AINPB 內網 IoT 設備聯防模組

系統概述

AINPB–IoT 裝置之網路管理模組系統(L4 層以下)

建議售價：洽業務 sale@yesee.com.tw

主系統概覽

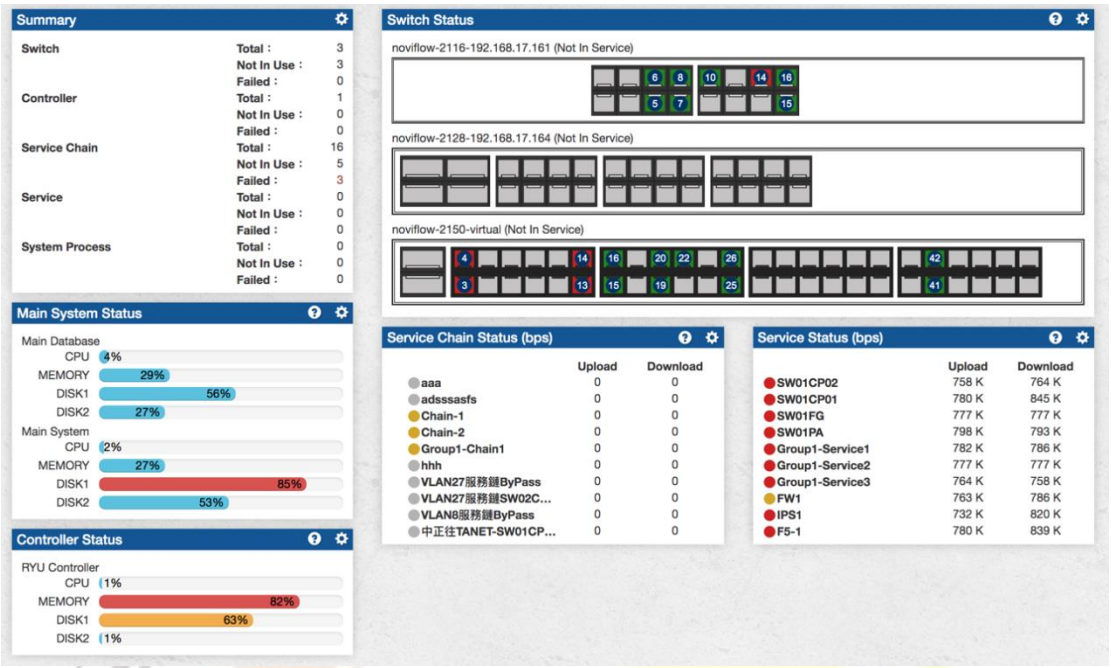
越世公司提供新一代 AI 高度自動化網路管理系統的主要架構上由一個主系統加任何多個選購功能模組(至少需要搭配一個功能模組)，可以搭配支援開放流交換機，實現功能模組的具體功能。

適用場景

◆ 有 IoT 設備被攻擊感染疑慮的環境，有開放流交換機使用的場域，統一管理開放流交換機，提高管理效率。

1. 提高管理效率。
2. 統一管理開放流交換機。
3. 統一管理管理者帳號。
4. 有清楚的登入記錄、操作記錄可以查詢。以有效降低現有資安設備，以避免因連線單位擴頻、流量爆增，造成暨有資安設備負擔過高的狀況。
5. 減輕資安設備的負載量。
6. 資安設備資源最佳運用。
7. 提高可承受的總流量或 Session 總量。
8. 避免主要幹線網路斷網過久。
9. 有 IoT 設備被攻擊感染疑慮的環境

易讀視覺化統計



本功能模組主功能(standard version):

1. 開放流交換機管理。
2. 管理人員帳號管理。
3. 操作記錄管理。
4. 登入記錄管理。
5. 儀錶盤介面管理。
6. 支援 100 組 IoT 結點保護設定。

IoT 設備防禦功能模組概覽

我們正處於一個資訊爆發的年代，網路的負載越來越大，使得網路出口流量日漸擴張，在舊有的網路架構下，當流量變大使得資安設備不敷使用時，解決方案往往是新購一台更大容量的資安設備，是基於 AINPB 架構下所研發的服務鏈機制，可透過政策的擬定，讓資安設備可以更有效的運用，讓各設備各司其職，避免不必要的流量流進設備，當設備真的不敷使用時，可保留原有設備並能讓加購的新設備同時使用，避免資源的浪費，此外透過自動修復機制修復異常設備，避免骨幹網路斷線過久，以保持骨幹網路的穩定性。

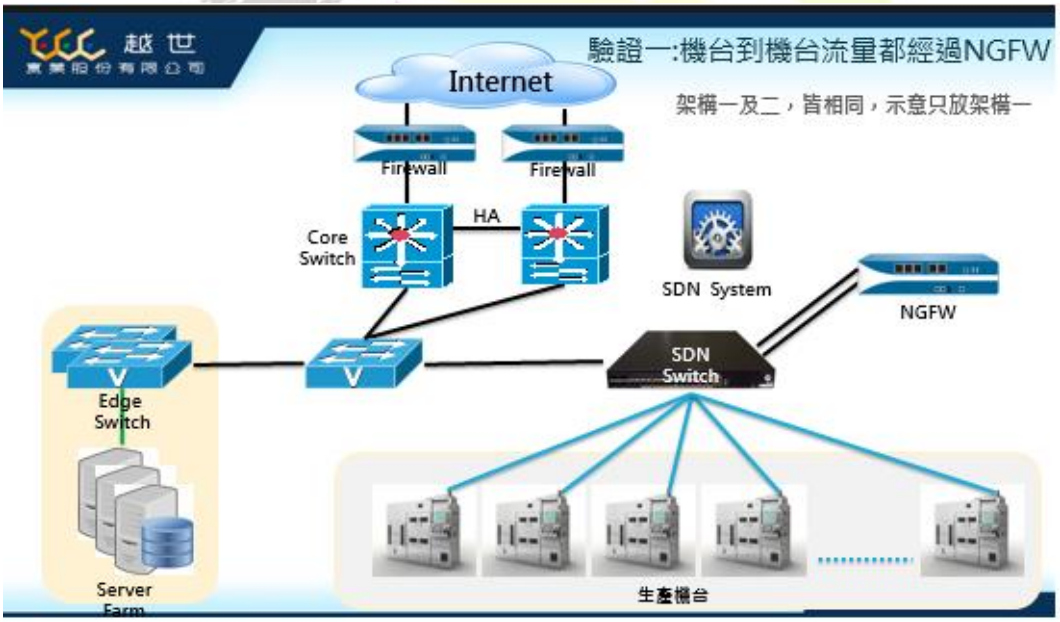
資源最佳運用

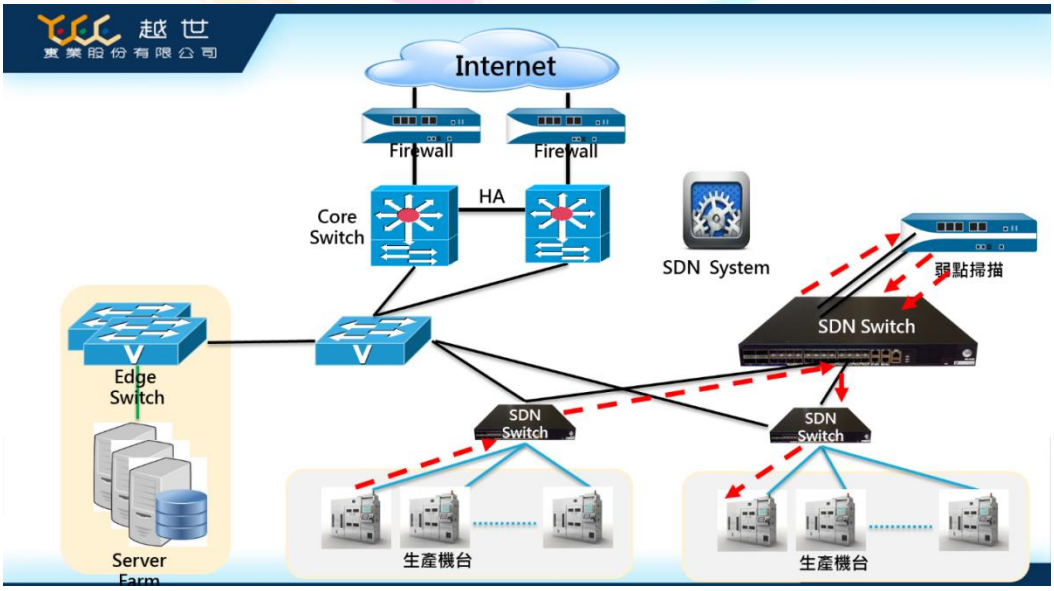
- ◆ 傳統的網路架構，各機器各司其職，資源的使用比重不一。
- ◆ AINPB 架構，網路設備只專注於傳遞封包，不做網路管理。

傳輸效率提升

- ◆ AINPB 的特色是修改了傳統網路架構的控制模式，將網路分為控制層(Control Plane)與資料層 (Data Plane)，將網路的管理權限交由控制層的控制器(Controller) 軟體負責，採用集中控管的方式。

網路架構概念圖





IoT 設備網路流量安全？IoT 設備網路流量不經過資安設備，互相感染？

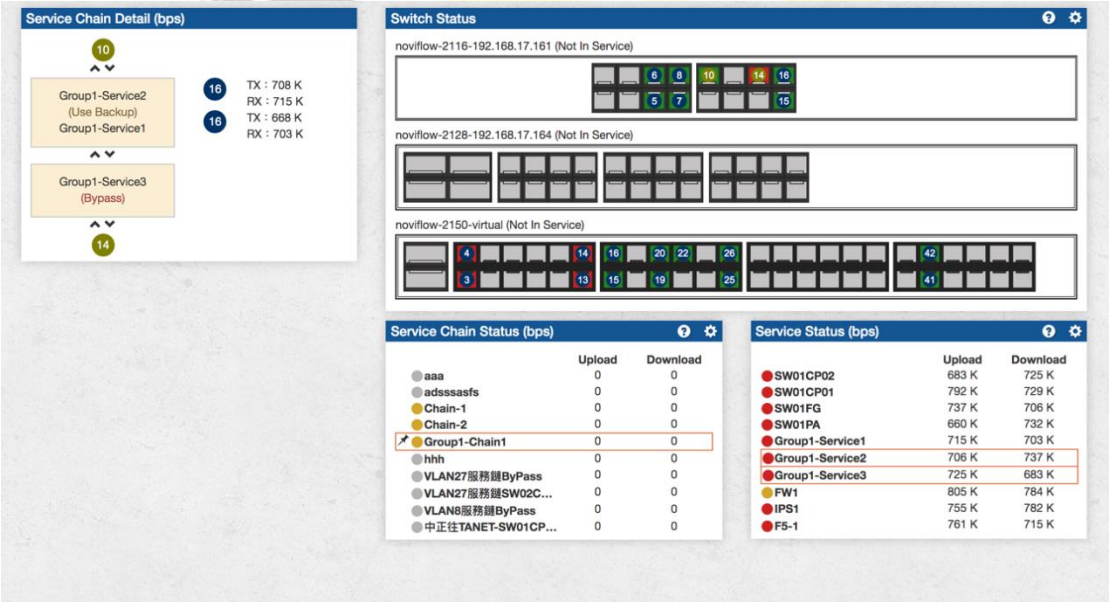
故障排查複雜，誰來做？設備故障後，更換困難？

資安設備投資龐大？內網安全需投入大量資安設備？

新產品、新功能測試困難？多用戶、多許可權、安全管理？

有限的視覺化程度？內網或 VM 之間交互流量難以處理？

易讀視覺化統計



IoT 設備防禦功能模組:(請敘述功能說明)

1. IoT 網路流量之東西向流量安全機制，可由單台或多台不同功能之設備組合而成。須考量不同網段，不同用戶，不用出口，不同入口等等的各式各樣節東西向攻擊，在內網發生造成網路流量中斷。
2. 支援資安設備池功能之智慧分流機制導出之流量，可同時支持 in-line 與 out-of-band 資安設備(IPS、Web filter 或防火牆等設備)。
3. 透過資安池機制，可自行調配將導入流量分散至多個不同的 In-line 資安設備上進行處理。

4. 具偵測資安設備、線路及分流機制本身之功能是否正常，如遇設備異常或線路不通之狀況，可自動 bypass 到其他設備或線路，以避免網路服務中斷。
5. 資安池須具備下列功能：
   ◆黑名單：有害或惡意 IP 網段(IP list、IP subnet 或 IP range)直接 drop 封包。
   ◆白名單：針對特定的信任網段(IP list、IP subnet 或 IP range)、視訊流(streaming)或通訊協定(protocol)跳過資安設備，直接進入到核心路由器(CoreRouter)。
   ◆可指定特定或未知網段、區域(IPsubnet 或 IP range)或通訊協定(protocol)，導流至指定的資安設備(IPS 或 FW)進行封包的檢測與清洗。
   ◆可導入網路流量數據並依過濾條件篩選後輸出，所有傳輸介面可按需求自行定義用途（流量導入埠或輸出埠），並需支援所有導入與輸出之流量，可依據使用者需求設定之。
   ◆介接之資安設備，可指定不同的規則，並可依不同設備順序，訂定不同之連續規則。規則條件至少具 MAC Source 或 Destination address、IP Source 或 Destination address、IP Subnets、Ethertypes、VLAN ID、TCP/UDP port number…等，其中 IP address 須同時支援 IPv4 與 IPv6。
6. 提供圖形化(GUI Interface)及命令列(Command-Line Interface)之管理方式。
7. 提供 Syslog 及 SNMP Traps 之告警能力，並須提供至少一種主動式告警通知的機制(如 email、簡訊、IM(Line、Message…)…等)。
8. 提供 Telnet 或 SSHv2 及透過 Console 埠等，多種方式進行管理。
9. 規劃之網路流量智慧分流機制，若為多項設備組合而成者，建議提供單一管理機制為宜，以方便該機制之管理與運作。
10. 未來擴充能力，未來當分流機制總 port 不敷使用時，可採購部份元件或設備方式，以利擴充上下行電路或資安設備。

本功能模組其它加強版功能說明:

1. Redundant 模組:

   主功能 Reduandan 模組，以避免設備異常造成網路流量中斷。主功能在控制器上具備 HA 的機制，可以在控制器有二個控制器資料同步，達到控制器不會有單點故障的問題。

2. CSC 功能:

   網路流量智慧分流機制支援 CSC，以避免設備效能不足需重新購買新設備，造成設備浪費。在相同功能的資安設備下，支援將相同功能的資安設備放進資源池，達到該功能之資源池多了一個設備的處理能力，網路流量智慧分流機制能將這個需要該資源設備清洗的流量，依管理者設定的政策分流到該資源池中各個設備清洗，達到資安設備效能不足時，可以並行添加設備，提高設備架動率。

3. HA 功能

   網路流量智慧分流機制設備 HA 或備援等機制，以避免設 OFS 備異常造成網路流量中斷。

4. By Pass 功能

   具偵測資安設備、線路及分流機制本身之功能是否正常，如遇設備異常或線路不通之狀況，可自動 bypass 到其他設備，以避免網路服務中斷。

5. 白名單功能

   支援管理者設定成白名單的網路流量可以將流量不導進管理者設定之資安設備，可以讓資安設備的使用率提高，不會執行無謂的檢查。例如：SSL 加密流量，在無解密封包時，不需要轉發到 IPS 設備，因為 IPS 設備無法解析被加密過的流量；此時，管理者可以設定加密封包無需流進 IPS 清洗，提供 IPS 的使用率；讓對的封包流到對的設備中。白名單支援 L2/L3/L4 等。

6. 黑名單功能

   管理者可以自行準備黑名單，黑名單透過主系統匯入，主系統會將黑名單寫入主系統所控制的開放流交換機，當開放流交換機收到流量中包含黑名單時，會直接將封包丟入黑洞。黑名單支援 L2/L3/L4 等。

7. 內網安全流量設定

   管理者透過系統設定內網資安設定。

8. 主功能可以控制開放流交換機數量。

   主功能在控制器可以控制開放流交換機數量授權。

AINPB Benefits for Customer：

◆AI 人工智能快速服務。

◆快速服務 - AINPB 相較于傳統網路可快速供裝服務，縮短服務開通的週期。

◆降低維運成本-AINPB 可確切的節約成本，提升網路使用效率和降低運營費用，更大的吸引力是由於提高了大型網路管理效率可有效降低運營成本。

◆減少硬體依賴- AINPB 可大幅降低服務供應商對於專用設備的依賴度，如特定的硬體設備才能達成特定的目的。通過應用 AINPB，可以節省大量的硬體支出，尤其可通過軟體的升級代替硬體的升級。通過軟體整合硬體資源能顯著降低。

◆靈活的安全性-相較于傳統式的安全性佈署方式，AINPB 可依據網路大小，靈活調整安全性規模，此外，AINPB 可定義資料的流向，將可疑的流量快速回復位向，用於加強安全處理，而這些處理需求可以避免對網路中的所有流量進行檢查。