ShareTech UTM
1GB / 2GB / 5GB / 10GB

ShareTech眾至UTM (United Threat Management)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。

1 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 UTM雲端管控平臺可管控多台 ShareTech 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UTM軟體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。

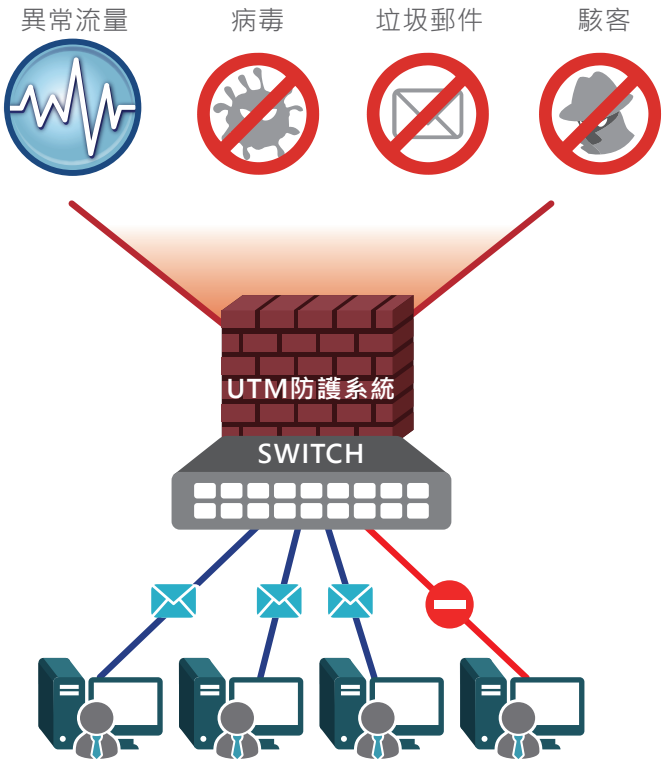
動態威脅保護

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。

2 系統架構



3 功能

▼安全防護

•防火牆防護
可防範多種網路攻擊行為，使駭客或意圖不軌人士無法入侵，徹底保障機關內部網路的安全。

•駭客木馬防護
對於遭受異常洪流的主機，即時發出警告，並根據預先制訂的洪流量數值，阻擋駭客將網路資源用完。

•防ARP欺騙
發佈可信ARP清單，使所有主機綁定真實的IP/MAC，並定期進行ARP欺騙檢測，保證內網的穩定性。

•協同防禦
整合交換器一同進行防護，一旦偵測到威脅，立即將有問題的電腦交換器Port直接關閉，不僅可以節省UTM的資源，也確保此危害不會蔓延內部網路。

•郵件稽核
提供郵件稽核過濾設定、進階設定與過濾隔離區。

•病毒防護
提供ClamAV與卡巴（選購）雙引擎防毒防護，ClamAV永久免費韌體更新。可針對連線中的WEB/FTP資料及進出閘道的郵件，進行即時掃毒。

•IPS 防禦
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。

• 網路異常使用分析及阻擋
自動將非法的行為執行記錄、通知、阻擋的動作，並提供例外IP設定、異常記錄語阻擋清單。

•垃圾郵件過濾防護
提供六大防禦機制，並能自動學習垃圾郵件特徵。提供垃圾郵件通知信件，並可快速進行寄送、隔離與刪除。

▼上網管理

• 頻寬管理
具有策略流控、頻寬優先權等功能。管理者可自訂保證頻寬與最大頻寬，並提供頻寬設定模式。

•負載平衡
具有自動分配、手動分配、依來源IP分配與依目的 IP分配4種分配模式。對於擁有2條以上線路的用戶，也有對外線路的負載平衡機制。

•認證
提供本機使用者/AD/POP3認證授權機制，協助網管人員監控內部所有使用者帳號，在確認使用者ID 有效授權後，才允許其使用網路，讓機關可以有效管理網路使用資源。

•上網程式管理
提供多類應用程式管制，包含P2P軟體管制、影音服務與VOIP、社群網路、即時通訊、運動與旅行、飲食、金融保險、賭博與色情、遊戲等。

• URL 資料庫
內建「雲端URL資料庫」，自動將網頁分類，管理者只要針對有害的URL進行防堵，便可輕鬆管制，不需要再逐一輸入網站 IP 位址、關鍵字來阻擋。

▼設備管理

•日誌
內建系統、警告、錯誤等日誌，並支援日誌查找功能，可詳細列出管理員改變前及改變後的資料。

•即時消息通知
讓網管人員能隨時掌握設備運作狀態，當發生當機或不能正常運作時能在第一時間處理，讓網路運作風險降到最低程度。

• 韌體定時檢查更新
自動檢查是否已經更新到最新版本，並下載最新韌體，管理者只需要按下更新鈕或是安排時間定時更新韌體。

• 網路串接方式
支援 PPPoE和DHCP(Server和Client) 協定，支援：ADSL、Cable Modem、FTTB、DDN 等各種接入方式。

▼其他功能

•虛擬伺服器
提供內部區域網路的特定主機成為 WEB、FTP、DNS或Mail伺服器的連接。具備完全對應IP功能，使特定電腦可以不受限制的存取網路資源。

•雙機備援
可建構兩套ShareTech UTM作雙機備援工作。

•測試小工具
具備PING、Traceroute、DNSQuery、Server Link、IP Route / Rule、IP Addr Show掃描等6種網路工具。

•DNS 伺服器
提供標準的DNS伺服器功能，如A、MX、NS、CNAME等記錄，不論是正向或是反向，統統都可以設定。

•VPN安全管理
支援IPSec VPN、PPTP VPN、SSL VPN、L2TP、SD-WAN。

•DHCP 伺服器
可以自行修改閘道的DHCP伺服器，並可以跟MAC 位址綁定 IP 位址。

4 建構UTM 安全防護系統需求

硬體建議需求

•ISO 檔必須安裝在 64 位虛擬機器上。
•虛擬機器的記憶體至少 1GB ，越大越好。
•硬碟：如有紀錄，建議至少 500GB。
•CPU 至少為 Intel P4 以上才支持頻寬：ADSL、專線均可。

使用者端建議需求

•流覽器建議使用IE 7.0以上版本，FireFox與Google Chrome均支援。