解决方案概述

具有零信任安全功能的 Aruba ESP

边缘安全

随着用户越来越分散，攻击变得越来越复杂和持久，网络安全挑战在过去几年中发生了重大变化。采用传统安全方案，主要聚焦在网络边界安全的策略已经失去效果。现代网络安全方案必须适应不断变化的多样化的用户和设备，以及针对网络基础设施中先前“可信”部分的更普遍的威胁。

新兴的“零信任”方案已经成为一种有效的模型，通过假设所有用户、设备、服务器和网段本身都是不安全的，并且可能是恶意的，可以更好地满足现代企业不断变化的安全需求。具有零信任安全功能的 Aruba ESP 智能边缘架构通过对以前被信任的网络资源实施一系列更为严格的安全最佳实践和控制方法来改进网络的总体安全状况。

ARUBA ESP：零信任原则

零信任根据所考虑的安全域而有很大的不同。尽管在应用程序级别进行控制一直是零信任话题关注的一个焦点，但全面的策略还必须包括网络层安全和日益增多的联网设备，包括在家办公的场景。具有零信任安全功能的 Aruba ESP 集成了全面的可见性、最严格的精细隔离和控制功能，以及持续的监视和强制能力。尽管传统的 VPN 解决方案通过确保将应用于园区网或分支机构网络的控制策略扩展到家庭或远程工作者，进而对方案进行强化。

但是随着物联网时代到来，一些基本的网络安全原则往往难以实现。只要存在可能，所有设备和用户都应该首先被正确识别和验证，然后才能授予网络访问权限。除了身份验证之外，用户和设备在它们接入网络后只应该被授予执行关键业务活动所需要的最小的访问权限。这意味着授权任何给定的用户或设备可以访问哪些网络资源和应用程序。最后，终端用户和应用程序之间的所有通信都应该加密。

全面可见性的需要

随着物联网的日益普及，网络上所有设备和用户的全方位可见性已成为一项越来越具有挑战性的任务。没有可见性，支撑零信任模型的关键安全控制就很难实现。自动化、基于人工智能的机器学习以及快速识别设备类型的能力至关重要。

Aruba ClearPass Device Insight 可以组合使用主动和被动发现以及各种分析技术，来全面检测已连接或试图连接到网络的设备。这包括常见的基于用户的设备，如笔记本电脑和平板电脑。它与传统工具的不同之处在于，它能够对越来越多样化，在当今网络中越来越普及的物联网设备进行查看。

采用“最少访问”和精细网络隔离

实现可见性之后，实施零信任最佳实践，实现“最少访问”和精细网络隔离是关键的后续步骤。这意味着，对网络上的每个端点使用尽可能最佳的身份验证方法（即对用户设备使用完整的 802.1X 和多因素身份验证），并应用访问控制策略，授权该设备或用户只能对绝对必要的资源进行访问。

Aruba ClearPass Policy Manager 允许创建基于角色的访问策略，使 IT 和安全团队能够根据最佳实践，使用相应的角色并在网络任何位置（有线或无线网络基础设施、分支机构或园区内）实施相关的访问权限。在设备被识别后，会自动获得正确的访问控制策略，并通过 Aruba 动态隔离功能与其他设备进行隔离。该操作由嵌入在 Aruba 网络基础设施中的完全的应用层防火墙—— Aruba 策略实施防火墙 (PEF) 来实施。Aruba 基础设施还会在无线网络上利用类似WPA3标准这些最安全的加密协议。

ClearPass Policy Manager 集成了多种身份认证解决方案，进而允许使用多因素身份认证，并能够在整个网络的关键点强制实施重认证。通过 ClearPass 生态系统，客户还可以轻松集成其他解决方案，以满足与上下文信息和其他安全遥测数据相关的零信任要求。

这意味着，ClearPass 可以与端点安全工具等各种各样的解决方案集成，以便根据设备的态势做出更智能的访问控制决策。我们还可以根据正在使用的设备类型、用户的连接位置和其他基于上下文的标准更改访问控制策略。

持续监控和策略实施

实现基于角色的访问控制，进而实施细粒度网络隔离后，对网络上的用户和设备进行持续监控就成为另一种零信任最佳做法。这种做法可以防范与内部威胁、高级恶意软件或绕过传统外围防御的持续威胁相关的风险。

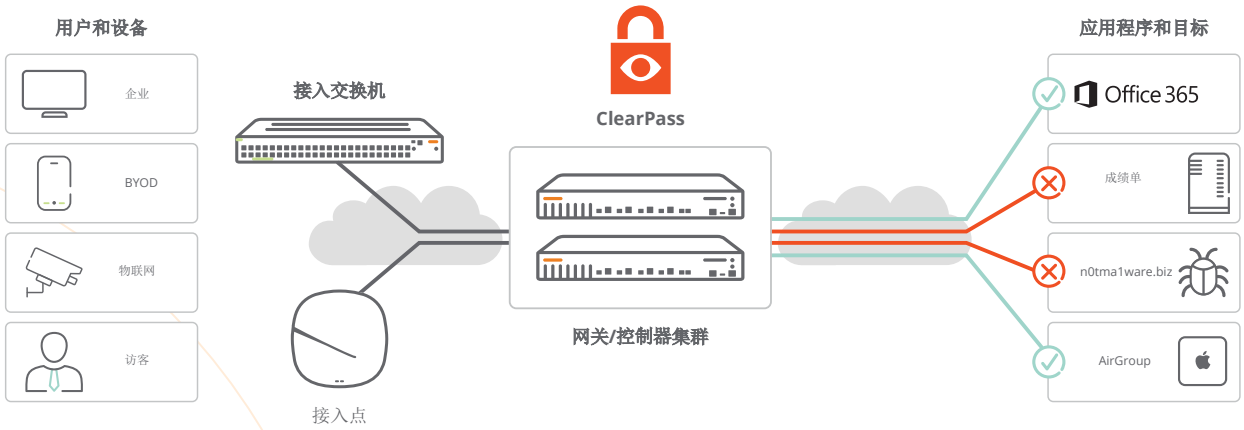

图 1：Aruba ClearPass 可自动分配通过动态网络隔离实现的，基于角色的访问控制策略

图 2：零信任安全是 Aruba ESP 的核心功能

使用 IDS/IPS 进行威胁防御

Aruba 的威胁防御能力可以抵御各种威胁，包括网络钓鱼、拒绝服务 (DoS) 和越来越广泛的勒索软件攻击。Aruba 9000 SD-WAN 网关可执行基于身份的入侵检测和防范 (IDS/IPS)，与 Aruba Central、ClearPass Policy Manager 和策略实施防火墙进行协同工作。基于身份的 IDS/IPS 可对通过网关的分支办公室 LAN（东西向）流量和 SD-WAN（南北向）流量执行基于签名和特征的流量检查，以提供内在的分支机构网络安全功能。Aruba Central 中的高级安全仪表板可为 IT 团队提供整个网络的可见性、多维度威胁度量、威胁情报数据以及相关性和事件管理。威胁事件将被发送到 SIEM 系统和 ClearPass 进行修复。

360 Security Exchange

ClearPass Policy Manager 能够集成 150 多种由包括安全操作和响应 (SOAR) 工具集在内的同类最佳安全解决方案，可以根据来自多个来源的实时威胁遥测实现动态访问控制。可以根据来自下一代防火墙 (NGFW)、安全信息和事件管理 (SIEM) 工具以及多种其他来源的警报创建策略，以做出实时访问控制决策。ClearPass 操作可以被配置为从限制访问（即仅限互联网）到从网络中彻底删除设备，以便进行补救。

ARUBA ESP（边缘服务平台）

为了帮助我们的客户充分利用来自边缘的机会，我们开发了全球首款专门用于对边缘进行统一、自动化处理和保护的人工智能平台 Aruba ESP。零信任安全性 (Zero Trust Security) 是 Aruba ESP 的一个关键组件，与 AIOps 和统一的基础设施相结合后，可以帮助组织降低成本、简化操作并保持安全。

总结

今天的网络环境和威胁态势需要一种不同的方案。过去以边界为中心的网络安全方案无法再满足时下移动员工或新兴物联网设备的要求。具有零信任安全功能的 Aruba ESP 可提供包含可见性、控制和强制的全套功能，可以满足物联网驱动的分散型网络基础设施的需求。

SO_ZeroTrustSecurity_051120 a00097694enw