中小企業專用
Next-Generation UTM
NU-860H

眾至Next Generation UTM網路安全設備具有高運作效能、多重安全防護機制及分層授權管理等特色，是中大型企業首選的網路安全及管理設備。NU-860H 具有新世代防火牆的強悍功能，包含以Deep Packet Inspection(DPI) 為基礎的應用程式辨識及管制、IPS、SSL解析與阻擋、Web Filtering、頻寬管理、防毒、垃圾郵件過濾及支援外部認證整合等功能，可以阻止駭客惡意潛入攻擊或未授權存取內部網路資源。亦支援雙機備援機制(HA)，可確保設備運作不斷線。

NU-860H打破傳統對埠口的限制，內建6個Giga埠，除1個埠為管理埠外，其餘5個埠允許管理者可自行定義(WAN、LAN或DMZ)。為了強化內網安全，NU-860H提供內網協防功能，可整合無線基地台(AP)跟網管型交換器，打造有線、無線一體的安全防護，讓管理者內外兼顧，並支援USB 2.0埠口。此外，ShareTech提供雲端管理機制，透過Cloud服務方式，單一介面直接監控UTM、交換器、無線基地台的運作狀態，任一設備發生故障，管理者就能在第一時間內知道並排除。

安 全

- 防火牆
- IPS入侵偵測
- 防毒(WEB/MAIL)
- Sandstorm惡意程式偵測
- 勒索軟體防護
- 垃圾信件過濾
- 協同防禦(交換器、無線AP)

管 控

- 頻寬管控
- 網站內容過濾
- 應用程式管制
- 上網行為管控
- 異常流量監控
- VPN管控
- 雲端管理服務
- SD-WAN管控

記 錄

- 郵件通聯記錄
- 威脅情報儀表
- 異常IP 紀錄
- Web病毒紀錄
- IPS 紀錄
- VPN紀錄
- 防火牆防護紀錄

企業網路閘道安全守護神

整合防火牆、DPI應用程式分類、防毒、垃圾郵件過濾、入侵偵測跟SSL的內容解析跟阻擋等功能，隨時做好APT防禦及阻斷Botnet等惡意程式入侵。

- **SPI防火牆技術，主動攔截、阻擋駭客攻擊，不論是DOS、DDOS、UDP Flood等攻擊方式都可以阻擋。**
- **網頁內容過濾(HTTP / HTTPS)**
- **IPS入侵偵測**
- **應用程式管制**
- **防毒 / 垃圾郵件過濾**
- **網路流量監控與協同防禦**

搭載Intel處理器 強化內對內管制行為

NU-860H搭載了4核Intel 處理器，6埠GbE 網路介面，整體提供9 Gbps防火牆效能及950 Mbps的VPN效能。

支援SD-WAN管制

傳統廣域網路功能會將分點的使用者連線至託管於資料中心伺服器的應用程式。一般使用 MPLS 專用電路確保安全和穩定的連線。但在新世代網路雲端環境中，此方法已不再適用。SD-WAN軟體定義廣域網路，除了可降低多站點部署的營運成本，也能改善資源使用情況。網路管理員可更有效率地使用頻寬，並為重要的應用程式提高效能，同時又不犧牲安全或資料隱私。

DPI(深度封包檢測技術)與應用程式控管與記錄

眾至研發之網頁應用程式防火牆技術，能針對網路瀏覽行為，檢測一般防火牆無法深入檢查的HTTP、HTTPS...等資料封包，作為補強傳統防火牆不足之深層防禦機制；達到有效防範機密被盜取，彌補入侵防護系統(IPS)不足。

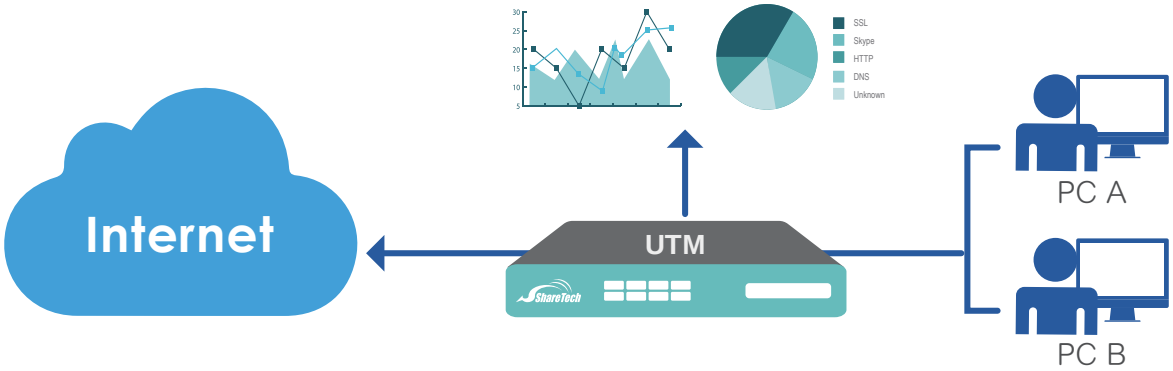
深度封包檢測DPI分析機制，可用來監視應用程式流量、分析應用程式以及協助網管人員挑選合適方法控管流量。DPI的封包層級分析能讓網管人員在問題影響使用者之前快速做出反應來解決問題。

- **支援多種類應用程式(包含網路協定、即時通訊、影音服務、P2P...等)**
- **細項控制：包含檔案傳輸、遠端控制、VOIP、網路遊戲、瀏覽器...等。**
- **SSL加密協定(HTTPS)監控**
- **Cloud資料庫更新**

威脅情報儀表讓資料往來一目了然

威脅情報儀表以Dashboard即時地反映網路的狀態，包含六大常見網路威脅、即時連線數、應用程式分類、使用最多網路資源的使用者、http及 https 流量跟防火牆的攻防等資訊，用動態圖表讓管理者掌握全部的網路狀態。

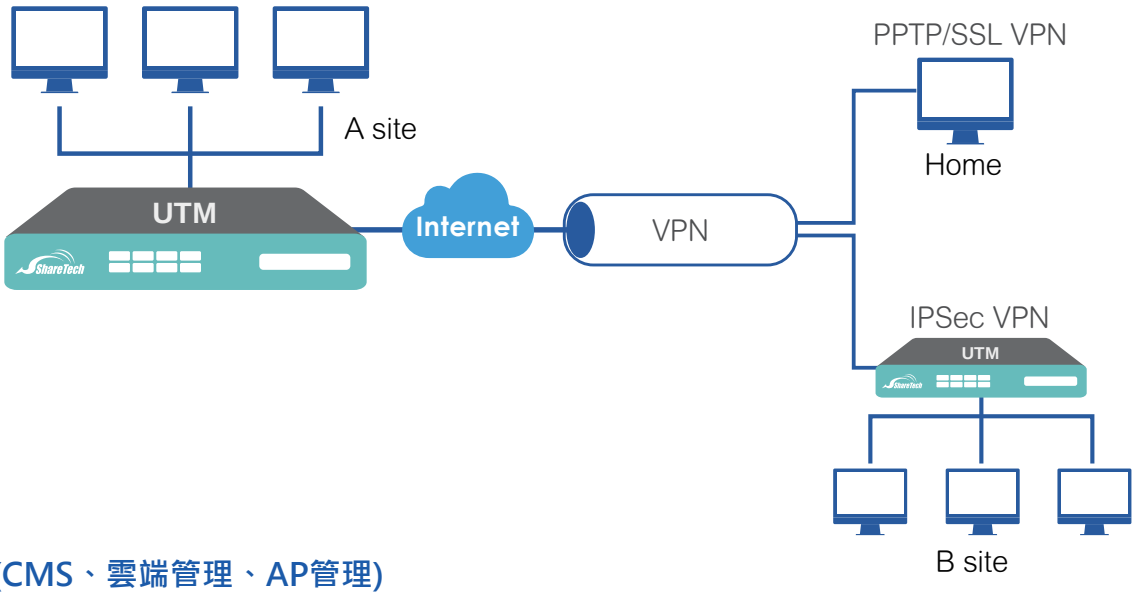
- 利用應用層 DPI 技術，從企業裝置、使用者和應用程式收集資料。
- 以單一介面、簡化除錯程序，優化使用者體驗。
- 取得網路可視性，透視即時連線、應用程式、郵件、防禦及網頁使用。
- 資訊整合效率高，分析即時與歷史資料，協助企業選擇最合適的解決方案。
- 資料可輔助企業自訂企業安全規範，掌握所有資安訊息。



完整VPN運用方案 (IPSec、PPTP、L2TP、SSL VPN、IP Tunnel)

提供IPSec、PPTP、L2TP、SSL、與 IP Tunnel 等VPN連線模式，可經由佈建於兩地間建立加密通道，具多樣化的加密方式，確保資訊傳輸的安全性。同時針對Tunnel間的傳遞封包進行管制，例如；限定Web、SMTP、POP3服務。

- DES、3DES、AES加密服務 SHA-1/MD5認證支援
- SSL VPN Client支援 (Android / IOS)
- 支援Auto VPN Server & Client
- 透由中心端直接管控分點網路服務



中央控管 (CMS、雲端管理、AP管理)

具CMS中央管理功能，方便管理者由中控平台遠端監控、啟動、重新啟動與管理裝置，可同時監控多台UTM設備。為了便利管理散在各地的UTM，眾至推出雲端的中央控管平臺(Eye Cloud)，IT管理員只要登入雲管理平臺，可統一監看所有 UTM 設備，也包含內部的無線基地台跟交換器的即時狀況。中央管控設備可以管理不同的佈署、提供完整檢視與分權遠端管控等簡化管理作業，大幅降低企業營運成本。

一、功能說明

兼顧優異效能與進階功能

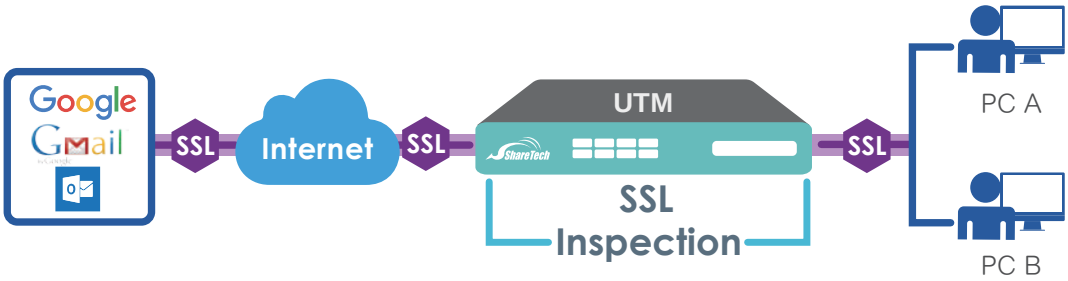
硬體平台精心採用X86硬體設備，目的是為了讓企業用戶都可以充分感受到UTM所提供的安全防護功能。針對高連線能力需求的客戶，提供高效能安全模組，以提高連線能力，並支援USB快速還原機制。

IP v4 / v6 雙頻技術

整合IPv4/v6趨勢，同一個網路接口，不管它被定義成 WAN 或是 LAN，都可以同時綁定v4或v6的IP地址，所以不管是在純v4的環境、v4/v6 混合、純v6 的環境都一樣合用。

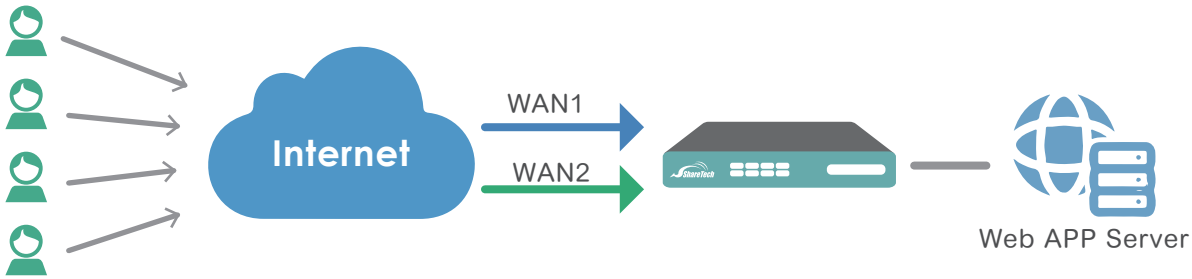
SSL加密連線檢測

具備檢測 SSL 流量的能力，當面臨到 SSL 加密連線的流量時，可應用入侵偵測防禦、閘道防毒、內容過濾與應用程式頻寬管控等功能。



負載平衡

以多種負載平衡演算法則，提供Outbound和Inbound雙向負載平衡機制，當其中一條線路斷線之後，所有的網路封包會自動轉向另一條正常的線路，確保內部的用戶網路暢通，當線路恢復之後，封包又會自動分配。企業可依需求自行設定負載平衡規則，而網路存取可參照所設定的規則，執行網路流量負載平衡導引。演算法則有：自動分配、手動分配、依來源IP分配、依目的IP分配。



IPS 入侵防禦

IPS它會檢查對應到OSI模型第4到7層的內容，是否有惡意的攻擊程式、病毒，隱藏在 TCP/IP 的通信協定中，透過詳細的內容檢查後，符合條件的特徵碼就會被標示出來，一旦發現後能夠即時地將封包阻止，讓這些穿過防火牆的惡意封包無所遁形。

威脅偵測防禦

提供企業最完整的縱深防禦機制，現今網路的攻擊行為不能只依賴單點防護而需要完整的縱深防禦，藉由不同層面的防禦技術才有辦法降低企業可能遭受的潛在威脅行為。除了提供防火牆、入侵偵測系統(IPS)、防毒做為企業資安防護基礎外，並可針對流量、網頁與郵件，加強惡意程式的偵測，藉由不同安全機制的關連分析，發揮縱深防禦的功效。

郵件閘道防護

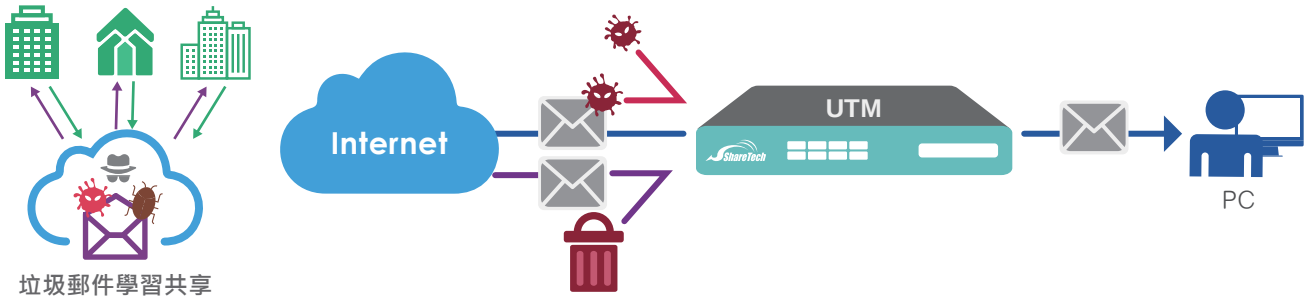
若企業已有郵件主機，但對垃圾信過濾效能不滿意，可將新世代UTM當作閘道安全設備，補原來郵件伺服器不足的功能，如垃圾郵件過濾、病毒信過濾、郵件稽核(選購)等功能。會再過濾完病毒及廣告郵件後，將乾淨的郵件傳送到郵件主機。

病毒信過濾

系統免費提供Clam AV防毒引擎，可偵測數百多萬種以上的病毒、蠕蟲、木馬程式，可對電子郵件自動掃描病毒，每日自動透過網際網路更新病毒檔，並提供病毒郵件搜尋條件。管理者可自行設定中毒郵件處理方式，包含自動刪除、中毒郵件副檔名儲存與中毒郵件通知信主旨。新世代UTM內建一年卡巴防毒引擎，客戶可選購續享掃毒率最高、病毒修復最強的卡巴斯基防毒引擎領導廠商。

垃圾信過濾

內部郵件或外部郵件都可以過濾，並提供ST-IP網路信評、貝氏過濾法、貝氏過濾法自動學習機制、自動白名單機制、垃圾信特徵過濾與指紋辨識法等，並有黑、白名單比對和智慧型辨識學習資料庫（Auto-Learning），甚至可以設定個人化規則，彈性制定過濾規則，處理垃圾郵件，無誤判確保全面性防護，準確率達95%以上。能進行郵件內文過濾，將符合管理者設定過濾條件的信件，執行轉送、刪除、阻擋等動作。並加入「垃圾郵件學習共享」機制，確保企業擁有最新更高偵測率與最低誤攔截率。

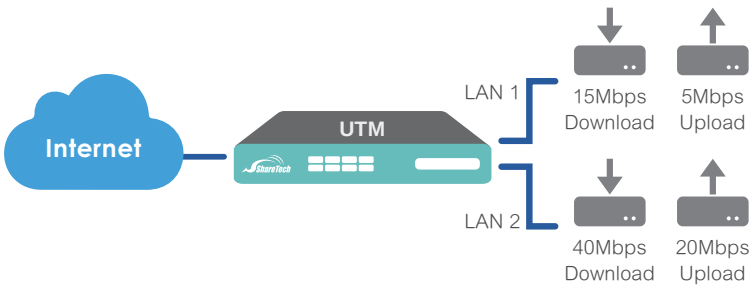


異常 IP 分析

不論使用者執行哪一種軟體，從網路封包的角度，大致分成上傳、下載的連線數量、流量(Flow)跟持續時間(Time)，藉由偵測這些數量的組合，推估使用者是正常使用網路或是有異常的行為。當發現內部使用者異常行為後，管理者可以採取多種策略，例如，阻擋上網、立即限制它的最大頻寬、啟用協同防禦機制通知交換器將它封鎖或是通知管理者就好。

頻寬管理(QoS)

協助網管人員控管網路流量，有效的減緩企業網路的阻塞、提升服務性與頻寬使用率。具有QoS(頻寬管理)功能，可將有限的頻寬分給所有使用者。與一般頻寬管理器的差異是，UTM除了可以提供最大頻寬、優先順序管理之外，還具有保證頻寬功能。並且還具有個人化頻寬管理之設計，可針對個人使用者做頻寬管理之設定。若頻寬管理搭配個人化頻寬管理使用時，可將頻寬管理功能所預留的頻寬，再分配給企業下面之使用者，可有效防範頻寬被使用者獨占之現象。

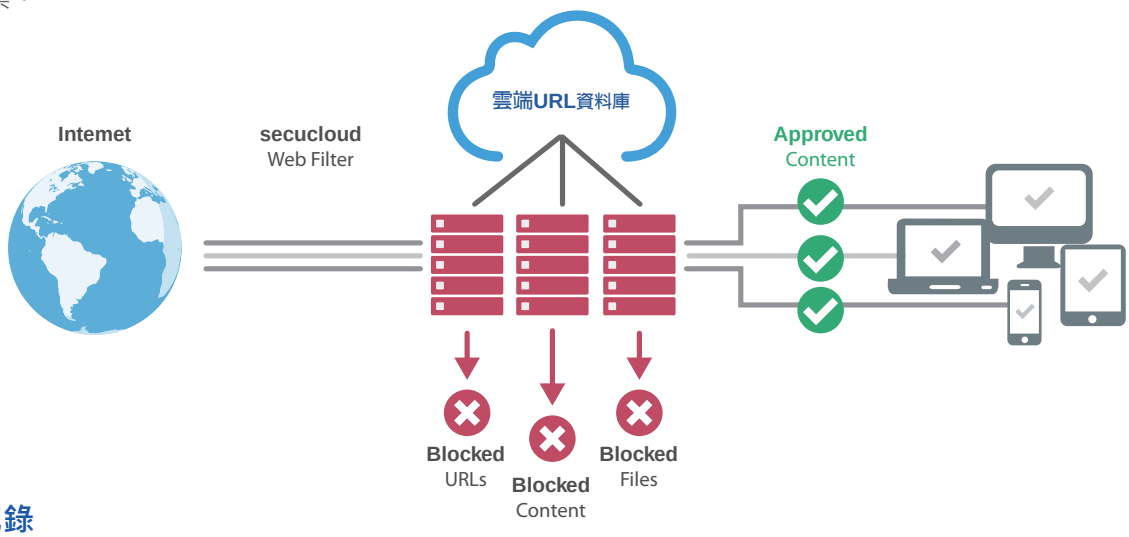


內容過濾

提供Web Filter(網頁過濾)功能，能阻擋工作端存取不當網頁(如色情、暴力)和攻擊性網頁(如駭客、病毒)，且能自設過濾條件，阻擋不當網站。

URL資料庫管理

進階眾至「URL資料庫」自動將網頁分類，管理者只要針對有害的URL網址進行防堵，可以輕鬆管制，不需要再逐一輸入網站IP位址、關鍵字....來阻擋。任意點選有害的URL　網址是罪惡的淵源，最好的防堵方式是禁止使用網路，如果無法全面禁止，使用時時更新的URL 資料庫就是最好的防護機制。新世代UTM內建一年URL 資料庫更新，客戶可選購續享即時更新或選擇免費方案。



上網行為全記錄

有部分企業員工，在上班時間上網，做非工作用途的事情，聊天事小，洩密事大。新世代 UTM除了可以限定使用者相關應用程式使用的權限外，還可記錄相關上網行為動作，包含瀏覽網頁與郵件收送。當企業發生洩密事件時，這些被保存下來的資訊，就是拿來當作呈堂證供的最好證據。

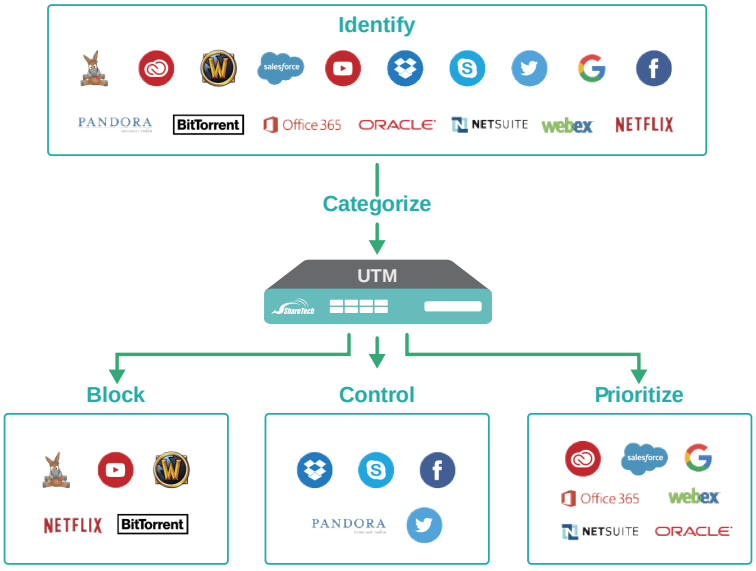
流量分析

提供流量分析利器，不論是內部使用者電腦開關機狀態、網路流量即時顯示、通訊協定分配及流量排行榜，當線路滿載時，可以馬上找出流量兇手。

應用程式管理

各種網路應用軟體不僅管理不易，更容易成為資料洩密、病毒攻擊的最佳管道。新世代UTM內建多種應用程式管理功能，包含P2P軟體、VPN與遠端控制、影音服務、VOIP、網路服務、資料共享與儲存、網站服務、社群網路、即時通訊、系統與更新、新聞媒體、購物拍賣、娛樂與藝術、運動與旅行、飲食、金融保險、賭博與色情、遊戲等等，可輕鬆控管員工使用應用軟體之權限，保護企業網路安全。

內建一年URL 資料庫更新，客戶可選購續享即時更新或選擇免費方案。

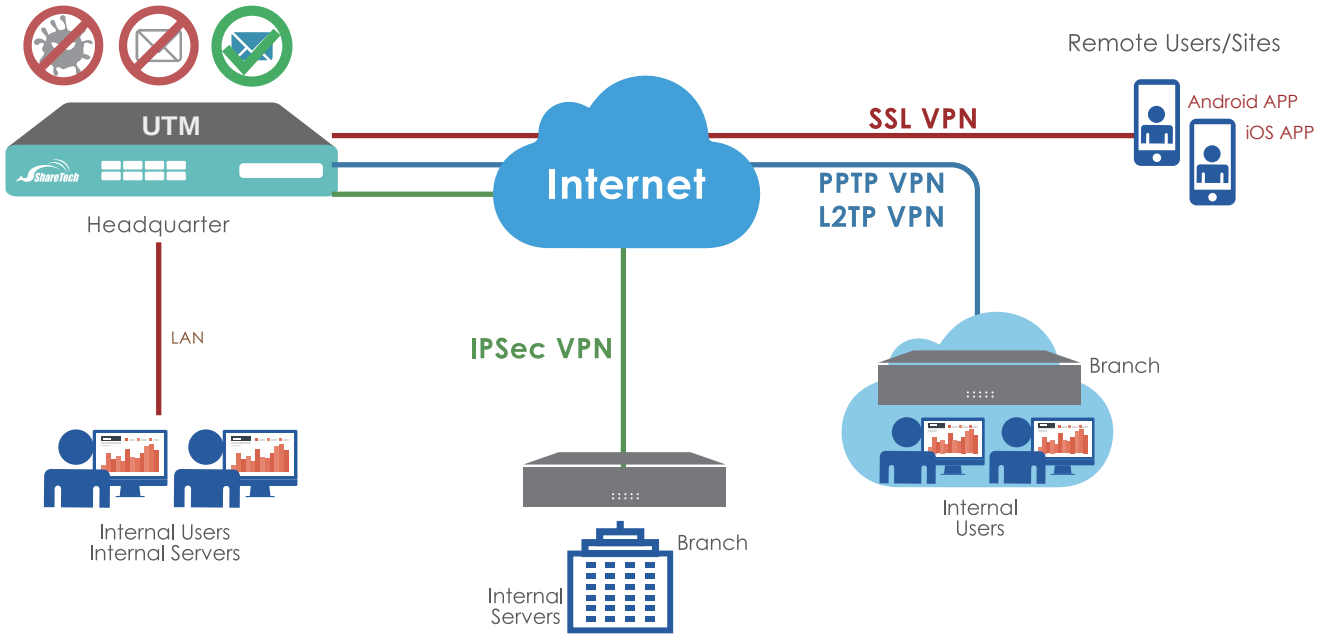


圖形化流量報表

提供WEB介面的流量報表，將系統歷史狀態繪成圖表，讓管理者可以很隨時掌握目前系統運作狀態，例如：系統狀態圖表(包含CPU負載圖、記憶體負載圖、系統負載)、網路流量圖表(LAN流量、WAN1~WAN6流量與DMZ流量)，並提供查詢條件可以快速搜尋各流量狀態歷史紀錄。

VPN功能

使用IPSec、PPTP和SSL VPN安全的進行Site to Site、Point to Site和遠端使用者之間的連線。透過這些VPN的機制方便使用者可以從不同的位置，包括家中、外部公共資訊服務站、網際網路，連結到不同的設備像是筆記型電腦、分公司辦公室、營業據點、行動通訊設備或家中...等。SSL VPN是目前多數企業、客戶與合作夥伴之間最重要的遠距安全傳輸連線。



Sandstorm惡意程式偵測

ShareTech Sandstorm 防護機制可以有效偵測未知的進階惡意程式附檔 (如常見Microsoft Word、Excel、Power Point或PDF)、針對性的釣魚郵件(phishing)、與壓縮檔(常見的ZIP與RAR)。若使用者誤點惡意網址或郵件附檔含有惡意程式，Sandstorm 會自動比對並進行阻擋。NU系列提供 File Hash、Web URL、Domain、IP 四種類型的比對，並提供雲端測試掃描分析，讓郵件潛藏的惡意連結和惡意附檔現形。

WAF網頁應用程式防火牆

WAF (Web Application Firewall) 專門處理網頁上的流量控管，包括對用HTTP/HTTPS協定的強化、異常連線的過濾。在企業尚未確認或改善網站的安全性之前，拉起一道防護網保護內部主機。讓網站主機免於常見的網站攻擊，如XSS跨網站指令碼攻擊、SQL隱碼注入、Remote Command Execution 執行遠端命令等常見的多種網站入侵行為。

二、特色與效益

特色	效益
威脅防禦 (Anti-Virus / IPS / SSL流量檢測)	1.提供Clam AV防毒引擎，資料庫達百萬筆即時更新，不需年費 2.內建一年卡巴防毒引擎 3.提供IPS資料庫，特徵碼高達數萬筆，定期更新維護 4.IPS 特徵資料庫會依照危險程度分為高、中、低三種 5.具備檢測SSL流量的能力
防火牆防護(Firewall)	1.主動攔截、阻擋駭客攻擊，不論是DOS、DDOS、UDP Flood攻擊都可阻擋 2.QoS，提供保證頻寬、最大頻寬、優先權 3.可限定內部來源IP與外部來源IP使用頻寬量 4.提供IPv6 & IPv4運作雙架構 5.具備Load Balance負載平衡功能(對外/對內/群組) 6.提供DNS伺服器服務與DDNS服務
潛在風險偵測(Flow Analysis)	1.提供異常IP分析，偵測Session量、上傳/下載流量 2.可針對異常流量進行通知、阻擋與記錄 3.結合交換器，可進行內網協同防禦與POE排程設定 4.阻擋ARP欺騙 5.提供交換器拓樸圖
郵件安全管理(Mail Filtering)	1.提供多層垃圾郵件過濾機制，包含貝氏過濾、自動學習、灰名單、指紋辨識、黑白名單等。 2.提供郵件內文過濾與垃圾信特徵過濾 3.垃圾郵件學習共享 4.可選購郵件稽核過濾設定、進階設定與過濾隔離區。 5.提供Client端垃圾信搜尋Web介面 6.可以對所有進出信件做稽核，可執行隔離/刪除/IP封鎖/副本抄收動作。 7.提供郵件記錄查詢
應用程式識別(App & Database)	1.提供多類應用程式管制，支援P2P軟體/VPN與遠端控制/影音服務與VOIP/網路服務/資料共享與儲存/網站服務/社群網路/即時通訊/系統與更新/新聞媒體/購物拍賣/娛樂與藝術/運動與旅行/飲食/金融保險/賭博與色情/遊戲等等。 2.管理者可自行藉由Policy進行控管 3.內建一年應用程式管制資料庫更新
惡意網址過濾(URL & Database)	1.提供URL過濾條件與資料庫管制 2.可自行設定URL過濾條例 3.URL黑白名單，系統管理員可透過完整網址功能、關鍵字，進行管制。 4.內建一年URL黑名單資料庫更新
使用者識別(Radius)	1.提供本機與整合POP3、Radius、AD 2.可自訂使用者群組 3.執行網路訪問策略控制 4.提供相關認證記錄與認證連線狀態
上網行為全紀錄(Content Record)	1.記錄所有進出之郵件 2.郵件記錄格式為eml檔 3.今日網頁瀏覽紀錄與查詢 4.今日網頁病毒瀏覽紀錄與查詢
負載平衡(Load Balance)	1.打造不斷線網路環境 2.提供Outbound/Inbound負載平衡 3.提供自動分配、手動分配、依來源IP分配與目的IP分配負載平衡模式 4.內建 Smart DNS Server

特色	效益
VPN安全連線	1.支援Windows VPN用戶端 2.支援IPSec Tunnel，並可管制Server和Client端 3.支援IPSec、PPTP、L2TP VPN、SSL VPN安全連線與記錄 4.可針對VPN連線進行管制，並支援VPN備援、Auto VPN
頻寬管理(QoS)	1.獨特QoS機制 2.具有保證頻寬與最大頻寬限制 3.可限定內部來源IP與外部來源IP使用頻寬量 4.提供優先等級
運作模式	Routing、NAT
威脅情報儀表與日誌 (Dashboard & Logs)	1.可選購威脅情報儀表，提供常用威脅統計、APP分析、郵件分析圖表、IPS分析、WEB分析、防禦分析、即時動態session分析與報表。 2.提供多項日誌，如登入/出日誌、安裝精靈、系統網路設定、管制條例與目標、網路服務、進階防護、IPS、郵件管理、內容記錄、VPN等與詳細的日誌搜尋系統。 3.供除錯分析、系統效能的評估以及被非法入侵時的證明與追查依據
虛擬伺服器(Virtual Server)	支援虛擬伺服器，不透過任何交換器或路由而將一個埠的所有通訊流傳遞到另外一個埠。
HA雙機備援	亦支援雙機備援HA服務機制
CMS中控管理	1.管理多台防火牆與AP設備 2.支援CMS Server & Client 3.提供即時監測、維護與管理 4.可整合Eye Cloud雲眼管理系統
電子白板	等同電子公佈欄，利於企業利用網路對所有員工作即時政策宣導
網路檢測工具	提供Ping、Trace Route、DNS Query、Port Scan、IP Route、Interface Information、Wake Up、SNMP等等檢測連線工具
系統管理(System Management)	1.Wizard快速安裝精靈 2.管理者權限管控與密碼自訂規則。 3.硬體CPU服務中斷設定 4.提供HTTPS、HTTPS網頁管理 5.提供系統備份、韌體升級、自動備份、韌體下載記錄。 6.具重新啟動系統與關機功能 7.UPS不斷電系統 8.具有VLAN 802.1Q功能 9.支援靜態路由、動態路由(RIPv2、BGP)、動態路由列表。 10.支援DDNS服務、DNS伺服器、SNMP服務。 11.支援遠端記錄伺服器 12.支援DHCP Client & Server 13.多因子認證機制，強化管理者、本機使用者、POP3使用者、SSL VPN使用者連線登入安全。
其他	1.提供自主化管理介面，繁體、簡體中文、英文語系。 2.網路區域設定可定義埠為LAN、WAN、Bridge、HA。 3.定時硬碟檢測與修復 4.資料自動備份與顯示資料空間狀態 5.LCM顯示板 6.支援1組 LAN Bypass 7.韌體免費升級 8.支援雲端、USB離線兩種特徵碼更新機制。

三、技術規格

	NU-840	NU-840H	NU-860H	NU-860T
硬體規格				
架機高度	1U	1U	1U	1U
建議使用人數	100人以下	100人以下	200人以下	300人以下
網路介面	6 x Gigabit	6 x Gigabit	6 x Gigabit	6 x Gigabit 2 x 10G SFP+
自定義埠	5	5	5	7
USB	3.0 x 2	3.0 x 2	2.0 x 2	2.0 x 2
LAN Bypass	x	x	•	•
電源耗瓦數	65W	65W	120W	120W
處理效能				
防火牆最大處理速度	4.2 Gbps	4.2 Gbps	9 Gbps	15 Gbps
最大同時連線數	2,000,000	2,000,000	3,000,000	3,400,000
每秒新增連線數	65,000	65,000	100,000	120,000
郵件掃描封數/天	3,100,000	3,100,000	4,800,000	5,200,000
防毒效能	750 Mbps	750 Mbps	950 Mbps	950 Mbps
IPS效能	750 Mbps	750 Mbps	1 Gbps	1 Gbps
VPN效能	650 Mbps	650 Mbps	800 Mbps	850 Mbps
VPN通道數				
IPSec VPN 通道數	2,000	2,000	3,000	3,000
PPTP/L2TP/SSL VPN 通道數	600	600	1,200	1,200
IP Tunnel 通道數	300	300	600	600
網路安全防護				
防毒引擎	Clam AV	Clam AV	Clam AV	Clam AV
卡巴斯基防毒引擎	選購	選購	內建一年	內建一年
IPS防禦與資料庫	•	•	•	•
Sandstorm惡意程式過濾	•	•	•	•
垃圾郵件過濾&垃圾郵件學習共享	•	•	•	•
郵件稽核	選購	選購	選購	•
進階URL管控與資料庫	內建一年	內建一年	內建一年	內建一年
進階APP管控與資料庫	內建一年	內建一年	內建一年	內建一年
WAF 網路應用程式防火牆	•	•	•	•
Geo IP 國別設定	•	•	•	•
威脅情報儀表Dashboard	x	選購	選購	•
交換器協同管理	•	•	•	•
交換器支援型號	ML-9324E、GS2220-28、GS2220-50、XGS2210-52、XGS2210-28、XS3800-28			
AP 無線控管	100台	100台	100台	100台
AP 支援型號	NWA50-AX、NWA90-AX、NWA110-AX、NWA210-AX、NWA1123-ACv3、NWA90AX PRO			
負載平衡(外/內)	•/•	•/•	•/•	•/•
虛擬伺服器	•	•	•	•
上網認證	•	•	•	•
兩步驟驗證	•	•	•	•
高可用性	•	•	•	•
VPN	•	•	•	•
IPSec Tunnel	•	•	•	•
SD-WAN	•	•	•	•
Wizard快速安裝設定	•	•	•	•
CMS	•	•	•	•
Eye Cloud雲端管理	•	•	•	•

三、技術規格

	NU-860C	NU-8700C	NU-8700F	NU-8700T	NU-8800T
硬體規格					
架機高度	1U	1U	1U	1U	1U
建議使用人數	300人以下	400人以下	400人以下	400人以下	1000-2000人
網路介面	14 x Gigabit	14 x Gigabit	6 x Gigabit 8 x 1G SFP	6 x Gigabit 4 x 10G SFP+	* 10 x Gigabit 8 x 1G SFP 4 x 10G SFP+
自定義埠	13	13	5 / 8	5 / 4	9 / 8 / 4
USB	2.0 x 2	3.0 x 2	3.0 x 2	3.0 x 2	2.0 x 2
LAN Bypass	•	•	•	•	•
電源耗瓦數	120W	220W	220W	220W	400W
處理效能					
防火牆最大處理速度	12 Gbps	18 Gbps	18 Gbps	25 Gbps	50 Gbps
最大同時連線數	3,400,000	3,500,000	5,000,000	5,000,000	6,000,000
每秒新增連線數	120,000	170,000	170,000	200,000	300,000
郵件掃描封數/天	5,200,000	5,200,000	5,200,000	5,200,000	6,000,000
防毒效能	950 Mbps	1.2 Gbps	1.2 Gbps	1.5 Gbps	2 Gbps
IPS效能	1 Gbps	1.1 Gbps	1.1 Gbps	1.4 Gbps	1.8 Gbps
VPN效能	850 Mbps	2.1 Gbps	2.1 Gbps	2.4 Gbps	2.5 Gbps
VPN通道數					
IPSec VPN 通道數	3,000	6,000	6,000	8,000	10,000
PPTP/L2TP/SSL VPN 通道數	1,200	3,000	3,000	3,000	4,000
IP Tunnel 通道數	600	1,500	1,500	1,750	2,000
網路安全防護					
防毒引擎	Clam AV	Clam AV	Clam AV	Clam AV	Clam AV
卡巴斯基防毒引擎	內建一年	內建一年	內建一年	內建一年	內建一年
IPS防禦與資料庫	•	•	•	•	•
Sandstorm惡意程式過濾	•	•	•	•	•
垃圾郵件過濾&垃圾郵件學習共享	•	•	•	•	•
郵件稽核	•	•	•	•	•
進階URL管控與資料庫	內建一年	內建一年	內建一年	內建一年	內建一年
進階APP管控與資料庫	內建一年	內建一年	內建一年	內建一年	內建一年
WAF 網路應用程式防火牆	•	•	•	•	•
Geo IP 國別設定	•	•	•	•	•
威脅情報儀表Dashboard	•	•	•	•	•
交換器協同管理	•	•	•	•	•
交換器支援型號	ML-9324E、GS2220-28、GS2220-50、XGS2210-52、XGS2210-28、XS3800-28				
AP 無線控管	100台	300台	300台	300台	無限
AP 支援型號	NWA50-AX、NWA90-AX、NWA110-AX、NWA210-AX、NWA1123-ACv3、NWA90AX PRO				
負載平衡(外/內)	•/•	•/•	•/•	•/•	•/•
虛擬伺服器	•	•	•	•	•
上網認證	•	•	•	•	•
兩步驟驗證	•	•	•	•	•
高可用性	•	•	•	•	•
VPN	•	•	•	•	•
IPSec Tunnel	•	•	•	•	•
SD-WAN	•	•	•	•	•
Wizard快速安裝設定	•	x	x	x	x
CMS	•	•	•	•	•
Eye Cloud雲端管理	•	•	•	•	•

* NU-8800T 可支援模組擴充。