技術概要

支援動態分割技術的 POLICY ENFORCEMENT FIREWALL (PEF)

隨著企業網路催化數位轉型和連線能力的普及，我們需要新的政策執行和網路安全解決方案，才能解決傳統網路和安全防護方式所面臨的挑戰。在邊界不斷變動的公司無線和有線網路上，物聯網 (IoT) 裝置正在連結員工、客戶與訪客。套用標準規則的防火牆、基於 IP 位址的實體網路設定等標準防護方式，皆不再足以因應目前情況。

POLICY ENFORCEMENT FIREWALL (PEF)

新式的內部攻擊經過強化設計，能夠迴避並利用傳統安全防護機制的漏洞。這些攻擊通常會在網路中蟄伏數週或數個月，只為了在最出乎意料的時機解壓縮、嚴重加密資料，或是入侵 IT 資源。意外發生的時候，若IT 人員缺乏應用程式層級的掌控能力，則會直接影響網路效能和使用者體驗。

做為無線和有線網路領域的領導廠商，Hewlett Packard Enterprise 旗下的 Aruba 率先使用了全方位的邊緣式防護，包括軍事級加密，以及名為Policy Enforcement Firewall (PEF) 的專屬身分識別式存取解決方案。PEF 透過 ArubaOS 和 InstantOS 運行，相關技術已經證實有效，且**在全世界已安裝超過 400 萬份**。PEF 是唯一針對使用者和裝置的防火牆，能在AP提供「零信任」邊界。

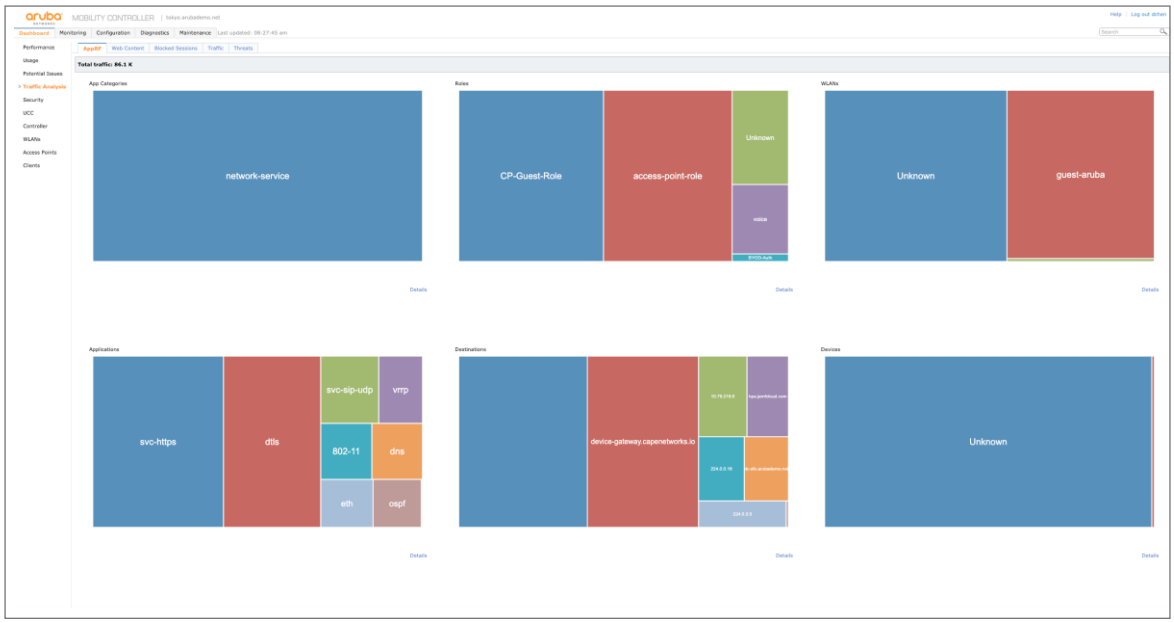
傳統防火牆運用 IP 型 VLAN 進行控制，只會在使用者或裝置受允許進入網路後才會啟用，留下易於遭到進階攻擊利用的破綻。與此不同，Aruba 的使用者和應用程式防火牆做法會運用 PEF，透過身分、流量屬性和其他情境，在初始連線時集中控制存取權限，藉此消弭弱點。由於攻擊者無時無刻不與網路連線，釋出數以千計的惡意軟體封包，因此我們務必要填補前述的空檔。

主要優點

- **集中式零信任存取**：減少初始網路連線和傳統防火牆執行間的空檔
- **Marsh 認可 PEF 符合其網路風險管理計劃 Cyber Catalyst℠**: PEF 降低風險的能力能協助企業獲得相關資格，在向特定保險公司投保時享有更好的網路保險保單條款
- **使用者和應用程式防火牆**：角色型存取控制可盡量減少設定錯誤
- **不需其他硬體**：PEF 可在現有的 Aruba 網路基礎架構上執行
- **提高效能**：包含硬體加速流量處理
- **自動化自我學習**：提供深入解析的網路和應用程式使用資料
- **可重複使用政策庫**：讓管理員輕鬆建立實用且一致的政策
- **獨立連線**：不論有線、無線還是遠端連線，使用者和裝置將持續使用指派給他們的角色
- **安全認證**：各種政府支持的認證

獲選為 Cyber Catalyst℠ 的解決方案

使用 Aruba 政策執行防火牆技術的組織可執行零信任存取模式，透過身分、流量屬性和其他情境，在初始連線時集中執行存取權限。由於動態執行安全角色型政策的技術和能力，Aruba 政策執行防火牆能夠有效降低風險，因此獲選為「Cyber Catalyst℠」。



ArubaOS 儀表板檢視：清楚掌控 3000 多個應用程式

簡單又安全的網路存取

PEF 也是讓動態分割得以進行的基礎技術。動態分割是 Aruba Experience Edge 內的關鍵技術解決方案，能簡化及保護有線和無線網路。透過使用者和應用程式控制，IT 人員可消除新增 VLAN、SSID 或 ACL 的需求，大幅降低複雜度。

PEF 的應用程式掌控功能，讓網路管理員能夠取得豐富的深入見解，瞭解網路中運行的應用程式，以及有哪些人在使用這些程式。WebCC 則是訂閱型的新增功能，可提供 URL 過濾、IP 信譽和地理定位過濾來強化 PEF 功能。

高強度驗證和角色型控制提供零信任防護

首先，系統會整合 Active Directory (AD)、RADIUS、LDAP、SQL 資料庫、LDAP 式身分儲存庫或來賓資料庫，藉此在網路登入流程期間驗證每位使用者或裝置的身分，並在建立身分後指派角色。角色即是權限的邏輯分組，其中包括應用程式存取權限和使用者或裝置間的通訊。

將使用者與角色關聯的價值在於，如果使用者的安全情境有所變更 (例如：裝置遭到入侵)，系統可立即指派受到更多限制的新角色，不必重新設定網路就能變更存取權限。

指派使用者或裝置角色後，系統會根據組織的防護優先順序套用政策。不論是無線、有線還是 VPN 連線，使用者使用網路期間將持續適用同一組政策。若裝置未在目錄中註冊，系統可根據已記錄指紋的裝置類型套用預設政策 (例如：「給予所有電視螢幕 DNS、DHCP 和網際網路型 HTTPS 服務存取權限，但不得存取內部資源」)。

已識別的使用者連線至由 PEF 管理存取權限的網路時，會在一開始被指派一個角色 (例如：「醫院人資管理員」)，並根據角色獲得一組 IT 權限。在本例中，管理員將只能存取其工作所需的工具和網路服務：電子郵件、Microsoft Office 和員工記錄，但無法存取病患的醫療資訊。若使用者遭到入侵，系統會自動套用並執行新的角色 (「可能入侵，傳送至隔離區」)。

因此，PEF 消除了困難且容易出錯的手動工作，不必決定及變更 VLAN 設定，就能提供精準而即時的執行功能。

另外，PEF 使用深層封包檢測技術，因此具備**第七層應用程式感知能力，能夠識別 3,000 個以上的應用程式**。因此，PEF 可在分隔流量時讓一個特定應用程式對應單一使用者或裝置，這是 VLAN 方式無法做到的精細程度。

豐富的應用程式可見度

深層封包檢測 (DPI) 技術提供豐富的應用程式可見度，可用於即時排除應用程式效能問題、設定全域政策，以及為未來成長做規劃。

內建儀表板可為 IT 人員提供簡單強大的功能，讓他們檢視行動應用程式使用和效能情況，並根據使用者角色、應用程式、網路和其他條件排序：

- **行動應用程式**：即使公司應用程式 (例如 Box) 和個人應用程式 (例如 Apple FaceTime) 在同一台行動裝置上執行，也能加以區分。
- **網路服務 (例如 Apple AirPrint 和 AirPlay)**：Aruba 可最佳化 IP 多點傳送視訊流量及自動優先處理服務，並新增政策控制。
- **網頁型應用程式**：許多網頁型應用程式使用相同連接埠用戶端通訊，並顯示為 HTTP 流量。Aruba 的技術可解析目的地位址，識別 Facebook、Twitter、Box、WebEx 和其他數百種獨特應用程式。
- **加密應用程式**：針對加密流量，Aruba 會透過啟發法找出流量模式，並建立專屬指紋以識別這些應用程式。

政策型流量管理和控制

PEF 功能控制可最佳化流量用量。角色型政策可限制特定使用者或使用者等級的頻寬使用量上限，並防止強大的使用者獨占網路資源。

在此同時，流量管理政策可為裝置保障最低限度頻寬，確保使用者能保持工作效率。PEF 可最佳化佔用效能的廣播和多點傳送流量，藉此提高應用程式效能。

PEF 也可徹底過濾其他佔用大量頻寬的通訊協定 (例如：mDNS、ARP 和 NetBIOS 廣播)，並限制其只能使用網路的特定區塊。

另外，PEF 提供全面的線上威脅情報，即時保護使用者和網路免受惡意檔案和 URL 威脅。政策可根據 URL 過濾、IP 信譽和地理定位 (WebCC 訂閱)，以及使用者角色或裝置使用情境來執行。

服務控制品質

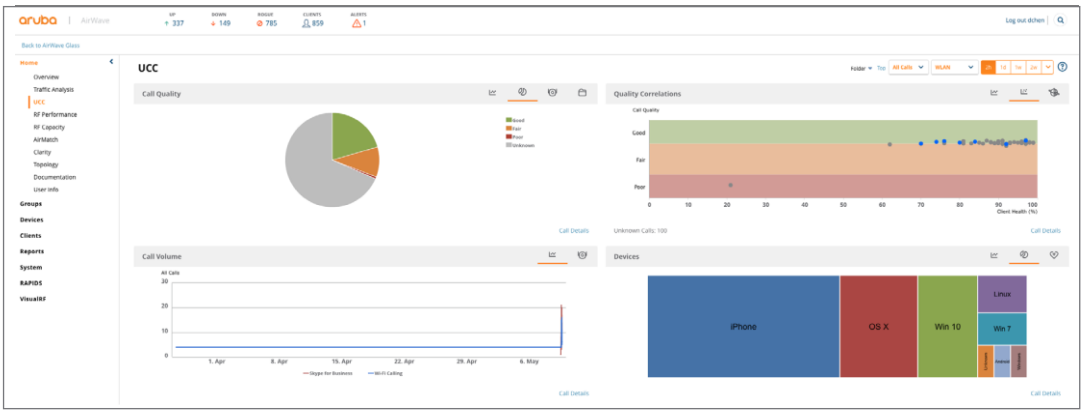
識別並視覺化處理行動應用程式後，系統即可套用存取控制和政策，藉此優先提高企業應用程式而非個人應用程式的效能。當行動裝置彼此競爭 Wi-Fi 頻寬時，PEF 可為您最重視的應用程式保障頻寬。

PEF 會最佳化 Apple AirPrint 和 AirPlay 等網路服務，自動優先處理 IP 多點傳送視訊流量，並自動識別及優先處理專屬 Apple FaceTime 流量，以及 Microsoft Teams 或商務用 Skype 等加密的語音及視訊工作階段。

另外，PEF 也可根據使用者、裝置和位置，優先處理網路中的 Pandora、Netflix、Google Drive、Citrix GoToMeeting、Salesforce.com 和 Dropbox 等一般網頁服務。

PEF 可將數種防火牆安全行動套用至流量，包括允許、中斷、記錄或拒絕。PEF 也可透過 802.1p 或 DSCP 標記標記封包，提高封包在多個佇列中的優先順序，並根據通訊協定將其重新導向至其他目的地。

進階語音及視訊協議感知能力可讓系統自動將適當的 QoS 套用至控制協定和通話工作階段。



Aruba UCC 儀表板檢視

PEF 可確保適當的優先順序對應至適當的通訊協定。例如，如果往來於一位使用者間的流量與相關的 QoS 語音設定不一致，該流量會被重新分類至適當的優先順序。

針對重要整合通訊 (UCC) 服務，可透過通話狀態和品質知識進行更智慧化的 VoIP 管理。人工智慧 (AI) 驅動的智慧功能，搭配 Aruba 的 AirMatch 和 ClientMatch RF 最佳化技術，可遏阻任何會導致活動中工作階段中斷的情況。

最佳化 UCC 體驗

Aruba 透過整合式 UCC 儀表板，以易於檢視的方式顯示多種 UCC 應用程式的重要通話品質指標。這些應用程式包括：Microsoft Teams、Microsoft 商務用 Skype、Apple FaceTime、Wi-Fi 通話、Jabber/Spark 和 SIP。

只要將游標暫留在儀表板上再直接按一下，您就能查看詳細報告和疑難排解資訊，例如電話號碼關聯、通話品質追蹤、詳細通話記錄 (CDR) 和通話許可控制 (CAC)。只要將游標暫留在儀表板上再直接按一下，您就能查看詳細報告和疑難排解資訊，例如電話號碼關聯、通話品質追蹤、詳細通話記錄 (CDR) 和通話許可控制 (CAC)。

儀表板中包括：

- 通話品質與關聯：這些圖表在「WLAN」索引標籤底下顯示 AP 和用戶端間的通話品質，以及在「端對端」索引標籤下顯示端對端品質，包括有線及無線通話階段。
- 通話數：此圖表根據 UCC 應用程式類型顯示總通話數。例如：SIP、Lync、SCCP、H.323、NOE、SVP、VOCERA 和 FaceTime。
- 裝置：此圖表依裝置類型顯示語音工作階段明細。例如：iPhone、OS X、Win 10 等。

高效能流量處理

PEF 讓您在執行時不必犧牲效能，也不需配備其他外部硬體。

Aruba 行動控制器是專為高速處理專用網路流量而打造，擁有可用於控制處理、網路流量處理和加密的專用硬體。

結果便是高速、低延遲的政策執行能力，最高可擴充至數千位使用者和數十萬個活動中工作階段。

外部身分驗證和授權介面

PEF 可更細緻地管理授權及驗證伺服器的使用者，並可啟用自動中斷網路連線、重新指派角色和動態更新防火牆政策等控制項。

此功能可透過兩種應用程式開發介面 (API) 啟用：IETF 標準 RFC 3576，以及簡單但彈性的 XML 型 API。兩種 API 均允許外部系統透過行動控制器運用使用者和政策控制項。

第三方整合介面 (syslog 處理器) 可接受系統外的 syslog 訊息，根據規則運算式規則語言處理這些訊息，然後可設定的行動，例如變更使用者角色或將使用者加入黑名單。

減少平均攻擊回應時間

透過避免 VLAN 型網路設定執行控制項的方式，大幅減少執行 IT 存取政策所需的資源，並可自動執行攻擊回應。

PEF 的細緻控制可有效阻止借用合法憑證，並耐心地擴散至整個網路的內部攻擊。當使用者或裝置只擁有較小範圍的存取權限時，攻擊者的存取權限也一樣會受到限制。這樣做可以遏制橫向傳播。

偵測到資料外洩或勒索軟體之類的攻擊時，PEF 可自動變更角色，藉此變更使用者或裝置的權限。系統可能採取多種行動來回應攻擊，包括降低頻寬、隔離，以及當場封鎖。透過簡易 API 整合，組織安全生態系統內的任何資安產品均可發出攻擊警報。

整合 ClearPass Policy Manager

政策執行防火牆是獨立式存取控制解決方案，可選擇與 Aruba 的 ClearPass Policy Manager 整合。ClearPass 提供簡化驗證和政策定義服務的功能，讓 PEF 能大規模集中執行。ClearPass 的關鍵優勢在於統合從個別辦公室到全球企業的驗證和授權存取功能。

ClearPass 也支援 140 多種 Aruba 技術合作夥伴解決方案的政策整合、角色執行和攻擊回應，這些解決方案包括行動裝置管理和 ServiceNow 等客服解決方案。

最高級的安全認證

Aruba 的Policy Enforcement Firewall (PEF) 在通用準則和 DoDIN-APL 方面獲得 NIAP 認證。PEF 也名列 NATO 的核准產品清單。

易於執行

為確保 IT 人員可輕鬆執行及保護他們的環境，PEF 可以 Aruba 作業系統 (AOS) 內獨立授權軟體選項的形式，提供給控制器型基礎架構，並包含在無控制器存取點授權內。PEF 也會透過動態分割提供給 Aruba 網路交換器。不需其他硬體。

總結

由於傳統防火牆在完成存取後才運用 VLAN 型政策執行，IT 團隊必須努力因應，才能抵銷自網路連線時即開始的攻擊威脅。Aruba 的使用者防火牆做法使用 PEF，是唯一專門在網路連線時，不問位置、連線方式或裝置類型，僅根據使用者或裝置身分和角色提供零信任邊界的存取控制解決方案。

透過 PEF 執行的精細存取權限，組織可在偵測到供即時，透過精準隔離及自動封鎖或隔離端點的方式，避免遭入侵的使用者和裝置參與攻擊。

由於 PEF 是作為現有 Aruba 網路基礎架構的軟體解決方案執行，因此不需要安裝其他硬體，就能確保只有已識別及經過授權的使用者和裝置能連線至網路。

功能摘要	
功能	**優勢**
完整狀態的第 4 至 7 層應用程式可見度	控制雙向資料流動，提供專屬的網路邊緣可見度和安全性
完全不影響效能	不會降低控制器的流量處理速度
使用者防火牆	允許為使用者、裝置類型、應用程式或目的地設定角色型政策
UCC 儀表板	檢視通話品質指標 (例如 MOS) 和 UCC 服務 (例如 Teams 和 SIP) 的健康情況
應用程式感知型 QoS	讓管理員能提高應用程式流量優先順序，以及控制 RF 層級行為
即時應用程式儀表板	即時追蹤重要應用程式、裝置和目的地，藉此監控網路或疑難排解
可重複使用政策庫	讓管理員輕鬆建立實用且一致的政策
歷史資料收集	使用 AirWave 長期掌握應用程式使用與容量規劃情況
ClearPass 和外部 RADIUS 整合	驗證使用者，允許第三方裝置或 ClearPass 執行詳細裝置識別和動態政策更新

Cyber Catalyst

做為 Cyber Catalyst℠ 計畫的一環，業界頂尖的網路保險公司會評估並識別他們認為能有效降低網路風險的解決方案。參與的保險公司包括 Allianz、AXIS、AXA 旗下部門 AXA XL、Beazley、CFC、Munich Re、Sompo International 和 Zurich North America。Microsoft 則是此計畫的技術顧問。

aruba
a Hewlett Packard Enterprise company

TB_PEF_090419 a00073442enw