好的应用程序性能。




面向网络边缘的动态隔离解决方案

将基于角色的动态策略管理扩展到有线边缘，这针对移动性、IoT 和云的策略管理和实施，提供了一种截然不同的大幅简化且安全的方法。Aruba 的智能接入交换机软件利用 Aruba ClearPass 进行集中策略定义和实施，现在可以动态了解并利用角色。此功能在设备建立连接时动态分配到角色到有线端口，从而避免了管理复杂的静态 VLAN、ACL 和子网的耗时且易于出错的任务。

### 分段

Aruba 交换机利用的第二个基本功能是隔离。Aruba WLAN 架构在接入点和控制器或网关之间使用隧道，确保流量的安全和分离。此基于隧道的隔离通过使用 Aruba 的内置策略实施防火墙 (PEF)，提供了高风险流量防火墙检测等安全功能。PEF 提供的深度包检测功能可以提供细致的具体环境信息（用户、设备、应用程序、位置），从而无需在第一线使用昂贵的防火墙进行检测和防御。通过基于身份、设备类型和位置的环境策略，您可以通过单一网络配置满足不同用户组的需求，因为流量流可以轻松地适配到所分配的角色。

通过使用完全相同的隧道架构，Aruba 交换机现在可以提供基于角色的动态隔离方法，而传统的本地 VLAN 更多使用手动过程。对于不可信 IoT 设备或者对于提供应用程序监控能力，这非常有用，因为 Aruba 交换机现在可以动态通过隧道将选定的流量传输到控制器，进行深度包检测和设备身份验证，就像无线接入点所做的那样。例如，安全摄像头可以动态分配到一个角色，其权限限制将流量仅传输到指定的服务器，这就避免了摄像头恶意进入网络其他部分的可能性。

这种新的隔离功能利用隧道，可设置为采用基于端口的隧道 (PBT) 并在控制器上完成所有身份验证，或者采用基于用户的隧道 (UBT) 并在交换机上完成身份验证，大幅改进了安全状况。由于这种动态隔离技术以叠加方式运行，在选定区域中使用安全隧道，无需丢弃和更换整个基础设施，从而可以与传统的 VLAN 共存。

**通过隧道连接到 Aruba 移动控制器的设备上可以实施防火墙和访问策略，用于限制访问。网络管理员无需在网络基础设施中安装昂贵的防火墙，而是可以使用控制器的内置 PEF 功能来控制有线、无线和 VPN 访问，同时通过单一网络配置满足对不同用户组的需求。**

### ARUBA 动态隔离解决方案的优点

除了更高级别的有线访问安全性、可控性和效率之外，动态隔离解决方案还提供了：

- **更出色的一致用户体验** – 基于角色的集中统一策略控制，可以针对无线和有线流量，不论用户或 IoT 设备在什么位置以及如何连接（有线或无线），均能为其提供相同的策略及一致的用户体验。
- **简化操作** – IT 避免了手动配置静态 VLAN 和 ACL 的负担，可以节省时间和减少配置错误。与传统 VLAN 隔离共存意味着不需要终端网络设计，也不需要丢弃和更换交换基础设施。
- **改进安全状况** – 增强了具体环境感知信息，例如通过内置控制器服务进行的设备分析，这让您可以针对无线和有线流量利用防火墙、数据包检测和指纹等额外的安全功能。动态防火墙检测“存在风险”的有线流量，例如 IoT 设备，可以极大强化边缘的安全状况。

## 解决方案组成部分

### Aruba 无线接入点

802.11ac 和 802.11ax Wi-Fi 性能，满足任意环境的需求。内置的 AI 智能以及定位服务，提供 IT 所需的自动化和监控功能，为用户和 IoT 设备带来最优体验。

### Aruba 接入交换机

创建集成的无线/有线平台，为园区和分支机构网络提供可扩展性、安全性和高性能。动态隔离为 IT 团队带来了独有的简单方法，用于应用策略、利用高级服务以及在网络中的任意位置通过隧道对有线用户和 IoT 流量安全地分段，它采用基于端口的隧道 (PBT) 并在控制器上完成身份验证，或者通过基于用户的隧道 (UBT) 并在 Aruba 交换机（运行 ArubaOS-Switch 16.04 或更高版本）上进行身份验证。

### Aruba 控制器和网关

作为解决方案的关键组成部分，控制器或网关用作针对有线和无线流量的策略实施器。Aruba 移动控制器（运行 AOS 8.1 或更高版本）使得 IT 可以利用策略实施、带宽合同和其他流量限制。在分支机构环境中，Aruba Central 管理的分支机构网关（运行 AOS 8.4）执行此角色。Aruba 策略实施防火墙实施应用程序层安全性、优先级划分并实施网络访问策略，指定谁可以使用什么移动设备连接到网络以及可以访问网络的哪些分段。

### Aruba ClearPass

提供针对无线和有线访问控制策略的集中管理功能。其主要功能是设备分析、身份验证以及授权和策略分发。使用 ClearPass，在定义了角色和权限之后，这些角色和策略会跨有线和无线访问跟随用户或设备。因此，如果用户改为使用未知的设备，或者位于不安全的网络上，策略将自动更改授权权限。可下载用户角色 (DUR) 在 ClearPass 上配置，这消除了在交换机上定义角色或策略的需求。

## 总结

为了更好地处理移动性关键业务应用以及新兴的 IoT 连接要求，Aruba 的创新的动态隔离解决方案通过动态应用统一策略并在网络中随处实施高级服务，简化了 IT 操作并提高了安全性。这确保可以针对所有无线和有线用户及设备，无缝分配、自动应用并独立实施合适的访问与安全策略。

## 了解详细信息

http://www.arubanetworks.com/products/networking/

a Hewlett Packard Enterprise company

© 版权所有 2018 Hewlett Packard Enterprise Development LP。此处包含的信息可能会发生更改，恕不另行通知。对于 Hewlett Packard Enterprise 提供的产品和服务，仅在随产品和服务提供了明示担保声明时，Hewlett Packard Enterprise 方按照其中规定的条款提供担保，此处所述任何内容均不可理解为构成额外担保。对于其中包含的任何技术或编辑错误，或者任何遗漏，Hewlett Packard Enterprise 不承担任何责任。

SO_DynamicSegmentation_112618 a00058593enw