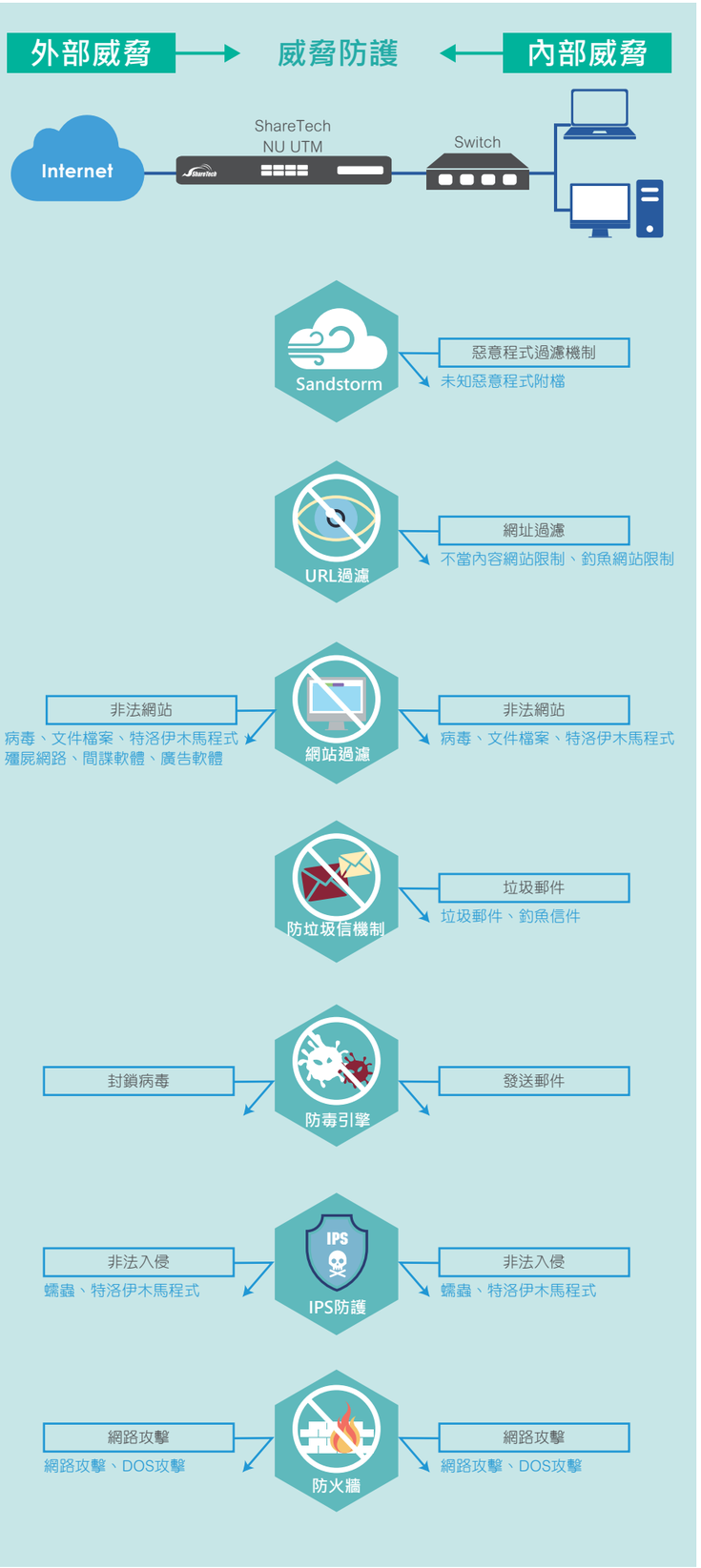


P2P

過濾經由P2P軟體所傳送檔案，是否隱藏惡意程式，管理員還可管控使用P2P權限，設定其最大使用頻寬、最高同時連線數。

URL過濾

進階URL資料庫，提供一年免費授權。近百萬筆網站分類資料庫，可有效阻擋語言暴力、線上影音、藥品、賭博、駭客、成人網站、代理篩檢程式、轉頁、後門程式、不信任網站、暴力網站與非法盜版的威脅。

防毒引擎

惡意攻擊行為如病毒、蠕蟲、惡意程式、木馬、零日弱點、駭客，都能藉由流經閘道的網路流量傳播惡意的攻擊行為。內建ClamAV防毒引擎，亦可搭載卡巴斯基防毒技術，提供用戶更完整的網路閘道防護。

防垃圾信機制

垃圾郵件引擎3.0合併自行研發的「垃圾郵件學習共享」機制，快速過濾上千種郵件威脅，達到比傳統垃圾郵件過濾更高的偵測率與最低的誤攔截率。

IPS防護

入侵偵測與預防系統Intrusion Prevention System，縮寫為IPS，特徵資料庫會依照危險程度分為高、中、低三種，能夠即時隔離不正常或具有傷害性的網路資料傳輸行為。

防火牆

套用合理流量觀念，認為每個來源不會同時產生太多封包/秒，萬一超過設定的合理封包數時，防火牆會要求將多餘的封包阻擋。全程監控封包連線，確保非法連線無法進入。

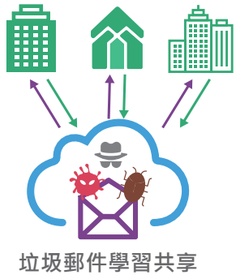
新世代多功能UTM特點

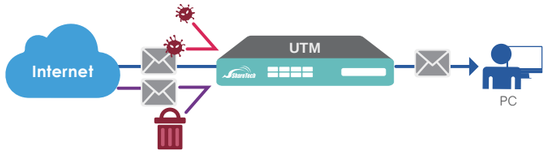
病毒信過濾

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。NU系列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。



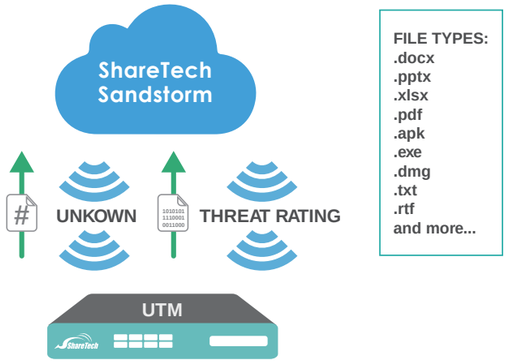


IPS 入侵防禦

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。

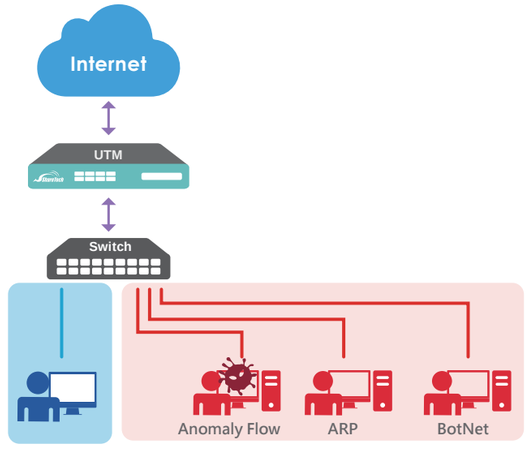
Sandstorm惡意程式過濾機制

進階Sandstorm可有效偵測未知的進階惡意程式附檔，諸如常見 Microsoft、Word、Excel、Power Point 或 PDF；或針對性的釣魚郵件，甚至壓縮檔，如常見的是ZIP與RAR，Sandstorm防禦在企業郵件掃描Spam或Virus前，針對可疑的附件先做比對，將有問題的信件進行隔離，讓潛藏的惡意程式現出原形，避免影響使用者郵件接收。



內網協防

NU系列UTM與合勤交換器整合，可針對中毒與異常之使用者即時封鎖避免影響整體網路，幫助企業做好協同防護的工作，保護內部網路不會受到病毒或惡意程式的破壞。內網協同防禦幫助企業在面對電腦病毒或後門程式侵略破壞時，可以藉由網路封包過濾分析應用程式(如 IPS / IDS / Sniffer等)在第一時間做偵測、阻絕，透過IP或MAC位址快速找出該使用者的詳細資料。並阻絕該使用者的網路，讓其無法連結上網進行任何存取行為，將惡意程式阻絕在企業網路之外，直到該網路使用者電腦恢復正常。

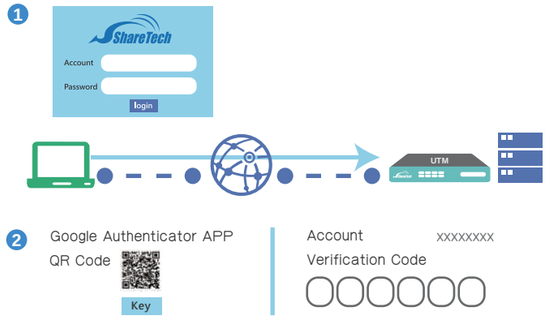


應用程式與URL資料管理

NU系列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。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。內建一年APP與URL資料庫更新，客戶可選購續享即時更新或選擇免費方案。

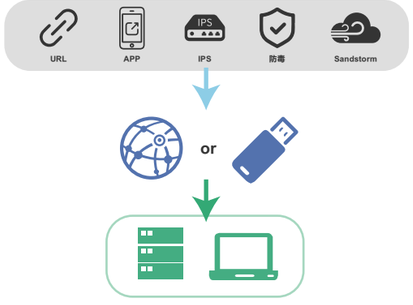
多因子認證(MFA)

使用者還可以在管理者、本機使用者、POP3使用者、SSL VPN使用者等部分使用其他認證因子(如Google與Microsoft Authenticator) 進行多重驗證，以降低系統相關帳密遭假冒或竊用之風險。



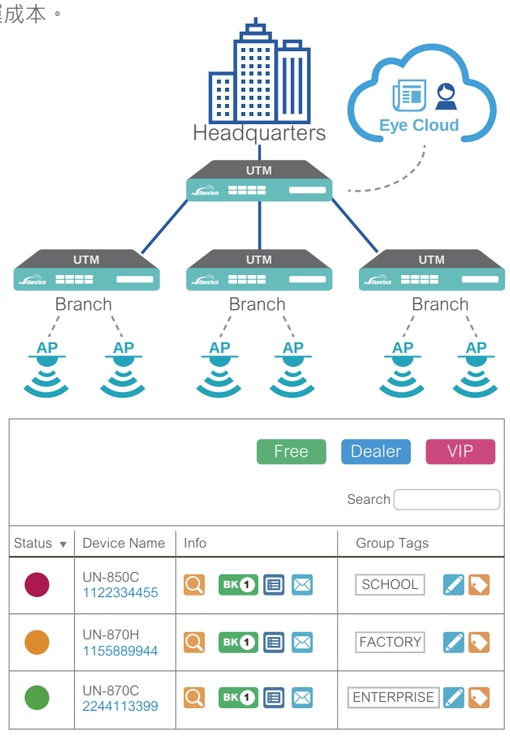
特徵碼更新機制

支援雲端與USB離線兩種方式，針對部分不開放對外連線的機關單位，USB離線更新機制可確保內網的設備也能得到最新、最完善的特徵碼更新。可離線更新的項目如下: IPS入侵偵測防禦、APP應用程式管制、URL黑名單、防毒軟體(ClamAV與Kaspersky)、Sandstorm等。



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。



LOG分析與CEF格式

NU系列UTM提供基本LOG分析，讓管理者在追查問題時，可快速查證何人、何事、何處所造成的，近年來資訊安全關注程度日漸增高，機關單位必須備份長時間整機LOG紀錄，當某天有威脅狀況發生時，有相對應的記錄可供查詢。LOG支援CEF格式，網管人員可以利用即時記錄分析套件Graylog閱讀並自訂格式。

User Name	IP	Sessions	Upload (bits)	Download (bits)	Record
PETER-H55M-UD2H	192.168.186.50	178	0	0	Record
192.168.186.70	192.168.186.70	107	0	0	Record
192.168.189.29	192.168.189.29	83	22.38K	33.4K	Record
syncs	192.168.189.21	78	2.7K	910	Record
192.168.189.19	192.168.189.19	65	0	0	Record

威脅情報儀表

直觀清晰的儀表板，管理者可於上方功能區選取項目，使導覽、工作速度更快速、更容易使用。
友善介面以即時流量圖、折線圖、圓餅圖呈現，讓管理者對於相關防護統計的掌握一目了然。

1 功能配置
一鍵快速切換到UTM管理介面

2 威脅情報
長條圖顯示近10天與上個月所有威脅攻擊比較，圓餅圖顯示威脅類型比例，管理者可檢視智慧防禦區中六大常見的威脅攻擊排行。

3 流量分析
折線圖顯示24小時內上傳與下載流量差異，圓餅圖顯示流量類型比例，管理者可依據協定、來源與目的IP位址等條件檢視上下載流量比例與排行。

4 連線狀態
顯示動態即時連線數據、圓餅圖顯示其比例，管理者可依據連線類型、連線IP位置等條件檢視數量與排行。

5 防火牆防護
折線圖顯示24小時內與上周防護數量的差異，圓餅圖顯示其類型比例，管理者可依據防護類型、主動與被攻擊IP等條件檢視數量與排行。

6 IPS
長條圖顯示24小時內低、中、高防護等級數量，圓餅圖顯示其比例，管理者可依據來源與目的IP、攻擊事件等條件檢視數量與排行。

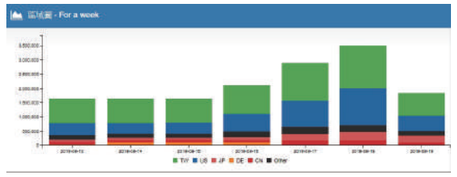
7 Web服務
長條圖顯示HTTP、HTTPS網頁流量，圓餅圖依網域顯示其比例，管理者可檢視網域、IP網址使用加密與非加密協定的流量與排行。

8 Web Control
長條圖顯示病毒、預設或自訂URL黑名單數量，圓餅圖顯示其比例，管理者可檢視網頁病毒攻擊、觸發過濾的URL類型，也可以來源與目的IP為條件統計其數量與排行。

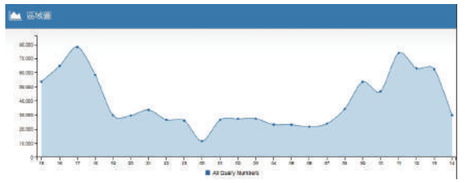
9 郵件服務
折線圖顯示指定區間內正常、垃圾信、病毒、傳送失敗與被退信件數量，圓餅圖顯示其比例，管理者可根據郵件帳號、郵件網域、正常郵件傳遞、垃圾郵件、病毒郵件、傳送失敗郵件、退信等不同條件檢視郵件收發雙向的數量與排行。

10 應用程式管制
折線圖顯示指定時間內應用程式數量，圓餅圖顯示其比例，管理者可依據名稱、來源與目的IP、群組等條件檢示數量與排行。

11 IP地區
長條圖顯示一周內來往IP位置的國家區別，圓餅圖顯示其比例，管理者可依據國家、對內對外IP等條件檢視數量與排行。



12 DNS查詢
折線圖顯示24小時內所有查詢數量，圓餅圖顯示其查詢比例，管理者可依據網域、來源IP、DNS Server等條件檢視數量與排行。



13 統計 14 報表
管理者可依據時間點、時間區間、顯示比數、IP模式與管理類型為條件顯示統計資料。同時，也可產生報表與寄送，設定SMTP、通知信件標題、備份數量、報表產生週期、排行等條件。

NU系列規格表

	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	4.8 Gbps	15 Gbps
UTM效能	2 Gbps	2 Gbps	3.3 Gbps	10 Gbps
VPN效能	650 Mbps	650 Mbps	800 Mbps	850 Mbps
防毒效能	750 Mbps	750 Mbps	950 Mbps	950 Mbps
IPS效能	750 Mbps	750 Mbps	1000 Mbps	1000 Mbps
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
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				
安全閘道	•	•	•	•
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
HTTPS過濾	•	•	•	•
垃圾郵件過濾&垃圾郵件學習共享	•	•	•	•
IPS防禦與資料庫	•	•	•	•
Sandstorm惡意程式過濾	•	•	•	•
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	•
遠端紀錄伺服器	•	•	•	•
交換器協同管理	•	•	•	•
負載平衡(外/內)	•/•	•/•	•/•	•/•
虛擬伺服器	•	•	•	•
上網認證	•	•	•	•
AP 無線控管	100台	100台	100台	100台
高可用性	•	•	•	•
內容紀錄-網頁&病毒	僅記錄含病毒網頁	•	•	•
硬碟韌體更新紀錄	x	•	•	•
自動備份與硬碟狀態	x	•	•	•
VPN	•	•	•	•
IPSec Tunnel	•	•	•	•
IP Tunnel	•	•	•	•
SD-WAN	•	•	•	•
Wizard快速安裝設定	•	•	•	•
CMS	•	•	•	•
Eye Cloud雲端管理	•	•	•	•

眾至資訊股份有限公司 ShareTech Information Co., LTD.
台中總公司 04-2705-0888
台北分公司 02-2501-1185
高雄分公司 07-2298-788
免付費專線 0800-666-188
sales@sharetech.com.tw
help@sharetech.com.tw
www.sharetech.com.tw
工程技術專線 04-2702-0906

2023.07

NU系列規格表

	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
UTM效能	8.4 Gbps	12.6 Gbps	12.6 Gbps	17.5 Gbps	25 Gbps
VPN效能	850 Mbps	2.1 Gbps	2.1 Gbps	2.4 Gbps	2.5 Gbps
防毒效能	950 Mbps	1.2 Gbps	1.2 Gbps	1.5 Gbps	2 Gbps
IPS效能	1000 Mbps	1.1 Gbps	1.1 Gbps	1.4 Gbps	1.8 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
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					
安全閘道	•	•	•	•	•
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
HTTPS過濾	•	•	•	•	•
垃圾郵件過濾&垃圾郵件學習共享	•	•	•	•	•
IPS防禦與資料庫	•	•	•	•	•
Sandstorm惡意程式過濾	•	•	•	•	•
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	•	•	•	•	•
遠端紀錄伺服器	•	•	•	•	•
交換器協同管理	•	•	•	•	•
負載平衡(外/內)	•/•	•/•	•/•	•/•	•/•
虛擬伺服器	•	•	•	•	•
上網認證	•	•	•	•	•
AP 無線控管	100台	300台	300台	300台	300台
高可用性	•	•	•	•	•
內容紀錄-網頁&病毒	•	•	•	•	•
硬碟韌體更新紀錄	•	•	•	•	•
自動備份與硬碟狀態	•	•	•	•	•
VPN	•	•	•	•	•
IPSec Tunnel	•	•	•	•	•
IP 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。