UM Series

整合威脅防禦管理器

企業整合資安威脅防禦管理與郵件安全的最佳解決方案

UTM Gateway

極致淨化・優化・安全化企業網路

整合威脅防禦管理器UM系列產品

企業整合資安威脅防禦管理與郵件安全的最佳解決方案

由於網際網路的開放與蓬勃發展，企業對於Internet的使用依賴度越來越高，單一廣域線路已不敷使用，且有斷線導致企業營運受損的困擾。企業有更多的網際網路ISP可供選擇，使用價廉物美的多線路ADSL、Cable 或固接線路的WAN負載平衡器已蔚為趨勢。由於Internet的使用度提高，導致企業網路充斥各種不當行為，如駭客攻擊、病毒侵襲、垃圾郵件、網頁威脅入侵、大量傳輸、頻寬佔用….等，管理者必須以負載平衡器、頻寬管理器、防火牆、防毒牆、IDP、WAF、網站過濾器、反垃圾郵件過濾器…等網路資安設備來防範與改善，企業也需要透過Internet來與各地分點或遠端連線，雖然方便但其資料安全性卻是無可保障，需要建置VPN的解決方案，確保企業往來資訊安全化，保障企業營運正常。

綜觀以上企業常見的網路資安使用問題，友旺科技特地推出整合威脅防禦管理器UM系列產品(UTM Gateway)，AboCom的UM產品採用獨立主機硬體崁入式設備的架構，提供品質穩定及高效能的專屬作業系統，來解決企業的網路使用與安全困擾。UM系列產品提供了4~12個網路介面(WAN/DMZ/LAN埠)，可由管理者依照企業資安政策，自行定義與分組管理，兼顧彈性與擴充性。同時內建防火牆(Firewall)、網路頻寬管控(QoS)、三合一VPN(IPSec/PPTP/SSL VPN)、In/out-bound負載平衡、VPN & Server負載平衡、兼具頻寬合併與自動備援的雙重考量，支援IPv4及IPv6網路協定、網路應用軟體(IM/P2P/FTP/Webmail/On-Line Game...)的過濾管控、上網認證、網站過濾管制、網路流量統計排行、郵件安全(垃圾郵件過濾、病毒郵件過濾、郵件歸檔與稽核)、防毒牆(Mail/HTTP/FTP)、主動式入侵偵側防禦系統(IDP)、網頁威脅防禦系統(WAF)…等多功能於一機，提供企業Internet連線、整合式資安威脅防禦管理與郵件安全的最佳解決方案。

產品特色(Feature & Benefit)：

※採用獨立主機的硬體崁入式設備的架構，提供品質穩定及高效能的專屬作業系統，符合19英吋機架式標準規格。

※提供4~12個網路介面(WAN/DMZ/LAN埠)，可由管理者依照企業資安政策，自行定義與分組管理，兼顧彈性與擴充性。

※支援IPv4及IPv6的網路協定，企業可全面提昇網路適用性與便利性，無需擔憂IP網址短缺與網路協定轉換的問題。

※提供全方位的郵件安全與服務：包含垃圾郵件過濾、病毒郵件過濾、郵件攻擊防禦、問題郵件郵寄通知、郵件歸檔與稽核…等多項功能。

※提供多種垃圾郵件過濾機制(指紋辨識、灰名單、貝式過濾、特徵資料庫、RBL、SPF、Domainkey、黑/白名單…)、多層交互掃瞄過濾郵件，達到最高99%垃圾郵件判斷率。

※提供硬體式防毒牆：支援Clam AV及Sophos 雙防毒引擎，可針對Mail(SMTP/POP3)、HTTP及FTP提供Anti-Virus整體解決方案(含DOC、EXE、OCX ...等檔案類型的過濾掃描功能)。

※提供全文檢索的條列式郵件日誌(Mail Log)、多樣化的圖形統計報表，讓管理者輕鬆掌握企業郵件流向及郵件系統運作狀況。

※內建主動式入侵偵測防禦系統(IDP)機制，提供約9,000個IDP特徵資料庫，可做到網際網路4~7應用層的檢測防禦，避免惡意網頁程式、木馬、間諜軟體、網路釣魚、駭客…等危害攻擊，有效保護企業網路。

※內建網頁威脅防禦系統(WAF)機制，支援Web 2.0、各種Web Server(IIS、Apache..)、腳本語言的網站應用防火牆。

※完整的負載平衡(In/Out-bound、VPN、Server Load balance)與策略路由機制(RIP/OSPF/BGP)，提供多個WAN埠線路多重定址(Multi-Homing)、負載平衡(Load balance)及容錯備援機制(Auto Backup)，企業可用最低投資，合併網路頻寬，斷線自動備援，讓企業享有永不斷線的Internet服務。

※全方位的自動備援(Auto Backup)機制：具備WAN多線路備援、VPN備援、Server備援、郵件備份、HA雙機備援...功能，提供企業穩定及無斷線之虞的網路環境，確保企業郵件的留存及方便日後隨時可調閱查察。

※3 in 1 VPN：提供IPSec、PPTP及SSL VPN(Web VPN)完整三合一VPN解決方案，透過Internet建立方便穩定安全的企業網路。

※提供全方位策略式(Policy-Base)防火牆及內部(Internal)防火牆機制，搭配全天候(24x7)排程表管控，確保企業網路安全。

※提供QoS網路頻寬控管、個人化頻寬控管、P2P使用頻寬控管及ToP N網路流量排行統計，管理者可輕鬆掌控及妥善分配企業對外頻寬的使用。

※提供網路認證、授權、統計的3A服務，透過內建的資料庫或從外部的POP3郵件帳密、LDAP/AD、RADIUS Server執行3A Service的管控，可輕鬆掌控企業內部網路的安全使用。

※提供完整的網路應用軟體過濾與控管：包含IM(即時通訊軟體)、P2P(多點傳輸軟體)、FTP、炒股軟體、影音軟體、網頁郵件、線上遊戲、遠端控制、穿牆軟體…等，確保企業網路安全及不必要的網路頻寬耗損及佔用。

※記錄IM即時通訊軟體交談內容，詳細記錄使用者的即時通訊(MSN、QQ…)交談內容，達到企業積極開放，有效管理的資安稽核。

※支援最先進的網站類別雲端資料庫過濾機制(URL Filter)、提供網站黑/白名單(URL Block)、MIME/Script、副檔名、ActiceX、Cookie、Popup、Java Applet…等網站過濾控管機制與統計分析報表。

※支援虛擬區域網路IEEE 802.1q VLAN及VLAN Trunk、Virtual Server Grouping 與SNMP Agent/Trap網路管理功能。

※提供異常流量及內部中毒者偵測警示功能，當發現內部網路異常傳輸量或連線數，立即通知管理者及使用者，讓管理者即時瞭解網路異狀，並立即做出相關應變處置。

※提供內部網路區域聯合防禦機制：可與具備ACL指令的網路交換器(Switch)聯合防護內部網路的異常流量或中毒問題。

※提供所有網路介面使用狀態、系統效能表、系統連線表、系統認證表、ARP表及DHCP用戶使用表，所有的系統使用狀態一目了然。

※網路流量排行統計分析記錄及系統效能記錄皆可直接記錄於硬碟內，方便做歷史追查，藉以調整網路使用政策。

※內建英文、繁/簡中文Web UI網頁式設定管理介面，管理者可隨時隨地透過Internet遠端掌控企業網路及系統設定與管理。

※UM系列產品無使用人數的授權與限制。

產品規格與功能(Specification & Function)：

◎提供網路介面(WAN/DMZ/LAN埠)可自行定義與分組管理

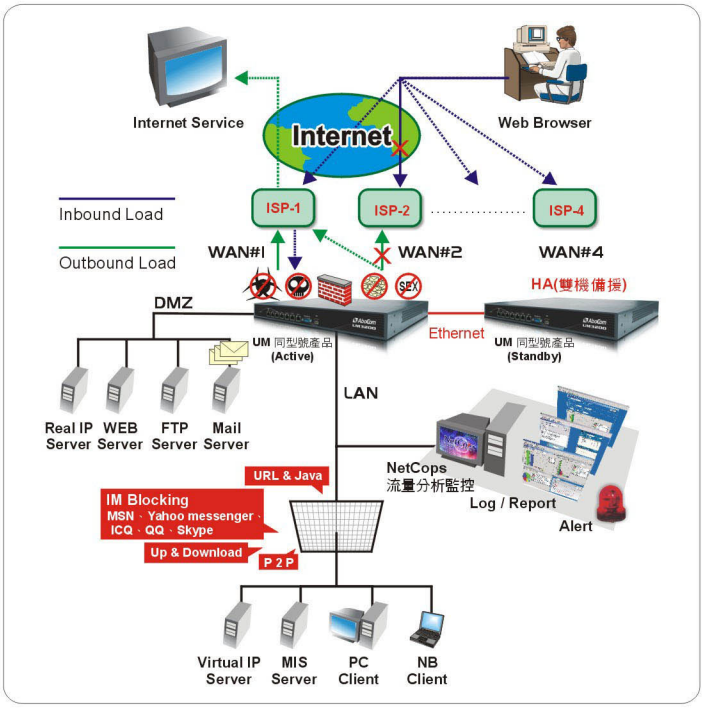
UM產品提供4~12個網路介面(WAN/DMZ/LAN埠)，可由管理者依照企業資安政策，自行定義與分組管理，不同組別的網路介面無法互連，滿足企業需要多個WAN/DMZ/LAN埠的需求並兼顧彈性與擴充性。如果將所有的網路介面都設為LAN埠，可將UM產品當做Internal Firewall(內部防火牆)架設於企業內部網路，將企業內網分隔為多個區域，提供區域間網路傳輸的多重安全防護與過濾控管(Anti-Virus、IDP、WAF…)，有效避免某個區域發生網路安全事件(內部中毒、異常流量攻擊…)，蔓延影響到整個企業網路，內建旁路(by pass)機制，不會因系統故障造成網路中斷，並具備In-Lin(Gateway)及Transparent的運作模式。

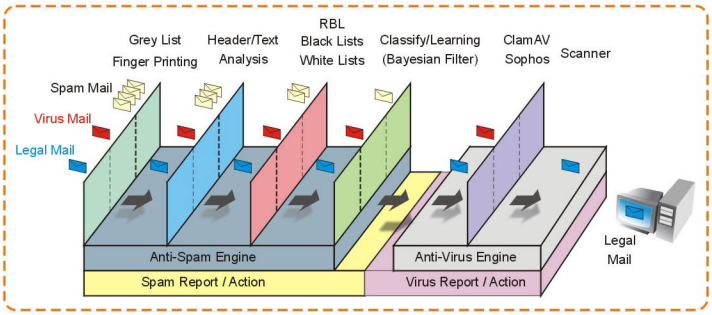
◎支援IPv4與IPv6的網路協定

UM產品除了支援傳統的IPv4網路協定，同時也支援最新的的IPv6網路協定，提供兩者並行使用的網路環境，企業可全面提昇網路適用性與便利性，無需擔憂IP網址短缺與網路協定轉換的問題。

◎高準確率的垃圾郵件過濾(Anti-Spam)

UM產品能定時自動回饋學習郵件過濾資料庫，再配合貝氏過濾(Bayesian Filter)郵件評分機制、自動學習機制、指紋辨識(Finger Printing)、灰名單(Grey List)及管理者與使用者可自訂的整體與個人郵件規則與評分與白/黑名單(RBL)使用，讓使用者與管理者隨時增加垃圾郵件與病毒郵件資料庫，UM產品隨時會學習最新過的濾機制，提高判斷率將近99%，有效降低誤判率，且可隨時取回信件，方便管理與掌控企業重要的電子郵件品質及效率。人工智慧型自動學習機制(Auto-





Learning)，可將SPAM判斷標準隨時作調整，以因應網路環境的成長與發信邏輯的改變，進以提高判斷垃圾信的精準度，同時降低誤判的機會。UM產品提供郵件隔離區可做出詳細的郵件過濾報告，與多樣化的處置方式，問題郵件可定時郵寄給郵件帳戶使用者，方便使用者隨時可取回隔離區的郵件。UM產品可自動隔離大量”字典攻擊”郵件，提供阻擋郵件攻擊(DoS)的防護功能，支援郵件內容黑名單連結掃瞄，保護Mail Server正常運作。具備DNS反查功能，並支援由內對外發信(Out-bound)及由外對內收信(In-bound)的垃圾郵件掃描過濾及病毒掃描過濾功能，用戶可在個人隔離區進行郵件檢索瀏覽及取回信件，管理者可自訂個人郵件隔離區的大小與存放時間。同時提供Gateway / Transparent / Relay Mode，不需額外安裝任何軟體及不需設定過濾關鍵字，不需改變現有環境與Mail Server，即可輕鬆完成垃圾郵件過濾防護。提供LDAP / Ad帳號認証功能，並支援郵件帳號匯入及匯出功能，可與企業的RADIUS或LDAP/AD Server整合同一帳號認證授權。支援Mail Realy及SMTP寄信認證功能，確保郵件安全性，具備郵件日誌記錄(Mail Log)可用條件查詢(含日期/收發信人/主旨/狀態)，透過UM產品的垃圾郵件過濾機制，可拒絕收取無效收信者及阻止使用者利用Spoof Domain寄信。貝氏過濾法可提供郵件加權評分，藉以調整垃圾郵件過濾條件及學習能力，並可自訂垃圾郵件過濾標準，可依不同標準將郵件分為隔離郵件、封鎖郵件、郵件主旨標記放行郵件。UM產品的Mail Log提供完整的郵件搜尋功能，查詢條件包含Mail處置狀態、收發者IP位址、網域(Domain)、主旨、日期…等關鍵字，並可置入黑/白名單過濾使用，具備SMTP郵件協定，相容於所有平台的Mail Server，支援多台郵件伺服器及多個網域(Domain)的企業環境，系統會透過Internet網路自動更新垃圾郵件特徵碼，維持最準確的垃圾郵件過濾機制。

◎郵件攻擊偵測防禦

UM產品除了內建垃圾郵件過濾及郵件病毒過濾的郵件安全機制外，提供DNS反查功能，針對各式各樣的郵件安全威脅與攻擊，例如：郵件阻斷(DoS)攻擊、郵件字典攻擊(Dictionary Attack)、阻絕寄件者偽裝網域(Spoof Domain)、阻絕無效收信者的郵件…系統內建郵件攻擊偵測防禦的保護機制，並可限制每個來源IP每分鐘產生的連線數及同時最大連線數，郵件在佇列中停留的最長時間，確保企業的電子郵件系統與服務運行正常。

◎郵件備份(Mail Backup)及郵件稽核歸檔(Mail Audit & Archive)

UM產品內建郵件備份(Mail backup)當Mail Server故障或無法收信時，UM產品仍可代為收信，等到Mail Server修復後, Um產品會將之前代收的郵件自動存入Mail Server。郵件稽核記錄(Mail Auditing)機制，當企業往來信件符合預設的稽核條例時，會執行稽核動作，例如執行"審查"稽核，系統會暫時阻擱該信件傳送，待管理人員審查無誤後放行，確保企業機密不外洩。

同時企業往來信件亦可歸檔備份保存(Mail Archive)，管理者可在任何時間及地點，連線進入系統調閱所歸檔的郵件，針對寄送大量郵件的用戶，管理者亦可透過"延遲"稽核另定企業離峰時間寄發此類用戶的大量信件，避免延誤其他用戶的寄信權益，確保企業正常營運。

◎多引擎的病毒過濾防護(Anti-Virus)

UM產品內建及可同時使用Clam AV及 Sophos兩種病毒過濾引擎，可準確地找出夾藏在郵件(POP3、SMTP)中的病毒或隱藏於HTTP(網頁)及FTP(傳檔)服務內的病毒，Clam AV能永久免費的自動更新病毒碼。這可讓UM產品的病毒防護功能，能以最低的成本，永遠保持在最新的狀態。並且可以針對HTTP及FTP的存取做病毒掃描，讓網路達到最嚴密的防護。UM產品每10~30分鐘會透過Internet網路自動更新病毒特徵碼，確保病毒碼隨時保持在最新狀態，可建立廣泛而堅實的防毒解決方案，保護企業網路免於病毒、蠕蟲(Worm)、特洛伊木馬、混合式威脅、間諜軟體、網路釣魚(Anti-Phishing)與其他不當的網路內容所造成的危害，提供完整病毒過濾報表及隔離通知，並支援異常警告(Alarm)，可記錄於Log及透過E-mail通知給指定人員。

◎詳細的郵件日誌記錄與圖形化統計分析報表(Mail Log & Report)

透過郵件日誌(Mail Log)以條列式詳細記錄每封郵件的處置動作與內容，提供關鍵字的全文檢索查詢，可提供日期/收發信者位址/主旨/處理方式等關鍵字查詢功能，方便管理追查信件流向與除錯分析。可自訂網域、郵件位址、郵件主旨、郵件表頭、郵件內容及黑/白名單的郵址或IP…等關鍵字。系統將記錄以圖形化統計報表呈現，管理者一目了然輕鬆獲得Anti-Spam & Anti-Virus運作狀態。

◎主動式入侵偵測防禦系統(IDP)

※內建主動式入侵偵測防禦系統(IDP)機制，可做到網際網路4~7應用層的檢測防護，有效阻絕各種攻擊，即時通知管理員並提供詳細的IDP報告及通信協定異常統計分析、流量統計異常分析報表，作為分析判斷及調整網路政策。

※有效防護威脅攻擊並提供『特徵資料庫』(Signature Databas)約7,000個預設攻擊模式，具備異常行為分析，並可主動線上更新(透過Internet網路，每30分鐘自動檢查更新)。

※為有效防範威脅攻擊，具備應用程式(服務)及DoS、DDos等即時阻斷服務偵測及防護，具備In-Line透通及旁聽的運作模式。

※預設的『特徵資料庫』可允許用戶自行修改它的Action與級數，具備兩種Action的模式(Pass及Drop)，可自行定義『特徵資料庫』，防範新類型攻擊。

※內建丟棄攻擊封包(Drop Atack Packet)、TCP Reset中斷入侵攻擊連線及SynFlood、UDP Flood、ICMP Flood、Port Sacn、HTTP Inspect…等異常入侵偵測防禦機制，並可設定最大流量、阻擋動作(放行/丟棄攻擊/中斷連線…)、阻擋時間、事件記錄件(Event Log)與警示通知(Alarm)管理者。

※提供威脅攻擊記錄及報表查詢功能，可查看Soure IP或Destination IP相關記錄，並提供攻擊事件記錄(Log)。

※報表查詢可查看多種記錄：Source IP or Destination IP相關記錄、特徵分類相關記錄、相關事件內容記錄。

◎網頁威脅防禦系統(WAF)

內建網頁威脅防禦系統(WAF)機制，支援Web 2.0、各種Web Server(IIS、Apache..)、腳本語言的網站應用防火牆，具備即時阻斷攻擊機制，防止HTTP連線分散式阻斷服務攻擊或程式。可防禦Cookie植入攻擊及Cookie加密連線防止連線被篡改。具備網頁參數竄改攻擊及網站攻擊偵測防禦，當偵測到入侵攻擊時，即時提供示警(Alert)及記錄(Log)並馬上以E-Mail通知管理者，協助企業防禦各種針對網站應用程式的攻擊，並提供詳細的圖形化統計報表並可輸出分析查察相關資訊，協助企業落實HIPAA、PCI-DSS…等標準規範。系統可針對特殊攻擊事件，如緩衝區溢位(Buffer overflow)、Cookie篡改下毒(Cookie Poisoning)、跨站腳本(Cross Site Scripting)、注入弱點(Injection Flaw)、惡意程式執行(Malicious File Execution)、連線竄改(Session Hijacking)、資料隱碼(SQL Injection)提供偵測與防禦機制。

◎完整的負載平衡機制與策略路由

In-bound / Out-bound Load balance

UM產品提供多個WAN埠(管理者可自行定義)，可連接對外不同的ISP線路(ADSL、Cable、E1、T1、T3)並提供In-bound及Out-bound的負載平衡機制。Out-bound load balance透過負載平衡演算法則，自動分配流量於各個線路，具備合併線路頻寬及斷線自動備援機制，也可選擇手動功能，提供循環分配、權重分配、依流量/連線數/封包數/線上遊戲/使用者/服務埠/目的位址…等手動設定模式，讓企業運用網際網路發揮最大使用效益並無斷線之虞。同時UM產品也提供In-bound load balance，In-bound負載平衡演算法則包括：Round Robin / Weight & Priority / Auto Backup / by Source IP…等，內建DNS伺服器服務，可以維護多個網域(Zone / Domain)，每個網域又可以新增多筆紀錄(A / CNAME / MX)，達到In-bound Load Sharing的功能，讓企業對外提供Internet服務能有效運作，妥善分配外部使用者訪問企業網站之流量於各個WAN埠線路，降低各條線路的負載量，確保網路連線品質，即使其中某條對外線路異常或中斷，也不會影響企業的正常營運，確保供企業網路快速穩定不斷線的服務品質。

Server Load balance

UM產品除了提供線路的In/Out-bound負載平衡，也提供了企業內部多主機的Server Load balance，具備循環分配/備援模式/依來源位址…等，提供多項內部伺服器的負載平衡與備援機制，強化企業的營運順暢與競爭力。

VPN Load balance

UM產品針對IPSec/PPTP提供VPN Trunk的VPN負載平衡機制，提供VPN使用WAN多線路的合併頻寬與斷線自動備援功能，大幅提高VPN連線速度與品質穩定性。

策略路由

企業如需更精確掌握對外線路的使用，可透過SG產品內建的策略路由(RIP/OSPF/BGP…)機制，透過多重路由(Multiple Subnet Routing)功能，可讓不同網域(Subnet)的用戶直接路由出去；並支援Transparent / Routing / NAT / PAT多種模式，並且可以同時運作。配合企業網路政策，調整控管對外線路的運作，發揮企業網路最大的使用效益。

◎策略式防火牆及內部防火牆 (Policy-base Firewall & Internal Firewall)

UM產品提供策略式防火牆功能，內建多種常見的駭客攻擊防禦模式，可主動攔截多種網路攻擊類型與自訂網路存取規則，配合24x7全天候排程表管理，即時預警(Alarm)及日誌紀錄(Log)，發現異常可傳送E-mail即時通知管理者，加強組織內部網路安全的防護。完整駭客防禦功能(Anti-Hacker)與網頁內容過濾(Content Filtering)，配合企業資安政策，可將其套用到UM產品的管制條例，並可針對特定IP/MAC/Group做範圍控管。針對癱瘓網路型攻擊或蠕蟲提供入侵偵測、防禦與警告通知，具備入侵攻擊偵測(IDS)並可記錄入侵方式及時間和IP來源，保護企業網路的安全性。

◎網路應用軟體過濾管制(Block IM、P2P、Tunnel、On-line Game…)

UM產品提供最讓MIS人員困擾的IM即時通訊(Skype、ICQ、QQ、MSN、Yahoo Messanger..)及P2P點對點傳輸軟體(eDonkey、Foxy、e-Mule、BitTorrent、WinMX..)的行為模式過濾，有別於一般傳統阻擋Port方式過濾，讓用戶再也無法透過更改Port(埠號)方式來使用IM或P2P軟體，可有效過濾控管IM即時通訊的交談與傳檔行為及P2P軟體阻擋機制。並提供特徵資料庫(Signature Database)，並可透過Internet網路自動線上更新，不需透過韌體更新方式，透過Internet網路直接下載最新的IM即時通訊或P2P點對點下載軟體的特徵資料庫。除了上述的IM、P2P的網路應用軟體外，UM產品亦可過濾管制網頁郵件(Web mail)、線上遊戲(On-line Game)、穿牆軟體(Tunnel)、影音軟體(PPLive、ezPeer..)、遠端控制(VNC、TeamViewer..)、炒股軟體….等，確保企業網路安全及避免網路頻寬不當佔用等問題。

◎網站過濾管制(URL Filter & URL Block)

支援最先進的網站類別雲端資料庫過濾機制(URL Filter)、提供網站黑/白名單(URL Block)、MIME/Script、副檔名、群組、ActiceX、Cookie、Popup、Java Applet…等網站過濾控管機制與統計分析報表，提供鉅細靡遺的記錄，協助管理者後續監控管理與資料存查，藉以調整網路資安使用政策。

透過網站類別雲端資料庫過濾(URL Filter)的機制，將Internet的所有網頁分為8類(非法網站、色情網站、博奕/遊戲、社會/經濟、互動/服務、休閒/嗜好、教育/新知、其他類別)共計64個子項目(URL Data Base)，提供資料庫更新下載機制。只要勾選需要過濾或放行的網站類別，套用到策略管制條例內，便可輕鬆執行企業用戶或部門/群組的網站(頁)瀏覽的過濾管制。透過網站過濾(URL Block)的機制，可以用萬用字元(Wildcard: *, ?)，或是用關鍵字(Key Word)建立黑/白名單，用來限制使用者無法瀏覽不雅或色情內容的網站(頁)或只能允許瀏覽指定的網站(頁)。

一般管制(Script Blocking)功能：可以阻擋網站使用MIME Type、Popup、ActiveX、Java Applet、Cookie...及檔案上傳下載的管制：可以限制使用者利用HTTP或FTP上傳下載任何檔案外，亦可限制特定檔案(例如：exe、zip、rar、pdf、bin...)的傳輸。

提供防止IP Spoofing偽裝攻擊行為，可解析原始客戶端來源IP位置給Web伺服器。支援HTTP、HTTPS、FTP、POP3、SMTP、TELNET...等網路協定的第7層應用程式的過濾阻擋控管，並支援IM即時通訊(MSN、Yahoo、Skype、QQ、AOL)及P2P等應該程式的過濾阻擋控管。

提供禁止存取時的提示相關畫面，畫面內容包含使用者名稱、來源IP、目的地網址所屬分類，並能針對使用者需求製定所需封鎖頁面，同時管理者可自訂使用者違規存取時之不同錯誤訊息，及自訂客製化提示畫面訊息。

可自訂網路瀏覽政策機制，可針對使用者、時間、位置、網路協定、瀏覽器及內容格式，訂定嚴謹的網路瀏覽規則，可針對不良網站提供連線過濾功能，管理者可彈性設定禁止瀏覽的過濾條件，及對外連線使用者授權。

提供報表功能，針對上網行為，監控紀錄IP Host、使用者名稱、特定分類及特定網址(URL)等內容進行分析控管，管理者可即時或自訂時間表產生紀錄，並可依不同使用者或自訂政策，將使用者上網行為產生記錄檔，寫入各自紀錄檔案。

提供禁止存取時的提示相關畫面，畫面內容包含使用者名稱、來源IP、目的地網址所屬分類，並能針對使用者需求製定所需封鎖頁面，同時管理者可自訂使用者違規存取時之不同錯誤訊息，及自訂客製化提示畫面訊息。

可自訂網路瀏覽政策機制，可針對使用者、時間、位置、網路協定、瀏覽器及內容格式，訂定嚴謹的網路瀏覽規則，可針對不良網站提供連線過濾功能，管理者可彈性設定禁止瀏覽的過濾條件，及對外連線使用者授權。

提供報表功能，針對上網行為，監控紀錄IP Host、使用者名稱、特定分類及特定網址(URL)等內容進行分析控管，管理者可即時或自訂時間表產生紀錄，並可依不同使用者或自訂政策，將使用者上網行為產生記錄檔，寫入各自紀錄檔案。

◎3 in 1 VPN (IPSec/PPTP/SSL VPN)

IPSec/PPTP VPN Gateway & VPN Trunk

UM產品內建IPSec / PPTP的VPN完整功能(包含Site to side、Client to Side)，提供Network及CPE的VPN功能，支援DES/3DES與256Bit AES加密功能，提供VPN QoS、Scheduler、HUB、認証功能，同時支援IKE、SHA-1、MD5認證與IKE、ISAKMP自動或手動KEY交換功能，PPTP支援Server與Client模式，並提供VPN Trunk 多路負載平衡與斷線自動備援功能。

SSL VPN (Web VPN)

為了滿足行動使用者需求，讓企業員工在任何有Internet的地方皆可安全的存取企業內部網路，SSL VPN無疑是最便利、最經濟的安全存取方式，透過SSL VPN遠端安全存取服務，企業僅需透過最熟悉的網路瀏覽器介面(Web Browser)，即可輕鬆連線至企業內部網路。不論是企業高階主管進行商務旅行或外部會議，需要連線回公司進行資料搜尋或公文簽審；業務人員在外接洽客戶，必須連進公司內部系統詢價或報價或連線至內部網路作業；或有上下游合作廠商欲連結企業內部ERP系統查詢相關作業…等，遠端行動使用者都可享有安全存取的服務。更方便的是，即使行動使用者未攜帶受企業管控的筆記型電腦，利用家用電腦、公用電腦、PDA等，甚至是透過無線區域網路都不影響安全連線的建立。UM產品更支援”SSL VPN硬體認証”機制，透過使用者個人電腦的各項硬體機碼認證，不需煩雜設定便可完成SSL VPN連線。

同時UM產品可針對運行於VPN的各項網路傳輸再加以控管，包含VPN頻寬管理、連線權限、再認證…等項目，有效提昇VPN連線之安全性與品質。

◎網路頻寬控管/個人化頻寬控管/P2P使用頻寬控管

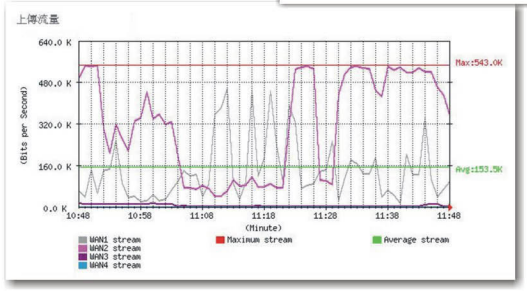
UM產品可針對不同的網路使用者與應用服務，提供最大可使用頻寬(Max. Bandwidth)及最低保證頻寬(Guaranty Bandwidth)，並可設定優先順序(Priority)及安排24x7全天候排程表的頻寬控管機制，以便讓每個Connection能得到最佳服務，有效控管網路頻寬(Global QoS)。

提供個人化頻寬管理(Personal QoS)設計。可針對個別用戶做頻寬分配之設限，簡化在頻寬分配上的規劃，並確保頻寬不會被他人所佔用。將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，再分配給內部每個使用者，依照企業網路政策，妥善分配網路頻寬給所有使用者，並可針對外送(Out-Bound)與內送(In-bound)流量分別設定頻寬控管政策，可有效防止內部用戶獨占頻寬之問題發生，避免企業無法正常運作，系統提供詳細的網路頻寬管理記錄資訊及ToP N網路流量排行統計，管理者可輕鬆掌控及妥善分配企業對外頻寬的使用，同時針對擾人的P2P多點傳播軟體，提供有效的頻寬控管機制(P2P QoS)。

網路流量排行

In-bound Load Balance

Out-bound Load Balance



圖形化網路流量統計分析

◎上網認證/授權/統計3A Service

無線網路盛行的時代，如何確認內部使用者的身份並允許上網?上網認證功能提供管理者可以限制用戶需做帳密登入確認後方可使用 Internet 網際網路，管理者可於UM產品的「內部Database」建立用戶上網認證的帳號與密碼，當使用者要透過UM產品上網或存取資料，必需輸入帳號及密碼，方能授權使用外部網際網路。除了內部帳號外，UM產品同時還提供利用網路現有的伺服器如POP3(郵件帳密)、LDAP/AD及RADIUS等已存在帳號做為上網認證，免除管理人員另建帳號，並提供單純的帳號管理。

UM產品提供上網認證/授權/統計的3A Service：AAA

Authentication：內建認證資料庫，要求使用者通過帳密認證後才可上網，並支援外部RADIUS、POP3(郵件帳密)、LDAP/AD 統一管理認證帳密。

Authorization：內含Policy策略管制功能，可嚴格控管所有進出的連線，輕鬆達成企業網路政策。

Accounting：管理人員可從鉅細靡遺的連線統計報告，獲得相關資訊藉以調整企業網路政策。

◎網路流量排行統計分析(GUI Statistics & ToP-N Account Report)

提供即時及歷史圖形化統計分析報表(可記錄於硬碟內留存)，所有網路封包的進出流量紀錄，並做網路使用監控稽核及統計記錄。更提供SNMP網管功能及網路事件與流量排行榜(TOP-N)的統計與查詢，方便MIS工程師統一管控網路設備系統效能，提供事件警訊(Event Alert)及日誌記錄(Event Log)管理功能。

◎異常流量偵測與警示(Anomaly Flow IP)

提供異常流量及內部中毒者偵測警示功能，當發現內部網路異常的傳輸量或連線數，大量發送封包企圖癱瘓企業網路時，UM產品會將攻擊加以阻擋並立即示警通知管理者及使用者，讓管理者即時瞭解網路異狀，並立即做出相關應變處置。

◎區域聯合防禦偵測與警示(Zone Defence)

企業內部若有架設網路核心交換器，UM產品提供內部網路區域聯合防禦機制：可與具備ACL指令的交換器(Switch)聯合防禦內部網路的異常流量或中毒問題，當發現飽和式及異常流量的攻擊時，可封鎖攻擊來源的IP位址，並提出警示通知管理者及使用者，讓管理者即時瞭解網路異狀，避免災情持續擴大。

◎支援VLAN / VLAN Trunk及SNMP Agent / Trap

支援虛擬區域網路VLAN及VLAN Trunk、虛擬伺服器群組(Virtual Server Grouping) 與SNMP Agent/Trap網路管理功能。

◎HA (High Availability)高可用性雙機即時備援

使用HA功能，必須使用2台相同型號的UM產品，可將一台UM產品設為Master(主要)，另一台UM產品設為Standby(備援)。

Master的UM產品會即時透過網路將設定檔複製到Standby的UM產品，且Master和Standby之間會不斷偵測彼此的運作狀況。如果Master設備故障，Standby會依照原本由Master寫入之設定來保持網路正常運作，此時正在傳輸中的資料亦不會因此而中斷，透過2台UM產品的HA雙機即時備援機制，可提供整體網路的高可用性及最佳即時自動備援性，確保UM產品不會因故中斷運作。

◎Web UI & 遠端管理

內建繁、簡體中文及英文Web UI網頁式設定管理介面，提供線上說明(On-Line Help)，無需安裝任何軟體，管理者隨時隨地可透過網路進入管理介面設定與管理UM產品，支援HTTPS(SSL)連線加密，亦可設定指定人員(IP位址)允許遠端登入設定與管理設備。

◎系統管理與使用狀態

UM產品提供所有網路介面使用狀態、軟硬體系統效能表、系統連線表、系統認證表、ARP表及DHCP用戶使用表，所有的系統使用狀態一目了然。系統具備Event Log、Sys Log日誌記錄管理功能，若發生異常事件會主動記錄及警示，系統會以E-mail發給管理者。UM產品提供設定組態異動功能，提供設定檔匯入與匯出功能，可透過Web UI直接做升級韌體(Firmware)達到系統更新功能。系統管理者可用網路瀏覽器、終端機或Telnet、網路主機或網路管理工作站與設備連線，並能設定各種參數及監控作業。

系統管理者可分層授權設定管理者及使用者密碼。

◎無使用人數授權及限制

UM系列產品無使用人數的授權與限制；垃圾郵件過濾及Clam AV防毒過濾機制，皆無軟體或特徵資料庫的授權使用費用，替企業大幅節省投資成本與降低售後維運費用。

(網站類別雲端資料庫過濾機制，可提供免費試用或選購授權使用服務，Sophos Anti-Virus提供選購授權使用服務)

可自行定義網路介面及網路分組

支援IPv4 & IPv6 網路協定

網路頻寬控管(QoS)

網路應用軟體過濾管控
(特徵碼透過Internet自動更新)

異常流量IP阻擋與警示

垃圾郵件過濾(Anti-Spam)

病毒過濾防禦(Anti-Virus)

網站類別過濾管制
(雲端URL資料庫過濾)

整合威脅防禦管理器 UTM Gateway (UM系列產品)						
產品型號		UM1200-U	UM2200-U	UM3200-U	UM5200-U	UM6200-U
硬體規格						
網路介面 (WAN/DMZ/LAN)	網路埠數	4 (Gigabit 埠) 10/100/1000 Mbps	6 (Gigabit 埠) 10/100/1000 Mbps	7 (Gigabit 埠) 10/100/1000 Mbps	12 (Gigabit 埠 / Mini GBIC) 10/100/1000 Mbps	12 (Gigabit 埠 / Mini GBIC) 10/100/1000 Mbps
	網路型式	固定式(UTP埠)	固定式(UTP埠)	固定式(UTP埠)	模組抽換式(4~12埠)	模組抽換式(4~12埠)
	屬性可自行定義	○	○	○	○	○
	網路介面可分組	○	○	○	○	○
主記憶體 (Memory)		1 GB	2 GB	2 GB	2 GB	4 GB
硬碟(Hard Disk)		500 GB	500 GB	500 GB	1 TB	2 TB x 2 (RAID-1)
電源供應(Power Supply) AC 100~240V，50/60 HZ		○	○	○	○	○
備援電源(Dual Power Redundant)		X	X	X	○	○
外觀尺寸與重量(Dimension / Weight)		44(W)x28(D)x4.5(H)cm 4.5 Kg	44(W)x37(D)x4.5(H)cm 4.5 Kg	44(W)x37(D)x4.5(H)cm 4.5 Kg	44(W)x58(D)x9(H)cm 22 Kg	44(W)x58(D)x9(H)cm 22 Kg
外觀架構(19英吋 Rackmount)		1U機架式	1U機架式	1U機架式	2U機架式	2U機架式
產品效能						
整體最大傳輸效能 (Max. Total Throughput)		1.2 Gbps	2.5 Gbps	3 Gbps	6 Gbps	6 Gbps
Port to Port NAT Throughput		600 Mbps	750 Mbps	950 Mbps	1 Gbps	1 Gbps
每日處理的郵件量(1KB/封信)		2,000,000 封信	3,000,000 封信	5,000,000 封信	7,000,000 封信	9,000,000 封信
每小時處理郵件量(1KB/封信)		83,000 封信	125,000 封信	208,000 封信	291,000 封信	375,000 封信
Anti-Virus病毒過濾效能(HTTP/FTP)		260 / 325 Mbps	325 / 410 Mbps	500 / 550 Mbps	750 / 700 Mbps	950 / 900 Mbps
IDP效能		170 Mbps	200 Mbps	700 Mbps	1 Gbps	2 Gbps
WAF效能(HTTP Throughput)		x	x	250 Mbps	500 Mbps	1 Gbps
VPN效能(IPSec DES/3DS)		100 / 80 Mbps	200 / 150 Mbps	300 /180 Mbps	500 / 450 Mbps	600 / 550 Mbps
IPSec VPN Tunnel(最大通道數)		1000	4000	4000	8000	8000
最大同時連線數(Sessions)		1,000,000	2,000,000	2,000,000	2,000,000	4,000,000
建議使用環境		~ 250人	~ 650人	~ 1,500人	~ 2,500人	~ 4,000人
軟體功能						
WAN負載平衡(In-bound / Out-bound)		○	○	○	○	○
支援IPv4及IPv6網路協定		○	○	○	○	○
In-bound負載平衡支援IPv6		○	○	○	○	○
郵件安全	垃圾郵件過濾	○	○	○	○	○
	病毒郵件過濾	○	○	○	○	○
	郵件攻擊防禦	○	○	○	○	○
	問題郵件通知	○	○	○	○	○
	郵件歸檔/稽核	X	○	○	○	○
防毒牆(Mail、HTTP、FTP)		Sophos & Clam	Sophos & Clam	Sophos & Clam	Sophos & Clam	Sophos & Clam
網頁威脅防禦WAF(Web Application Firewall)		X	X	○	○	○
主動式入侵偵測防禦(IDP)		特徵總數約7,000	特徵總數約7,000	特徵總數約7,000	特徵總數約7,000	特徵總數約7,000
策略式防火牆 / 虛擬或內部防火牆		○	○	○	○	○
策略式路由(RIP-2、OSPF、BGP)		○	○	○	○	○
排程表(24x7 Time Schedule)		○	○	○	○	○
電子佈告欄 (Bulletin board system)		○	○	○	○	○
記錄即時通訊交談的內容(MSN、QQ…)		○	○	○	○	○
網路應用軟體過濾管制 URL Block (IM、P2P、Tunnel、Webmail…)		○	○	○	○	○
檔案傳輸(上傳/下載)過濾管制		○	○	○	○	○
網站過濾管制 (黑白名單/副檔/MIME/Script/群組)		○	○	○	○	○
網站類別管制(雲端URL資料庫過濾)		○ (三年授權使用)	○ (三年授權使用)	○ (三年授權使用)	○ (三年授權使用)	○ (三年授權使用)
Local Database / RADIUS / POP3 / LDAP(AD)	認證(Authentication)	○	○	○	○	○
	授權(Authorization)	○	○	○	○	○
	統計(Accounting)	○	○	○	○	○
網路頻寬控管(Global QoS)		○	○	○	○	○
個人化頻寬控管(Personal QoS)		○	○	○	○	○
P2P使用頻寬控管(P2P QoS)		○	○	○	○	○
流量排行統計分析(記錄於HD內)		○	○	○	○	○
系統效能統計分析(記錄於HD內)		○	○	○	○	○
VPN	IPSec / PPTP	○	○	○	○	○
	VPN Trunk+備援	○	○	○	○	○
	SSL VPN	○	○	○	○	○
SSL VPN硬體認證機制		○	○	○	○	○
VLAN / VLAN Trunk		○	○	○	○	○
Virtul Server Grouping		○	○	○	○	○
Server Load Balance		○	○	○	○	○
異常連線數及傳輸量過量報告		○	○	○	○	○
異常流量IP阻擋與警示通知		○	○	○	○	○
區域聯合防禦(可自定網路交換器)		○	○	○	○	○
SNMP v3 (Agent/Trap)		○	○	○	○	○
Web UI操控介面(英/繁/簡中文)		○	○	○	○	○
透過Web UI執行韌體(F/W)升級		○	○	○	○	○
HA雙機即時備援		○	○	○	○	○
使用人數授權限制		無限制	無限制	無限制	無限制	無限制

整合威脅防禦管理器
UTM Gateway

UM 系列產品

UM1200
4埠UTP 10/100/1000 Mbps
(WAN/DMZ/LAN網路介面可自行定義及分組)
SMB 500 GB硬碟 / 19英吋 / 1U機架式

UM2200
6埠UTP 10/100/1000 Mbps
(WAN/DMZ/LAN網路介面可自行定義及分組)
Enterprise 500 GB硬碟 / 19英吋 / 1U機架式

UM3200
7埠UTP 10/100/1000 Mbps
(WAN/DMZ/LAN網路介面可自行定義及分組)
Enterprise 500 GB硬碟 / 19英吋 / 1U機架式

UM5200
4~12埠模組(UTP/Mini-GBIC) 10/100/1000 Mbps
(WAN/DMZ/LAN網路介面可自行定義及分組)
Corporation 1 TB硬碟 / 雙電源備援 / 19英吋 / 2U 機架式

UM6200
4~12埠模組(UTP/Mini-GBIC) 10/100/1000 Mbps
(WAN/DMZ/LAN網路介面可自行定義及分組)
Corporation 2 TB硬碟 x2(RAID-1) / 雙電源備援 / 19英吋 / 2U 機架式

友旺科技產品 二年保固

AboCom®
友旺科技股份有限公司 AboCom Systems, Inc.
- 台北辦事處：台北縣新店市寶橋路235巷130-2號4樓
- TEL：02-8912-1658 FAX：02-8912-1858
- 友旺科技中文全球資訊網：http://www.aboway.com.tw

《以上圖片規格與內容，本公司保留修改之權力，如有變動恕不另行通知》

授/權/經/銷/商