中大型企業專用
多功能UTM
UR-980

ShareTech 眾至新世代 UTM UR-980，提供中大型企業能夠在複雜的環境中，擁有最完整的網路安全防護網。眾至提供安全防禦(防火牆、入侵偵測、防毒、郵件安全)、管制稽核(內容過濾、應用程式管制、VPN管制、頻寬管制、郵件稽核、認證機制)、監控記錄(Log、上網行為記錄、事件記錄)與簡易管理(中央管理平台、AP 聯合管控、公佈欄、流量報表)等四大服務功能，透過多項優異技術整合，協助企業共同防範未知與已知網路威脅。

ShareTech UTM 設備是高安全、高效能與彈性佈署的多合一解決方案，對多數中大企業來說，他們對網路安全的佈署目標很明確，就是必須能保護其網路的安全性並方便管理維護。ShareTech 新世代的資安防護平台，包含三項重要核心技術，分別是：

- 深層防護機制
- 垂直橫向整合
- 雲端管理系統

此三項核心技術，整合企業需求，並能彼此協同運作、全方位防護，讓您利用 ShareTech 新世代 UTM，輕鬆面對日趨複雜的網路環境，不用購置多項產品設備、花費時間學習管理，讓 ShareTech 為您實現一貫式資安服務流程。

安全

- 阻擋外部駭客攻擊
- 阻擋惡意程式攻擊
- 防毒(WEB / FTP / MAIL)
- 垃圾信過濾
- 交換器協同管理
- HTTPS / SSL 加密
- IDP / Botnet

管控

- 頻寬管控
- 網站內容過濾
- 即時通訊監控
- 流量監控管控
- 應用程式管控
- VPN/SSL VPN 管控
- 上網認證

記錄

- 郵件通聯記錄
- 即時通訊通聯記錄
- 網頁瀏覽記錄
- FTP 下載記錄
- 異常 IP 分析記錄
- 防火牆防護記錄
- ARP 防偽記錄
- 事件記錄

(一) 功能說明

兼顧效能與功能

ShareTech 新世代 UTM，其硬體平台都是精心設計，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 ShareTech 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，管理者可以自訂自動備份時程。

IPv4 / IPv6 雙頻技術

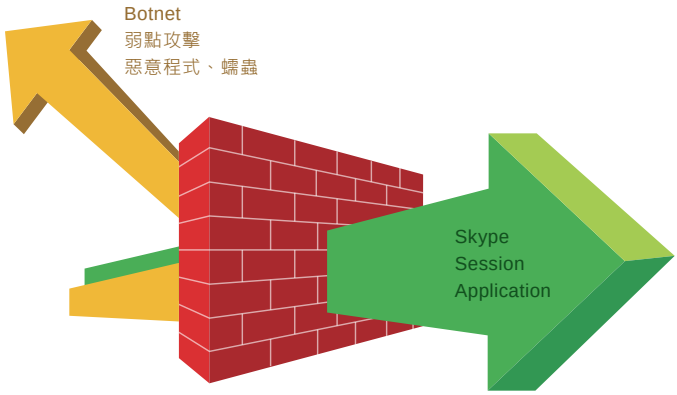
IPv4 位址短缺，IPv6 的年代遲早到來，所以 ShareTech 在研發下一代 UTM 時就已經將這個趨勢整合起來，同一個網路接口，不管它被定義成 WAN 或是 LAN，都可以同時綁定 IPv4 或 IPv6 的 IP 地址，所以不管是在純 IPv4的環境、IPv4 / IPv6 混合、純 IPv6 的環境，UR-980 都一樣合用。

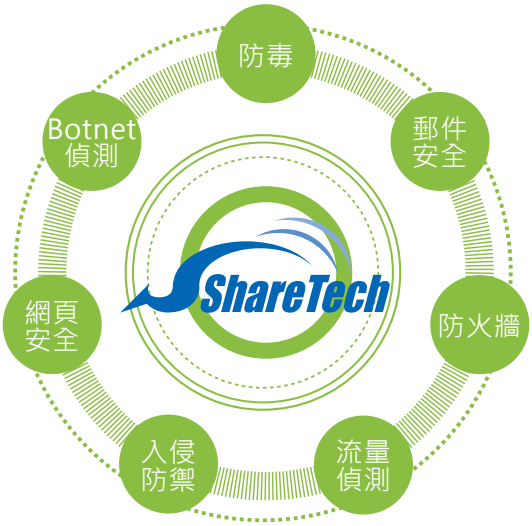
威脅偵測防禦

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。眾至 UR-980 除了提供防火牆、入侵偵測系統(IDP、Botnet)、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。

IDP 入侵防禦

IDP 它會檢查對應到 OSI 模型第 4 - 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。





Botnet 偵測防護

UR-980 兼具 Botnet 功能，因為本身兼具 NAT 的功能，當內部的使用者利用郵件伺服器寄出垃圾信件或是直接對外，設備可以快速掌握攻擊來源，快速將有危害的網路封包直接封鎖。目前提供兩種運作模式，分別為監聽與串接管理二種模式。監聽只監看是否有 Botnet 病毒，串接管理顧名思義只要是符合 Botnet 病毒碼做記錄或是阻擋。管理者可自行設定封包過濾數量的等級，從 Level 1 - Level 5。並且會記錄所有遭受 Botnet 攻擊的訊息。

郵件閘道防護

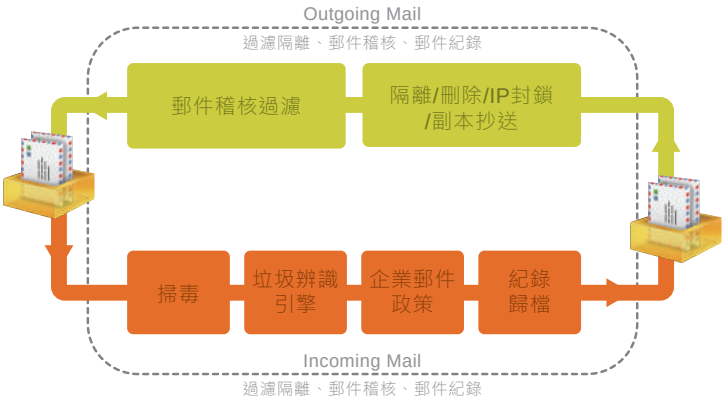
企業已有郵件主機，但垃圾信過濾效能不佳，可以將 UR-980 當作郵件閘道模式補原來郵件伺服器不足的功能，如垃圾郵件過濾、病毒信過濾。透過 UTM 過濾完病毒及廣告郵件後，將乾淨的郵件傳送到郵件主機。

防毒

Clam AV 防毒引擎防護，系統免費提供 Clam AV 防毒引擎，可偵測兩百多萬種以上的病毒、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。並可加值選購卡巴防毒引擎。

WEB、FTP防病毒過濾

當使用者開啟瀏覽器存取某網頁時，眾至 WEB 防毒會判別網頁的安全性。並可針對檔案的上傳、下載做過濾及檔案阻擋規則。根據以往經驗，利用 FTP 下載資料最容易讓自己的電腦中毒。所以利用網路做下載與上傳檔案須特別注意，因為有可能一不小心就讓自己的資料毀於一旦。



垃圾信過濾(Anti-Spam)

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。郵件過濾，能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。

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 (Connect Seesion)、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。

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。

郵件稽核

管理者可根據企業內部電子郵件稽核管理規則，將重要的郵件，授權稽核人員處置，稽核人員可針對被稽核的郵件執行包含放行、退回寄件者、刪除、延遲寄送等動作。

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，UR-980 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。

URL 資料庫管理

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 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。

上網行為全記錄

有部分企業員工，在上班時間使用 Skype 或者上臉書，做非工作用途的事情，聊天事小，洩密事大。UR-980 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，包含即時通訊(例如：Skype、QQ)、瀏覽網頁、郵件收送、FTP 下載等。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。

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。UR-980 內建多種應用程式管理功能，包含 P2P 軟體管制、即時通訊軟體、WEB 應用、娛樂軟體、其他應用程式，可輕鬆控管員工使用應用軟體之權限，保護企業網路安全。

流量分析(Flow Analysis)

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。

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。UR-980 提供系統狀態圖表(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記錄。

AP 無線管控

對多數企業而言，提早佈局無線上網辦公環境已經勢在必行，眾至提出藉由中央管理機制來掌握每一台 AP 使用人數與流量情形，而每一台 AP 之間緊密串連，更可以讓使用者在移動間工作時網路不中斷。

支援一組 Lan Bypass

為預防網路系統當機的問題，除針對電源輸入異常時，也支援 LAN Bypass 功能，在機器故障時會自動將網路接線自動導通，確保所有對外的網路保持暢通，也可提昇系統穩定及安全性。

內容過濾

使用者可自行定義關鍵字阻擋不當的網址，並可阻擋使用者直接使用 IP 位址上網。能阻擋由 Java applets 與 Active X 所控制的自動下載、網站 Cookies 等檔案形式：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。

網路測試工具

使用者可由系統主動發送封包(利用 Ping、Traceroute、DNS Query、Server Link 模式)，得知目前連外線路的資料傳輸品質和狀態。

靈活管制條例操控

UR-980 具有靈活的管制條例設計，管理人員可用各種排列組合方式達到企業網路管控的需求，所以操作皆在同一個介面中設定，並不需要停止服務即可立即修正，方便網管人員操作維護。

VPN功能

使用 IPSec、PPTP、L2TP 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。

而其中 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。

整合平台管理與監控

具有 CMS 中央管理功能，此功能方便管理者可以藉由中控平台遠端監控、啟動、重新啟動與管理裝置，可同時監控多台防火牆設備。此外，亦整合無線 AP 與交換器管理功能，降低企業營運成本。ShareTech UTM 提供管理者權限存取，可經由權責劃分來簡化管理作業。

內網防護(ARP 防偽)

對內網而言，最難偵測到的攻擊類型就是廣播型的封包，如 ARP 欺騙、私架 DHCP 伺服器等，因為通訊協定的先天性缺陷，導致這一類的攻擊行為很難被偵測出來，眾至 UR-980 的 ARP 偵測機制，可以在第一時間內就找到『濫發佈』ARP 訊息的人。另外，也可搭配協同防禦交換器的設備，可以標示出這個IP的實體位置，讓他無所遁形。

電子白板

UR-980 公佈欄設計理念就是，當員工在打開網頁之前必須閱讀電子白板裡面的通知才允許上網流覽網頁，而且只要閱讀了電子白板裡面的通知，就會記錄員工 ID 帳號,便於日後稽核證據，如果員工不閱讀可禁止其上網。

多功能管理介面

使用 WEB 方式設定和更新韌體，操作畫面可隨時切換為繁體中文 / 簡體中文 / 英文，並具有設定檔匯入、匯出的功能。

支援 USB 備份還原

藉由 USB 插槽隨時為企業做好 24 小時設定檔備份動作，當遇到突發狀況必須更換設備時，在設備開機時只要插入原本 USB 就會自動匯入備分設定檔

(二) 特色與效益

特色	效益
威脅防禦 (Anti-Virus / IDP / Botnet)	1. 提供免費 Clam AV 防毒引擎，資料庫達百萬筆 2. 內建卡巴防毒引擎(一年) 3. Clam AV 防毒引擎資料庫即時更新，不需年費 4. 提供 IDP 與 Botnet 資料庫 5. IDP 特徵資料庫會依照危險程度分為高、中、低三種 6. IDP & Botnet 資料庫無年費
惡意網址過濾 (URL & Databases)	1. URL 資料庫無年資 2. 提供 URL 過濾條件與資料庫管制 3. 可自行設定 URL 過濾條例 4. 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
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、優先權與 Smart QoS 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 4. 阻擋 ARP 欺騙 5. 提供交換器拓樸圖
郵件安全管理 (Anti-Spam、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. 提供郵件病毒掃描 3. 提供郵件稽核過濾設定、進階設定與過濾隔離區 4. 提供 Client 端垃圾信搜尋 WEB 介面 5. 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 6. 提供郵件記錄查詢
應用程式識別 (Applications Control)	1. 提供多類應用程式管制，包含 P2P 軟體管制、即時通訊、VOIP、WEB 應用管制、Webmail 管制、娛樂軟體、影音、惡意軟體、股票軟體等 2. 定期免費更新 3. 管理者可自行藉由 Policy 進行控管
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

特色	效益
上網行為全錄 (Content Record)	1. 記錄所有進出之郵件 2. 郵件記錄格式是 .eml 檔 3. FTP 上傳下載紀錄 4. 網頁瀏覽紀錄 5. 即時通訊談話內容記錄，例如：QQ、Skype
VPN安全連線	1. 提供 IPSec、PPTP、L2TP VPN 機制 2. 提供 SSL VPN 安全連線 3. 可針對 VPN 連線進行管制
頻寬管理	1. 獨特 Smart 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	Transparent, Bridge, Routing, NAT, Bypass
日誌與報表 (Log & Report)	1. 提供多項日誌記錄，包含系統設定、網路介面及路由、管理目標、網路服務、進階防護、郵件管理、VPN / SSL VPN 等日誌 2. 可定期產生各類行報表，包括統計、排行與圖表
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. 提供即時監測、維護與管理 3. 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	1. 提供 Ping、Trace Route、DNS Query、Port Scan 檢測連線工具 2. 提供 IP Route、Wake Up、SNMP、IPv6 檢測連線工具
其他	1. 韌體免費升級 2. 管理者權限控管 3. 定時硬碟檢測與修復 4. 802.1Q 服務 5. 資料備份及掛載 6. 提供自主化管理介面 7. LCD顯示板

(三) 技術規格

型號	UR-970C	UR-980
	處理效能與連線數目	
介面(Giga Port)	10	18
介面(Fiber Port)	4	-
UTM 處理效能	8Gbps	14 Gbps
VPN 效能	1,600Mbps	2,200Mbps
防毒效能	800Mbps	1,400Mbps
最大連線數	4 Million	6 Million
郵件掃描封數/天	5,000,000	6,000,000
	VPN通道數	
IPSec VPN 通道數	6,000	12,000
PPTP 通道數	1,000	4,000
L2TP 通道數	1,000	4,000
SSL VPN / 通道數	1,000	4,000
	網路安全防護	
閘道防毒	•	•
垃圾郵件過濾	•	•
IDP 入侵偵測	•	•
Botnet 防禦	•	•
應用程式管制	•	•
URL 資料庫	•	•
報表	•	•
郵件稽核	選購	•
上網行為記錄	•	•
異常 IP 分析	•	•
交換器管理	•	•
負載平衡(外/內)	•	•
頻寬管理功能(QoS)	•	•
公佈欄	•	•
上網認證	•	•
AP 無線控管	•(不限)	•(不限)
CMS 中央控管	•	•
HA 雙機備援	•	•
VPN (IPSec / PPTP)	•	•
L2TP VPN	•	•
SSL VPN	•	•
管理權限控管	•	•