ShareTech
內網防護系統2GB｜內網防護系統5GB

ShareTech 眾至內網防護系統是一套以 Linux 為基礎開發的作業系統。
提供 Anti-Virus、IPS、Anti-Botnet、Anti-Spam、Application Control 等功能。以提升網路層到應用層的安全，讓政府機關、學校對於內部資料與網路的安全可以有高等級防護水準。具便利性與管理性，降低管理人員維護運作上之困擾。藉此以有效保護內部重要資源與郵件使用安全，降低採購費用、提升資訊安全保護水準。

特點

高安全
整合多項防護功能，包含安全、網路應用、管理維護與郵件安全防護，於一般主機上即可即時預防威脅與網路安全監控。

易管理
經由 ShareTech 內網防護系統雲端管控平臺可管控多台UTM，政府機關、學校如於各地有佈署網路安全設備，可將它們全部集中管理。

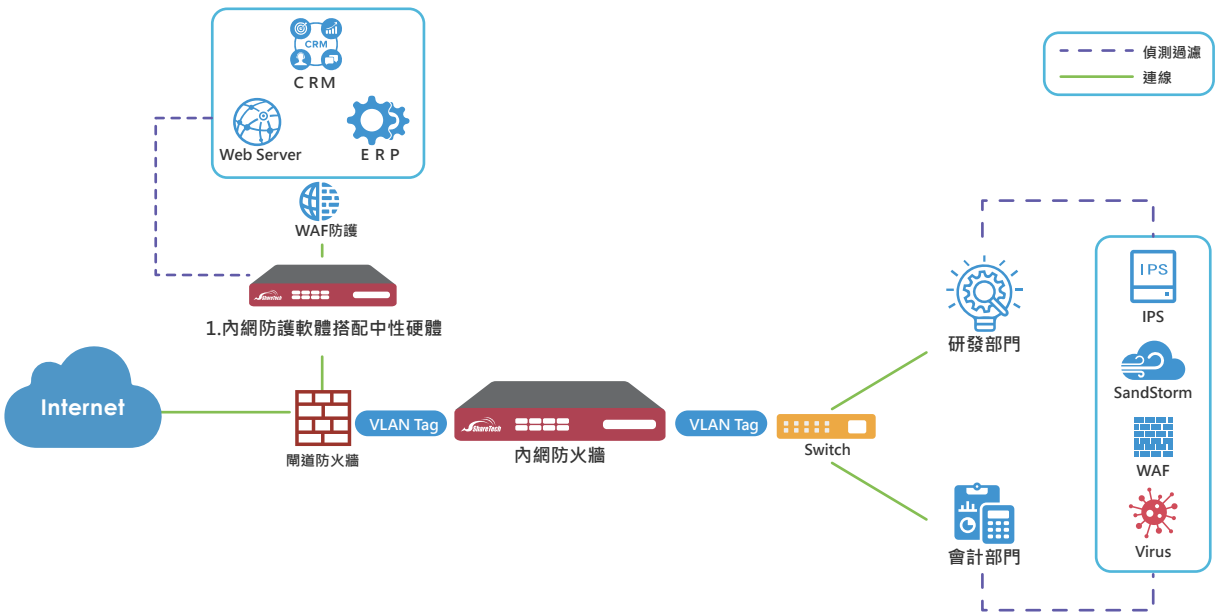
無線管控
將無線管控納入管制，避免BYOD使用者因使用無線網路而增加駭客、病毒與惡意軟體的攻擊困擾，並結合認證機制保護網路安全。

高整合
整合內網防護系統與其他安全防護設備(包含ZyXEL交換器、無線AP)的ShareTech控制中心，提供更完整的網路安全方案。

動態威脅保護
全年無休、持續更新，確保最大的安全性及降低成本。藉由修補程式管理、自動更新保護機制增加 IT產能。

VPN彈性運用
支持多種VPN機制，讓內部與信任的外部網路之間可建立安全連線，確保和遠端使用者之間的連線資訊不被竊取。

系統架構



功能

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，可同時監控多台內網防護設備。為了便利管理在各地的內網防護系統，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，可統一監看所有內網防護系統，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。

兼顧優異效能與進階功能

ShareTech 內網防護系統，可以輕鬆安裝於X86硬體，讓企業用戶都可以充分感受到內網防護軟體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

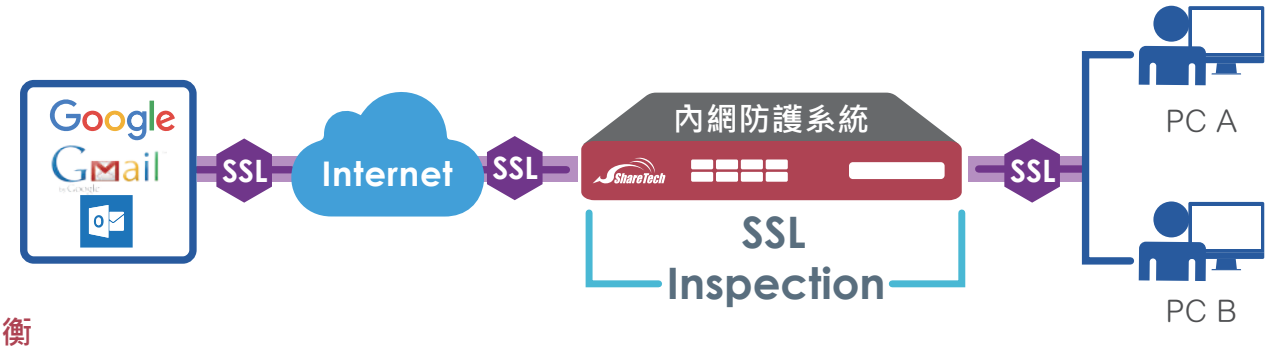
ShareTech 內網防護系統已整合IPv4/v6趨勢，同一個網路接口，不管它被定義成 WAN 或是 LAN，都可以同時綁定v4或v6的IP地址，所以不管是在純v4的環境、v4/v6 混合、純v6 的環境都一樣合用。

支援SDN控制器

支援SDN 控制器，可以讓1個以上的Port 組合成 ZONE，直接由SDN 控制器管理，而 ZONE 與 ZONE 封包傳遞，亦會透過內網防護系統的封包檢測。並具有VLAN 802.1Q功能，可以將內部網路切割成數個獨立的子網段，每一個網段各自獨立運作互不相干擾。

SL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

提供Outbound和Inbound負載平衡，提供多種負載平衡演算法則，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

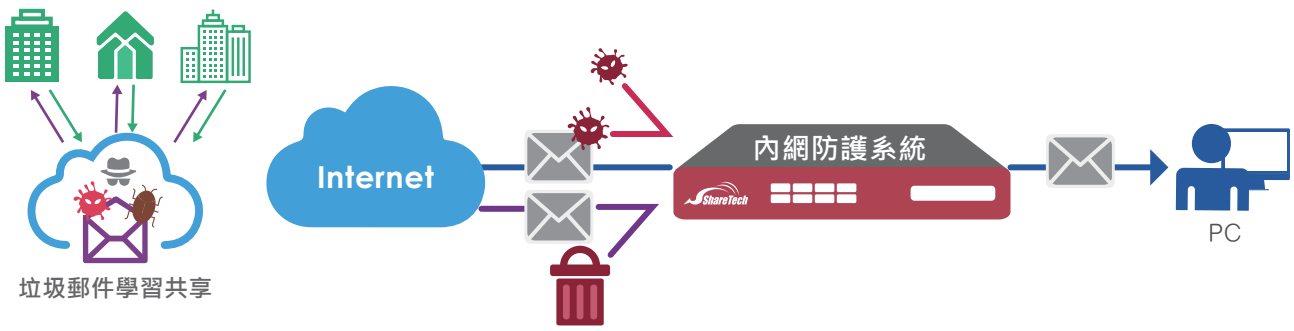
若企業已有郵件主機，但對垃圾信過濾效能不滿意，可將內網防護系統當作閘道安全設備，補原來郵件伺服器不足的功能，如垃圾郵件過濾、病毒信過濾、郵件稽核等功能。會再過濾完病毒及廣告郵件後，將乾淨的郵件傳送到郵件主機。

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。內網防護系統可加購卡巴防毒引擎，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

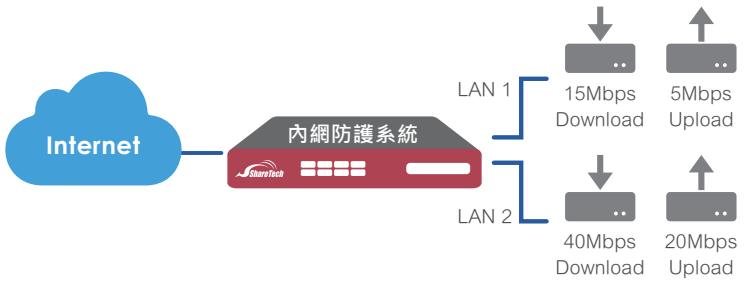
任何網路行為，不論使用者執行哪一種軟體，從網路封包的角度，大致分成上傳、下載的連線數量、流量(Flow)跟持續時間(Time)，藉由偵測這些數量的組合，推估使用者是正常使用網路或是有異常的行為。當發現內部使用者異常行為後，管理者可以採取多種策略，例如，阻擋上網、立即限制它的最大頻寬、啟用協同防禦機制通知交換器將它封鎖或是通知管理者就好。

Sandstorm防護

SandStorm防禦讓企業郵件在掃描spam或virus後，可以再針對可疑的附件做拆解，偵測後會將有疑慮的郵件送往Sand-Storm做進階掃描，讓這些潛藏的惡意程式現出原形，避免影響使用者郵件接收。

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，內網防護系統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。

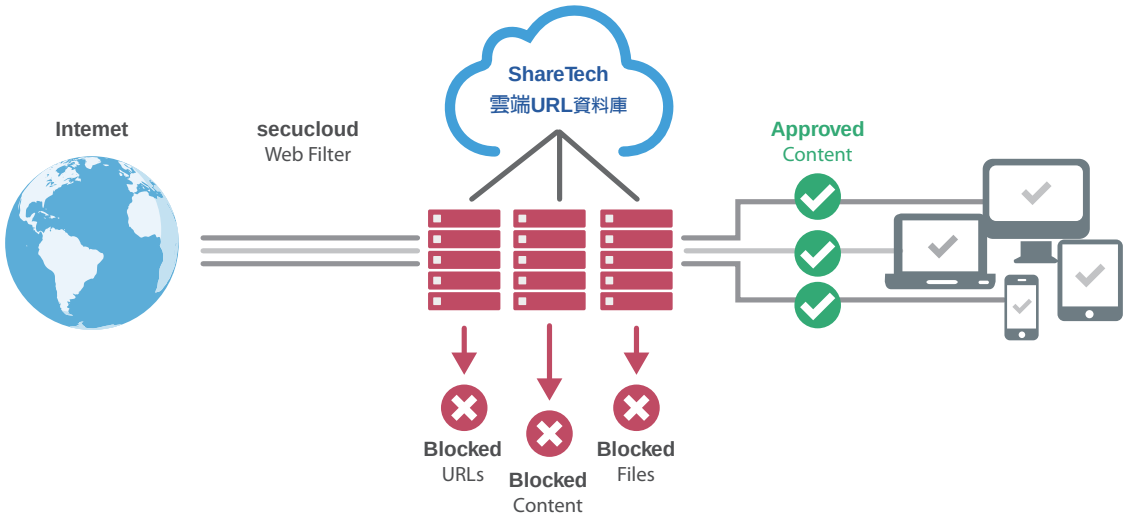


內容過濾

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。內網防護系統內建一年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。內網防護系統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。

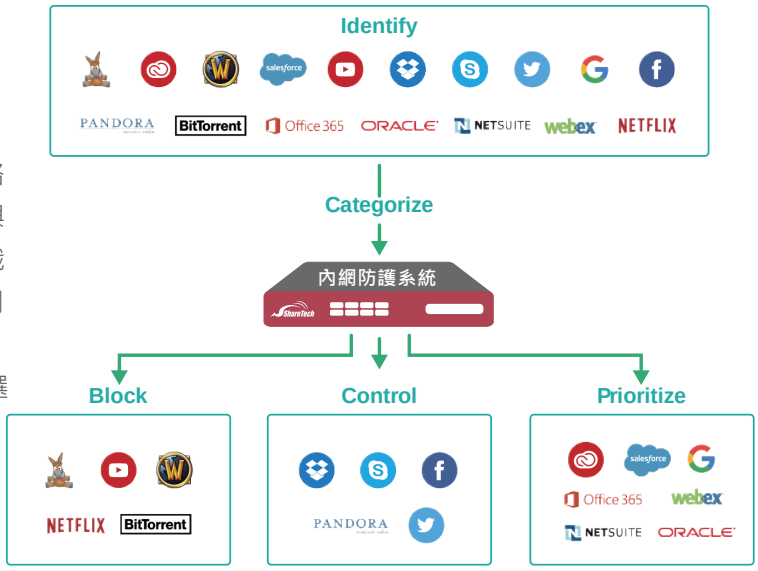
流量分析

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。 內網防護系統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。

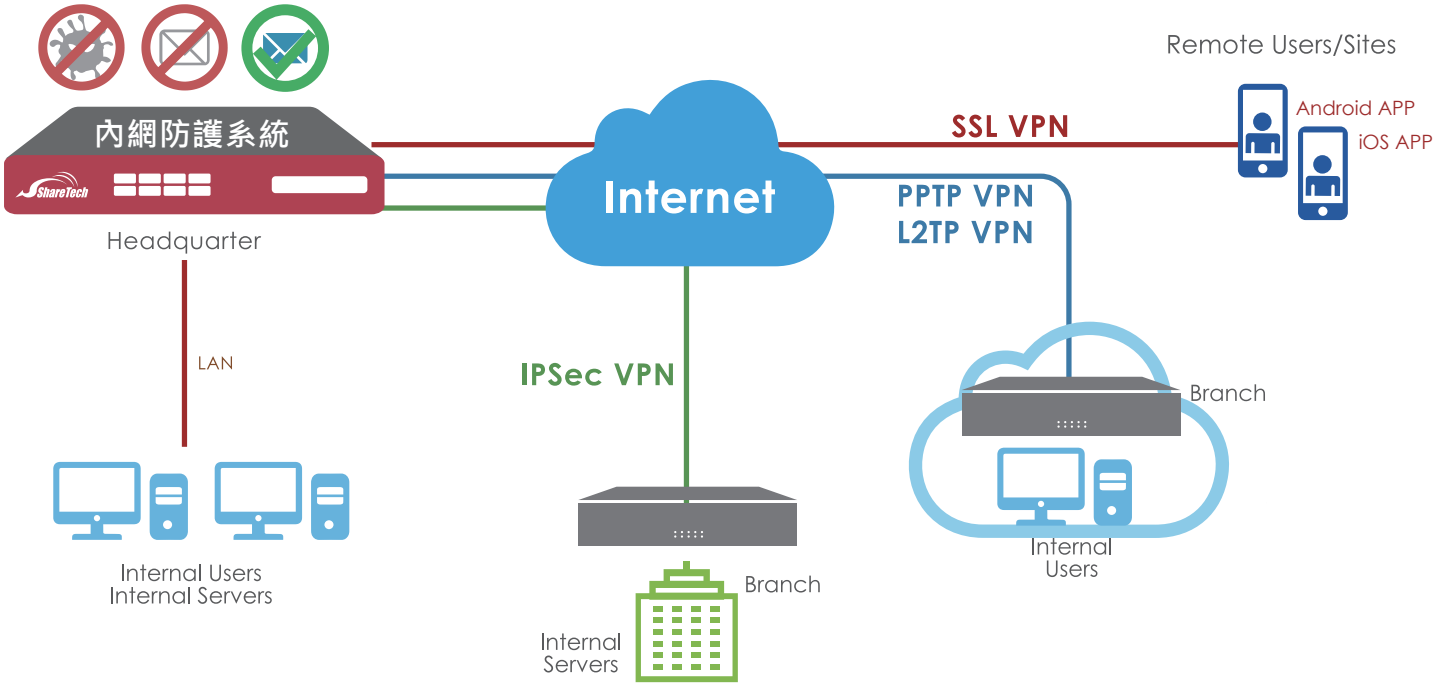


圖形化流量報表

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、WAN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。



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.可選購卡巴防毒引擎 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 7.且備10個虛擬網路防火牆
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.提供郵件稽核過濾設定、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.網頁瀏覽紀錄

特色	效益
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
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	Bridge
威脅情報中心與日誌 (Dashboard & Logs)	1.可選購威脅情報中心，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.硬體CPU服務中斷設定 2.提供HTTPS、HTTPS網頁管理 3.介面提供繁、簡中文、英文語系 4.提供系統備份、韌體升級、自動備份、韌體下載記錄 5.具重新啟動系統與關機功能 6.UPS不斷電系統 7.具有VLAN 802.1Q功能，可針對不同的VLAN套用不同安全政策 8.支援DDNS服務、DNS伺服器、SNMP服務 9.支援遠端記錄伺服器 10.支援DHCP Client & Server
其他	1.具備網路管理協定SNMP方式 2.管理者權限控管 3.定時硬碟檢測與修復 4.具備LAN bypass 5.安全管制條例建立筆數可達6000筆 6.支援Netflow和S-Flow資訊

硬體推薦型號

項目 \ 型號	Share Tech H1	Share Tech H2
CPU	Atom 3558	Core i3-4330
RAM	4G	4G
埠數	14 Giga Ports	10 Giga Ports
Consle	1	1
USB	2	2
HD	480G SSD	480G SSD
防火牆效能	9,6Gbps	12Gbps
最大連線數	3,000,000	5,000,000
新增連線數	120,000	165,000
內網防護(IPS、防毒)	260Mbps	320Mbps