五、NAC零信任網路存取管控模組

零接觸佈署網路統一 NAC存取管控政策

ISOinsight 智能營運平台實現「零信任網路」架構「零接觸」之有/無線網路佈署，提供統一IP/MAC/主機名/身分微分段存取管控安全服務政策伺服器。她以多種面向操作保障IT/OT場域網路的存取管控安全， 提供四種面向詳述如下：**①交換埠零接觸佈署整合裝置MAC security (Layer 1)** – 主要目的：IOT物聯網關鍵設施保護與未授權使用，提供IOT設備與裝置MAC或MAC+IP保護機制，滿足中華民國「104年國家關鍵基礎設施安全防護指導綱要」之CI與CII定義八大領域法規需求。**②ARP enforcer – 固定MAC/IP綁定驗證 … (Layer 2)** –整合L3交換器在網路VLAN內佈署ARP probe以監聽/掃描偵測內網主機MAC or MAC/IP綁定合法授驗驗證、非法異常ARP攻擊偵測、用戶/外包商主機上下線與認證稽核記錄。**③ DHCP enforcer – DHCP MAC驗證 … (Layer 3)** – 針對有線設備或無線網路, 因應mobile非固定IP設備主機入網，使用本機內建DHCP server進行MAC(或MAC+靜態IP)合法裝置驗證, 適用DHCP網段。**④ Identity auth. – 有/無線身分基礎認證 (Layer 7)** – 因應mobile人員與設備身分的驗證與授權, 系統結合無線控制器提供多元的認證機制，提供員工BYOD設備認證與註冊、訪客臨時帳號與漫遊(iTaiwan, EDUroaming)的管理，本項功能需要airPASS延伸授權。

IT/OT場域基於角色基礎管控策略略

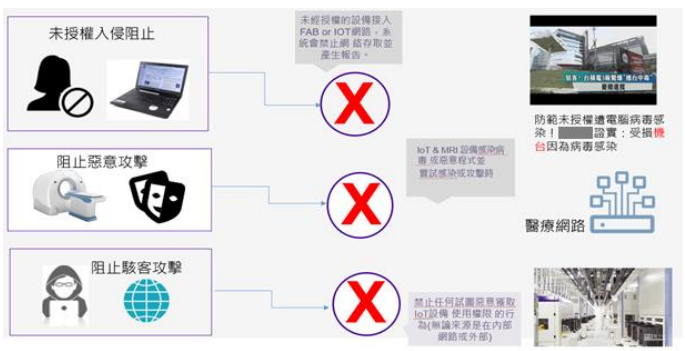
ISOinsight管控策略，基於角色的策略框架使網絡管理員能夠定義不同的操作群組角色或配置文件(profiles)，例如，系統管理員、IT/OT外包商、一般訪客). 每個定義的角色都被授予對特定網絡服務和應用程序的個性化訪問權限，當用戶接入或跨越有線和無線網絡訪問點時，這些訪問權限通過 IEEE 802.1X、MAC 地址或 Web 身份驗證進行身份驗證，並分配預定義的操作授權。實現**「零信任網路」**安全無縫接入認證與SDN細緻身分基礎網路定義微分段存取管控授權，管理員即可以輕鬆地從基本 VLAN 到復雜的 ACL 部署到角色的策略框架。

「零接觸」政策佈署

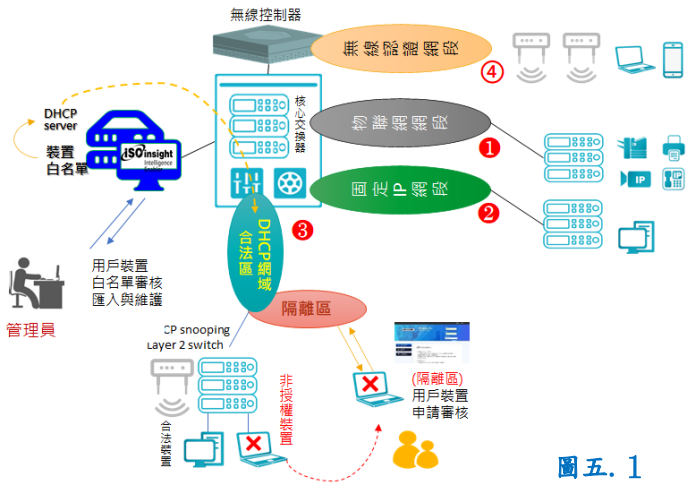
ISOinsight管理與統一安全管控政策伺服器整合交換器交換器或控制器介面管理允許將端口鎖定到給定的 MAC 地址並限制端口上的 MAC 地址數量以安全管理交換埠的使用， 此功能可用於將交換埠鎖定於特定主機或設備(例如 VoIP 電話或印表機)，並進行統一控管環境及參數設定與參數派送。

中央網路管理監控

搭配ISOinsight NMS及NPM管理授權，允許進行集中式管理拓樸監控，提供完整**FCAPS主網路管理**功能即時監測設備硬體、鏈路傳輸運作健康狀態，**效能管理**支援介面頻寬使用及介面/**IP**基礎流量分析、統計報表，**錯誤管理**則支援統一事件管理，集合異質設備或系統當發生異常或故障警報時，集中顯示事件異常內容及發生所在位置，**安全管理**支援統一管理權限具備資安 AAA 機制，並整合相關外部身分驗證協定(如:LDAP、OpenID 等)，並紀錄儲存各管理人員之操作程序。



圖五. 2



圖五. 1

實現多層次的安全防護：

Layer-1、阻止或限縮惡意程式攻擊

運用實體交換埠與微分段給與的權限限制，阻止或限縮IT/OT裝置因中毒引發之網路攻擊，本平台提供**Switch port交換埠介面管理**綁定功能，不只可以舒緩惡意程式攻擊亦可綁定授權裝置防止惡意的置換。

Layer-2、阻止未授權入侵

佈署ARP probe以監聽偵測內網是否有未授權主機入侵，平台提供**ARP enforcer – MAC or MAC/IP綁定驗證**功能，不只可以驗證入網主機的授權合法性，亦可偵測是否ARP廣播攻擊。

Layer-3、阻止駭客攻擊

配合機器學習裝置網路存取表，建置ACL Policy利用場域內Layer 3核心交換器存取管制表限制OT場域內機台/IOT物聯網裝置之連線路徑。

Layer-7、DHCP裝置認證、Identity auth.身分基礎認證

系統內建DHCP server服務可以啟動NAC網路存取管控模組授權，整合IP NAC 綁定管理加值管理，對合法MAC進行IP配發、非法MAC則進行隔離與告警等。

系統具備Identity身分基礎認證機制，針對有線端點或無線mobile裝置進行公有設備/員工BYoD/訪客/外包商角色帳號與密碼身分/802.1x登入認證、授權與操作記錄於管理平臺。