技術白皮書

以 **Alcatel-Lucent Access Guardian** 進化網路安全

企業網路客戶在設計與部署安全基礎架構時，往往面臨各式各樣的困難與複雜度。解決方案必須具備完整功能與彈性，而且要與網路及最新威脅齊頭並進地成長和進化。Alcatel-Lucent 擁有豐富的系列工具與解決方案來協助企業網路客戶，其中之一就是 Alcatel-Lucent Access Guardian，它將驗證、設備規範遵循與存取控管等功能，直接整合在網路基礎架構的交換層級。接下來的內容將探討幾種常見的用戶安全挑戰，以及 Access Guardian 如何讓這些挑戰迎刃而解。

目錄

簡介

每個企業網路都有各自的安全需求。Alcatel-Lucent 有多種工具與解決方案，可根據客戶的需求來提供量身打造的網路安全。

下列範例探討客戶常見的安全需求及可行的解決方案。

"只有對的人才能存取我的網路"

圖 1.Alcatel-Lucent 內嵌式網路安全框架

驗證 • 員工：802.1x • 訪客：設限入口網 • IP 電話：802.1x 或 Mac 式 • 印表機：埠式	身分	OmniSwitch 內嵌式網路安全框架	完整度	**主機完整度檢查** • 整合式 HIC（CyberGateKeeper）靜態代理程式或隨需安裝代理程式
存取防護 • 監看/稽核追蹤	透明度		權限	**使用者網路資料檔** • 根據職務獲准存取，包含 VLAN、QoS、ACL
AQM • 隔離與矯正	隔絕		威脅控管	**傳輸異常偵測** • 零時差攻擊

以 Access Guardian 進行網路驗證

雖然網路驗證技術已存在多年，但在絕大部分企業網路的部署卻很受限。無線網路（WLAN；Wireless LAN）基礎架構的興起，已經改變了對網路安全的既有認

知。高漲的安全意識，再加上行動設備的普及，以及將驗證方法納入無線加密程序（WPA、WPA2）的整合，皆驅使網路驗證重回網路安全技術的最前線。

即使驗證機制已在 WLAN 基礎架構廣獲採用，但在有線網路的部署仍跌跌撞撞。舊式設備、缺乏驅動程式支援及其他相容課題，都限縮了使用者及設備存取網路資源的方法。Alcatel-Lucent Access Guardian 將數種驗證技術結合於單一且可客製化的彈性框架，並納入邊界交換機，讓現有的驗證系統從手動進化爲動態，有效解決有線網路的問題。

員工存取

實行驗證所面臨的最大挑戰，應該就是決定授權設備的身分。並非所有設備都有明確的終端使用者負責輸入憑證（例如：印表機、影印機、販賣機、相機與部分 IP 電話），因而必須有替代作法來辨識這些設備，這也成爲網路管理人員的額外負擔。

針對未內建查問式驗證（802.1X 或 Web 式驗證）等類似功能的設備，爲了讓網路可對其進行存取，只要使用 RADIUS 伺服器及合適的資料庫（例如：SQL），就能實行媒介存取控管（MAC；Media Access Control）。資料庫內含所有 MAC 位址，可擔負回應交換器的最佳角色。

收集及管理所有 MAC 位址是令人望而生懼的工作，但利用幾項工具則可有效加以簡化。Alcatel-Lucent OmniVista™ 2500 Network Management System 內含 Locator 程式，可用來圈記及儲存網路上所有 MAC 位址的資訊。再與供應商的 IEEE 製造商編碼（OUI；Organizationally Unique Identifier）及 OmniVista 2500 NMS 資料庫進行交叉比對，網管人員就能快速地辨識不同的設備類別，例如：印表機或 IP 電話。

辨識網路訪客則是一連串篩選過程的結果。當員工及其他已知設備通過 802.1X、MAC 或 Web 式驗證的同時，其餘所有設備皆會被視爲是全新及/或訪客設備。接下來，網管人員就能決定是否准許存取。如果准許存取，就使用 Web 式驗證方法，並根據回傳的個別職務角色來確保訪客有不同的存取權限及虛擬網路（VLAN）。

另一個有效控管的方法是提供訪客憑證，在前檯或訪客櫃檯使用簽入程序。對每一位訪客指定暫用的登入密碼，這些憑證可用來取得對網路基礎架構的有線及/或無線存取。

公共區域的訪客存取

Access Guardian 驗證政策是以埠爲制訂基礎。也就是說，即使同一個埠對使用不同 VLAN 或存取控管的各種設備開放連結，但驗證政策的組態是以埠來制訂。要准許公共或半公共區域如大廳、會議室等地的網路存取，這些區域裡的實體埠必須組態採用 Web 式驗證。這項改變不像其他驗證方法必須大規模推行，而且還能精準用於特定區域，但又無需導入全新的安全基礎架構。

“我想要控制使用者能存取的網路範圍”

以 **Access Guardian** 進行存取控管

Access Guardian 框架可讓網管人員透過網路基礎架構實行動態存取控管。使用者網路資料檔（UNP；User Network Profile）會在邊界交換器實行，提供一個方法來建立使用者群組與特定存取控管政策集之間的關聯。

存取控管以使用者身分、驗證或連接埠所在地，做爲依據基礎。要做到以所在地爲基礎的控管，只需指定合適的 UNP 給特定連接埠，接下來就連結至邊界交換器硬體裡的存取控管清單（ACL；Access Control Lists）。可與內部清單結合的端點數量並未設限，因此這項設計可延展適用於任何規模的網路。UNP 亦可判定邊界交換器（802.1X、MAC 式與 Web 式驗證）所採用的任何驗證格式。透過 ACL 清單與 UNP 的結合，群組使用者即可獲得特定的存取權限。謹記這項結合並未將 VLAN 或來源 IP 位址考慮在內。ACL 是根據站點的 MAC 位址來實行，而非考量它是特定 VLAN 或子網路的一員。

如此一來，就能爲個別客戶提供可橫跨整體基礎架構的相同 UNP 名稱；值此同時，VLAN 結合則保存在各個交換器的本端。舉例來說，名爲「工程師」的 UNP 部署在配備 VLAN 10 的某座建築物，而在另一座建築物的 VLAN 20 也有相同的 UNP。在每座建築物裡執行的是相同的 ACL，也簡化了驗證及 RADIUS 提供給邊界交換器的存取屬性。

Alcatel-Lucent 最新一代的邊界交換器支援八種不同的 ACL 清單，且能讓多種不同的 UNP 共享。例如：客戶想在遠端辦公室實行兩種存取控管機制，但不想因此建立多重子網路。只要在同一個 VLAN 組態兩種 UNP 就能滿足上述需求，再搭配不同的 ACL 清單，更可區隔各個使用者群組的存取。

判定合適的存取權限是極複雜的過程。要判定使用者可存取哪些 IP 位址，就必須結合多重工具。先從主機的內部連結清單著手是個好的開始（在 Windows 或 Linux 使用「netstat」指令）。然而，最建議的是使用網路分析器來監看網路設備，幾乎所有分析器都會建立連結表單，針對群組轉譯爲適用的 ACL。此外，在導入初期即可建立 ACL 來記錄網路傳輸。有效抓取及利用網路活動，網管人員就能得到未來分析可用的記錄。

"我要確保網路端點的安全"

以 Access Guardian 確保端點規範遵循

不論邊界交換器採用哪種驗證與存取控管，Access Guardian 都能落實端點的規範遵循。這項功能無需額外硬體或變更網路技術架構。

爲了落實端點的規範遵循，組態交換器必須與集中式主機完整度檢查（HIC；Host Integrity Check）伺服器，也就是 InfoExpress CyberGatekeeper 伺服器進行互動。接下來，確認指定給設備的 UNP 職務及核准資源，例如：特定伺服器或子網路。UNP 可隨來源埠、來源 MAC 位址範圍、來源 IP 位址或透過驗證而有所不同。

未獲得確認或未通過檢查的設備將被隔離。邊界伺服器只會讓它們存取事先定義的資源集，其他存取一律設限。如此一來，網管人員仍能以 SMS 或遠端通訊會期來存取隔離使用者，以進行機器的修復或更新。或者，網管人員也能開放網路特定區域的存取，並對其餘部分設限，直至使用者的設備通過檢查爲止。要限制網路存取，就要擴大「矯正伺服器」的範疇，納入可存取的子網路。綜合來看，已有四種明確的登入方式可供採用，每一種都有它自己的 IP 範圍與防阻。

結語

透過將驗證、設備規範遵循及存取控管功能直接整合於硬體的作法，Access Guardian 可強化 Alcatel-Lucent 邊界交換器系列產品的功能。以交換器爲基礎的安全功能，無需任何額外的設備，即可讓網管人員更有效地組態、管理及維運整體安全基礎架構。主機完整度檢查與使用者資料檔除可簡化網路，同時還能自動管理端點的安全適用性，以及限制未獲授權的使用者及設備的存取。藉由在交換器層級建立彈性且可客製化的安全基礎架構，Alcatel-Lucent 讓安全功能廣佈於網路的所有角落，亦讓入侵者無隙可趁。

縮寫

802.1X	以埠爲基礎進行網路存取控管的 IEEE 標準
ACL	access control list（存取控管清單）
HIC	host integrity check（主機完整度檢查）
IEEE	Institute of Electrical and Electronics Engineers（電子電機工程學會）
IP	Internet Protocol（網際網路協定）
LAN	local area network（區域網路）
MAC	media access control（媒介存取控管）
OUI	organizationally unique identifier（製造商編碼）
RADIUS	remote authentication dial in user service（遠端驗證撥入用戶服務）
SMS	short message service（簡訊服務）
SQL	structured query language（結構式查詢語言）
UNP	user network profile（使用者網路資料檔）
VLAN	virtual local area network（虛擬網路）
WLAN	wireless local area network（無線網路）
WPA、WPA2	Wi-Fi protected access（Wi-Fi 防護存取）

連絡資訊

Vincent Vermeulen（vincent.vermeulen@alcatel-lucent.com）
企業解決方案部門
Alcatel-Lucent

Sarveshwar Rao（sarveshwar.rao@alcatel-lucent.com）
企業解決方案部門

Alcatel-Lucent

參考資訊

使用者導向的安全性：http://www.alcatel-lucent.com/enterprise/security
網路安全：http://www.alcatel-lucent.com/enterprise/networksecurity