aruba
a Hewlett Packard Enterprise company

解决方案概述

ARUBA CLEARPASS POLICY MANAGER

有线和无线网络访问的可见性与安全性

您还记得吗，IT 曾经扮演把关者的角色，依靠一系列严格的策略和完全封闭的生态系统来治理网络访问？这样的日子早已一去不复返。如今，在边界安全内外，IT 和用户自有设备已建立连接。

在工作中，随着笔记本电脑、智能手机、平板电脑以及物联网 (IoT) 设备的大量使用，确认网络中接入了哪些设备成为维护数据安全的首要环节。自动化策略的执行确保了只有授权用户和设备可以接入网络，实时威胁防护可以确保安全性满足内部和外部审计与合规性要求。

不出所料的话，物联网设备在有线和无线网络上的应用正在改变 IT 的关注点。大多数企业对无线网络和设备进行了保护，但却忽略了会议室、IP 电话和打印机区域的有线端口。同时，由于物联网设备可能缺少必要的安全属性，并且需要通过外部管理资源进行访问，导致有线访问成了新的安全隐患。

IT 想要控制局面，就必须拥有必要的工具，以便快速编程底层基础设施、控制已知和未知的物联网和移动设备的网络访问。如今的访问安全解决方案必须提供分析、策略执行、来宾访问、BYOD 设备入网等功能才能减轻 IT 负担，提高威胁防护并改善用户体验。

移动性和物联网正在改变我们对网络访问控制 (NAC) 的看法

IT 已不仅仅局限于企业办公区域之内了。许多企业的目标是随时随地提供安全的网络连接。IT 如何在不影响业务和用户体验的前提下保持其可见性和控制力？首先，要从下面三个步骤做起。

1. **识别**正在使用的设备及其数量、接入点和支持的操作系统；这是基础步骤。持续观察各种变化和设备接入和断开连接的情况，这可以逐渐建立起可见性。
2. **执行**准确的策略，不论用户、设备类别和位置如何，都能确保正确的用户和设备访问；这样才能提供期望的用户体验。企业必须适应不断推陈出新的设备及功能，不论是智能手机还是监控摄像机。
3. **保护**资源，使用动态策略控制和实际威胁补救措施，这些内容也要扩展到第三方系统。这是三步计划中的最后一步。要想从容应对凌晨三点突发的异常网络行为，需要一套统一的方法来阻断流量并改变设备的连接状态。

企业必须针对现有和可能发生的挑战做好准备。当用户想要远程工作或者购买新的智能机时，依赖 IT 或服务台工作人员的人工干预是不现实的。NAC 不再局限于在已知设备访问网络之前进行性能评估。

一目了然，尽在掌握

ClearPass 策略和 AAA 解决方案提供了内置设备分析、基于网络的管理界面、全面报告以及实时警报。所有收集到的上下文数据都将用于确保用户和设备都已获得相应的访问权限，而不用考虑访问方式和设备归属问题。

内置分析引擎负责收集包括设备类别、供应商、操作系统版本等在内的实时数据。这样一来，您就对有线和无线网络上接入的设备心中有数了。精细的可见性为通过审计以及判断网络性能和安全隐患提供了必要的数据。

CLEARPASS EXCHANGE 的强大功能

对于尚未准备好全面执行策略的企业或者尚未部署 ClearPass 的偏远地区，独立的 ClearPass Universal Profiler 可以提供同样的分析可见性。

基于模板的策略执行使 IT 能够建立以有线和无线网络为导向的策略，这些策略可充分利用用户角色、设备类型、MDM/EMM 数据、证书状态、位置、星期几等数据。这些策略可以针对员工、学生、医生、来宾、高管以及他们所携带的设备轻松执行相应规则。

ClearPass OnConnect 功能是内置的，企业可以通过它来关闭数以千计的未执行 AAA 的有线端口。无需进行设备配置，只需在交换机中敲入一条命令行即可。有线和无线网络还支持使用标准 AAA/802.1X 方法。

这可实现策略执行的一致性和端到端的连接方式，而孤岛式 AAA、NAC 和策略解决方案无法做到。ClearPass 能够在一个策略服务内使用多种身份存储，包括 Microsoft Active Directory、LDAP 兼容目录、ODBC 兼容 SQL 数据库、令牌服务器及内部数据库，与传统解决方案相比，这一优势使 ClearPass 脱颖而出。

设备配置不再需要 IT 干预

管理 BYOD 部署的个人设备入网可能会增加 IT 和服务台工作人员的工作量，同时也会带来一定的安全隐患。

ClearPass Onboard 帮助用户独立完成设备配置，以便接入安全的网络。每个设备独有的证书，甚至让用户不用整天重复输入登录凭据。单单是这种便捷性便可彰显 ClearPass Onboard 的独一无二。使用证书所带来的额外安全保障更是锦上添花。

IT 团队可以定义哪些用户可以接入设备、接入设备的类型及每个人可接入设备的数量。内置证书颁发机构使 IT 能够以内部 PKI 的形式更快速地支持个人设备，且后续无需占用 IT 资源。

简单快捷的来宾访问

BYOD 不只局限于员工设备，而是包括任何需要通过有线或无线方式访问网络的访客设备。IT 需要一个简单的模型，将设备连接到特定门户，自动配置访问凭据，同时提供使企业通信单独进行的安全功能。

借助 ClearPass Guest，无论是员工、接待员，甚至是活动协调员和其他非 IT 员工，都可以轻松地为任意数量的来宾创建临时网络访问帐户。MAC 缓存使来宾一整天都能轻松接入网络，不必在来宾门户上重复输入凭据。

来宾可以通过自助注册创建自己的凭据，不需要由员工进行操作。登录凭据通过打印徽章、短信或电子邮件提供。凭据可以在设置的时间段内存储在 ClearPass 中，也可以设置为在特定小时数或天数后自动过期。

设备安全性决定可否访问

在授权过程中，可能需要对特定设备进行安全状况评估，以确保它们符合企业的防病毒、防间谍和防火墙策略。自动化促使用户在接入企业网络之前进行防病毒扫描。

ClearPass OnGuard 具有一项内置功能，可基于状态执行安全状况检查，消除各种版本的计算机操作系统中的安全隐患。无论是使用永久性还是临时性客户端，ClearPass 都能在无线、有线及 VPN 基础设施上集中识别符合要求的端点。

可提供额外安全性的高级安全状况检查示例如下：

- 处理对等应用、服务和注册表项。
- 确定是否允许 USB 存储设备或虚拟机实例访问。
- 管理桥接网络接口和磁盘加密的使用。

从第三方解决方案获得更多益处

ClearPass Exchange 使您能够通过常见的第三方解决方案（如防火墙、MDM/EMM、MFA、访客注册和 SIEM 工具等），自动进行安全威胁补救或增强某项服务。利用 ClearPass 所含的上下文智能，可帮助组织确保在设备、网络访问、流量检查和威胁防护级方面提供安全性和可见性。

借助通用语言 (REST) API、syslog 消息和内置存储库 ClearPass Extensions，自动化工作流和决策可帮助简化任务，同时确保企业安全，不再需要复杂的脚本语言和繁重的手动配置。为了加速集成，Extensions 还允许合作伙伴上传扩展程序，实时为联合客户提供新的服务。

通过 ClearPass Exchange，网络可以自动采取操作：

- 可以根据设备的越狱状态等 MDM/EMM 数据确定设备能否接入网络。
- 防火墙可以根据用户、分组或特定设备属性准确执行策略，还能够利用 ClearPass 针对行为异常的设备进行修复。
- 可设置 SIEM 工具以存储所有已连接设备的身份验证数据。
- 在用户接入网络和访问资源时，系统可能会要求其使用多重身份验证以证明自己的身份。

通过触发双向操作，网络活动还可促使防火墙、SIEM 和其他工具通知 ClearPass 对某一设备采取操作。例如，当某一用户多次进行网络身份验证但都失败，ClearPass 会直接向该设备发出通知消息，或将其列入黑名单，拒绝其访问网络。

随时随地安全访问工作应用

对于日常登录工作应用而言，最重要的是方便快捷。为此，ClearPass 支持 SSO 和 ClearPass Auto Sign-On 功能。与需要每位人员都登录应用一次的单点登录相比，Auto Sign-On 使用有效的网络登录，从而自动为用户提供企业移动应用访问。用户只需进行网络登录，或者在设备上安装有效证书即可。

需要使用单点登录时，ClearPass 还可用作身份提供者 (IdP) 或服务提供者 (SP)。

Bonjour、DLNA 和 UPnP 服务

Aruba Wi-Fi 基础设施的用户可以共享具备 DLNA/UPnP、Apple AirPlay 或 AirPrint 技术的投影仪、电视、打印机和其他媒体设备。借助 ClearPass，寻找和共享这些设备将变得更加轻松。

例如，要从平板电脑显示演示文稿的老师将只能看到其所在教室中可用的显示屏，而不会看到校园里其他位置的设备。他们还可以通过该门户选择可使用该显示屏的其他人员，来防止学生操作显示屏。

再举一个医疗保健领域的例子，医生可以将自己 iPad 上的数字 PACS 影像轻松投影到医院内任何位置的较大屏幕上，以便多位医生进行会诊。

安全与服务的适应性基础

不论是为如今的移动用户提供无缝体验，还是快速普及物联网技术，都带来了许多全新的 IT 难题。需要完善的计划，采用合适的工具，并具备坚实的基础，才能确保随时随地安全地进行有线和无线访问。

ClearPass 借助一个完整全面的解决方案，提供设备标识、策略控制、工作流自动化和自动化威胁防护，一次性攻克了这些难题。通过捕获和关联实时上下文数据，您可以通过 ClearPass 来定义适用于任何环境（办公室、校园或球场）的策略。

最新的 ClearPass 增强功能还能应对以下新兴网络安全挑战：物联网的采用、增强的移动设备和应用身份验证，以及对于安全事件的更深层可见性。自动化威胁防护和智能服务功可确保准确无误地为每个设备分配正确的网络访问权限，最大限度地减少 IT 介入。

aruba
a Hewlett Packard Enterprise company

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

www.arubanetworks.com