解決方案概觀

ARUBA CLEARPASS POLICY MANAGER

有線和無線的存取可見性與安全性

您還記得嗎，IT 曾經擔當閘道管理員要職，並且在嚴格政策與全封閉式生態系統雙管齊下的治理下井然有序？這樣的時代早已過去。如今 IT 和使用者自有裝置在周邊安全性內外互相連接。

筆記型電腦、智慧型手機、平板電腦和物聯網 (IoT) 裝置不斷湧入工作場所，因此，保護資料安全的首要課題就是識別網路上到底有哪些裝置。自動化政策實施可確保只允許連接所需的使用者和裝置，並且需要即時威脅防護以確保符合內部與外部的稽核與合規性要求。

如果預期沒錯的話，在有線和無線網路上使用 IoT 裝置正在轉變 IT 的焦點。大多數公司會保護無線網路和裝置的安全，但卻忽略了會議室裡面、IP 電話後面及印表機區域中的有線連接埠。同時，由於 IoT 裝置可能缺少安全性屬性，但又需要從外部管理資源進行存取，由此使得有線存取成為新的風險隱患。

當 IT 苦惱於如何維持控制權時，他們需要一套適當的工具來快速編程基礎架構，進而控制任何已知和未知的 IoT 與行動裝置的網路存取權。今時今日的存取安全解決方案必須具備剖析、原則實施、訪客存取、BYOD 上線啟用及更多其他功能，才能提供 IT 卸載、強化的威脅防護以及增強的使用者體驗。

行動性和 IoT 正在改變我們對於網路存取控制 (NAC) 的認知

IT 領域的疆界現在已經延伸到企業的四面牆之外。企業的目標是隨時隨地提供連線能力，而完全不會危及安全性。IT 如何在不影響業務和使用者體驗的情況下維持可見性與控制權？有一個 3 步驟計畫可實現此目標。

1. **識別**正在使用的裝置類型、數量、連線來源位置，以及支援的作業系統 (此步驟可提供初步的基本資訊)。然後持續深入觀察變化，以及哪些裝置連入又退出網路，讓您隨時擁有必要的可見性。
2. **實施**準確的原則，以便提供適當的使用者和裝置存取權，而不用考慮使用者、裝置類型或所在位置；此步驟可提供預期的使用者體驗。公司必須適應當前不斷推陳出新的裝置及其用途，不論這些裝置是智慧型手機還是監控攝影機。
3. 透過延伸至協力廠商系統的動態原則控制和即時威脅修復**保護**資源。這是最後一個步驟。想要在凌晨 3 點因應異常的網路行為，需要一個統一的方法來封鎖流量並變更裝置的連線狀態。

公司必須針對現有和未預見的挑戰做出因應規劃。當使用者決定遠端工作或購買新的智慧型手機時，想要依賴 IT 和支援人員進行人工介入，無異於緣木求魚。NAC 不再只是用於在存取前對已知裝置進行評估。

在一個位置全盤掌握和管理

ClearPass 原則和 AAA 解決方案提供內建的裝置剖析、Web 型管理介面以及完備的報告和即時警示。運用所有收集到的環境資料，確保向使用者和裝置授予適當的存取權限，而不必考慮存取方法或裝置所有權。

內建的分析引擎會收集包括裝置類別、廠商，作業系統版本等即時資料。您再也不必猜測有線和無線網路上有多少已連線的裝置。精細的可見性提供通過稽核所需的資料，還能判斷效能和安全風險可能的出處。

CLEARPASS EXCHANGE 的強大功能

獨立式 ClearPass Universal Profiler 可以為尚未準備好全面實施政策的公司，或是一開始未部署 ClearPass 的遠端區域提供相同的分析可見性。

基於範本的政策實施可讓 IT 建置有線和無線導向的政策，這些政策可充分運用使用者角色、裝置類型、MDM/EMM 資料、憑證狀態、位置，以及星期幾等。只要使用原則，就可以輕鬆對員工、學生、教師、訪客、主管及這些人員決定攜帶的裝置實施規則。

ClearPass OnConnect 是一項內建功能，它可讓公司使用非 AAA 實施措施來鎖定這些數以千計的有線連接埠。不需要任何裝置組態，只需要在交換器中執行一條命令列命令。有線和無線亦支援標準 AAA/802.1X 方法。

這可實現一致的原則實施和端對端方法，而孤島式 AAA、NAC 以及很多原則解決方案都做不到這一點。在舊式解決方案之外，利用一項原則服務 (包括 Microsoft Active Directory、LDAP 相容目錄、ODBC 相容 SQL 資料庫、權杖伺服器和內部資料庫) 中儲存的多個身分識別來設定 ClearPass 的能力。

佈建裝置無需 IT 介入

管理個人裝置的載入以進行 BYOD 部署，不但會對 IT 和服務人員資源帶來壓力，也會形成安全隱憂。

ClearPass Onboard 可讓使用者自行架構裝置，以便能夠在安全的網路上使用。裝置特定憑證甚至能讓使用者不用整天重複輸入登入認證。這種便利性就是競爭優勢。使用憑證的額外好處是還能獲得安全性。

IT 團隊可以限定哪些人可以自攜裝置、可以自攜的裝置類型，以及每個人可攜帶的裝置數量。內建的憑證授權單位可讓 IT 在更短時間內支援個人裝置作為內部公開金鑰基礎架構 (PKI)，並且不需要後續的 IT 資源。

簡單且快速的訪客存取

BYOD 所指不只是員工裝置，而是所有其裝置需要有線或無線網路存取權的訪客。IT 需要一個簡單的模型來將裝置推送到品牌入口網站、自動佈建存取認證，並且還可提供能讓企業流量獨立運作的安全功能。

ClearPass Guest 能讓員工、接待員、活動協調員和其他非 IT 人員輕鬆且高效地每天為任意訪客人數建立臨時的網路存取帳戶。MAC 快取還可確保訪客輕鬆連線一整天，而不必在訪客入口網站上重複輸入認證。

自我註冊功能可讓訪客自行建立憑證，而不用由員工建立。登入認證會透過紙本識別證、簡訊或電子郵件提供。認證可以在設定的時間長度內儲存在 ClearPass 中，並可設定在指定的小時數或天數後自動失效。

裝置健全狀況決定存取權

在授權過程中，可能需要對特定裝置執行健全狀況評估，以確保其遵守公司的防毒、防間諜軟體和防火牆等政策。自動化可激勵使用者在連線到企業網路前執行防毒掃描。

ClearPass OnGuard 具有一項內建功能，可執行基於狀態的健全狀況檢查，以消除各種電腦作業系統和版本中的漏洞。無論使用的是永久性還是臨時性用戶端，ClearPass 都可以從中央位置識別無線、有線和 VPN 基礎架構上的合規端點。

可提供額外安全性的進階健全狀況檢查範例：

- 處理點對點應用程式、服務和登錄機碼。
- 確定是否允許 USB 儲存裝置或虛擬機器執行個體。
- 管理橋接網路介面和磁碟加密的使用。

藉由協力廠商解決方案發揮更大效益

ClearPass Exchange 允許您使用廣受歡迎的協力廠商解決方案 (例如防火牆、MDM/EMM、MFA、訪客註冊和 SIEM 工具) 來自動執行安全威脅修復或增強服務效能。透過利用 ClearPass 內含的環境智慧功能，公司可以確保在裝置、網路存取權以及流量檢查和威脅防護層級提供安全性和可見性。

藉由使用通用語言 (REST) API、Syslog 訊息和內建的儲存庫 (稱為 ClearPass Extensions)，自動化工作流程和決策有助於簡化工作並保護企業安全，完全摒棄複雜的指令碼語言和繁瑣的手動配置。ClearPass Extensions 允許合作夥伴上傳延伸模組，即時為共同客戶提供新服務，以實現更快速的整合。

使用 ClearPass Exchange，網路可以自動採取以下行動：

- MDM/EMM 資料 (如裝置的越獄狀態) 可以判斷裝置是否能連線到網路。
- 防火牆可以根據使用者、群組和特定裝置屬性準確地實施政策，並利用 ClearPass 修復行為不良的裝置。
- SIEM 工具可以設定為儲存所有已連線裝置的驗證資料。
- 可以要求使用者使用多因素驗證來證明確實是其本人連線到網路和資源。

網路事件還可以提示防火牆、SIEM 和其他工具，以通知 ClearPass 透過雙向方式觸發動作來對裝置採取行動。例如，如果使用者在網路驗證時失敗多次，ClearPass 可以直接向裝置觸發通知訊息，或將其列入禁止存取網路的黑名單。

隨時隨地安全存取工作應用程式

在一整天內登入工作應用程式必須既輕鬆又快速。為此，ClearPass 支援 SSO 和 ClearPass 自動登入功能。不同於每位使用者需要登入應用程式一次的單一登入，自動登入使用有效的網路登入資訊自動向使用者提供企業行動應用程式的存取權。使用者只需在其裝置上備妥網路登入資訊或有效憑證即可。

如果使用單一登入方式，ClearPass 也可以用作您的身分識別提供者 (IdP) 或服務提供者 (SP)。

Bonjour、DLNA 和 UPnP 服務

Aruba Wi-Fi 基礎架構上的所有使用者，都可以共用具備 DLNA/UPnP 或 Apple AirPlay 和 AirPrint 技術的投影機、電視、印表機和其他媒體應用裝置。ClearPass 可以讓使用者十分輕鬆地尋找及共用這些裝置。

例如，想要從平板電腦顯示簡報的教師，只會看到其所在教室中的可用顯示器，而不會看到校園裡其他地方的裝置。但他們可以使用入口網站來選擇誰可以使用顯示器，以避免學生操縱顯示器。

另一個例子是醫療保健領域，醫生可以輕鬆地將數位 PACS 影像從他們的 iPad 投影到醫院內任何地方的較大螢幕上，以便多位醫生共同研究病患的病情。

安全性與服務的適應性基礎

不論是為當今的行動使用者提供順暢的使用體驗，還是快速導入 IoT 技術，都帶來了許多新的 IT 挑戰。需要完善的規劃、使用正確的工具以及建置穩固的基礎架構，才能確保隨時隨地安全無虞地存取有線和無線網路。

ClearPass 利用一個緊密整合的解決方案，提供裝置身分識別、政策控制、工作流程自動化以及自動威脅防護，克服了這些挑戰。透過擷取並關聯即時的環境資料，ClearPass 讓您能夠定義適用於任何環境 (辦公室、校園或球場) 的政策。

最新的 ClearPass 增強功能也會處理因採用 IoT 引起的新興網路安全性挑戰，並且提供更強大的行動裝置和應用程式驗證，以及更深入地瞭解安全性事件。自動威脅防護和智慧服務功能可確保準確授予每部裝置應有的網路存取權限，將 IT 手動介入降至最低。

aruba
a Hewlett Packard Enterprise company
www.arubanetworks.com

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | 電話：1.408.227.4500 | 傳真：1.408.227.4550 | INFO@ARUBANETWORKS.COM